



**REFERENCE: 2/1/4
ENQUIRIES: V NJALO**

The Portfolio Committee on Justice and Correctional Services
Mr V Ramaano

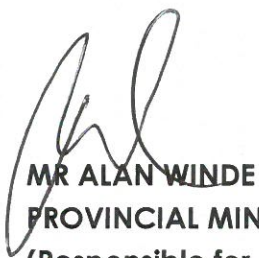
Per email: vramaano@parliament.gov.za

Dear Mr Ramaano

COMMENTS ON THE CYBERCRIMES AND CYBERSECURITY BILL

We refer to the Cybercrimes and Cybersecurity Bill, B6-2017 ("the Bill") published for public comment on the website of the Parliamentary Monitoring Group on 3 July 2017. The detailed comments of the Western Cape Government ("WCG") are attached hereto.

Yours sincerely



MR ALAN WINDE

**PROVINCIAL MINISTER OF ECONOMIC OPPORTUNITIES
(Responsible for Agriculture and Economic Development and Tourism)**

DATE: 27/7/2017

COMMENTS: DRAFT CYBERCRIMES AND CYBERSECURITY BILL

Clause <i>(Indicate clause/ regulation Number)</i>	Comment <i>(State why the clause/regulation or proposed amendment is not supported or what the problem is with the provision)</i>	Suggestion <i>(Suggested deletion/amendment/addition)</i>
General	<p>The Cybercrimes and Cybersecurity Bill [B6-2017] (“the Bill”) introduces much needed legislation that will bring South Africa in line with international laws governing internet-based crimes.</p> <p>There is a concern, however, that the Bill may go too far in imposing unnecessarily onerous standards, which might represent regulatory risks for which businesses are not yet prepared.</p> <p>The Bill also creates a number of new structures within the security cluster, as well as cross-functional ministerial and departmental responsibilities, all aimed at developing capacity to detect, prevent, apprehend and investigate cybercrime.</p> <p>An integrated approach will therefore be necessary to ensure the successful implementation of the Bill.</p> <p>A Regulatory Impact Assessment is necessary to identify any unintended consequences which may lead to unnecessary administrative burdens for businesses. A copy of the Regulatory Assessment is requested if one has</p>	

	been conducted.	
Clause 1	The word 'article' is used in the definition of article. This cannot be done as it makes the definition circular.	It is proposed that the words ' <i>the use of such an article</i> ' be deleted, and ' <i>the same means</i> ' inserted in its place.
Clause 7(3)	The contents of subparagraphs (i) and (ii) of subclause (3) should be out-dented (and the subparagraph numbering deleted) as they apply to all the items listed in paragraphs (a) to (g).	
Clause 9	The act of the offence of cyber uttering is described as "passes off". This phrase is also generally used in respect of certain acts of unlawful competition.	To avoid uncertainty, it is suggested that another phrase be used in the place of "passes off".
Clause 13	Clause 13 provides that the common law of theft must be interpreted so as not to exclude the theft of an incorporeal. The word "incorporeal" is an adjective, and hence the word "property" should be inserted after "incorporeal".	it is proposed that the word "property" be inserted after "incorporeal".
Clause 18	This clause criminalizes the distribution of data messages containing an intimate image without consent. While the addition of this offence is welcomed, it is proposed that consideration be given to broadening the scope of the offence to include sexual activity where there is no visible nudity as provided for in subclause (2)(b).	It is proposed that consideration be given to broadening the scope of this offence to include sexual activity where there is no visible nudity as contemplated in subclause (2)(b).
Clause 24	This clause rightly provides for the drafting of Standard Operating Procedures (SOP) to be followed in the investigation of cyber offences	To mitigate risks, the SOP should be aligned with the requirements of Electronic

	<p>or offences which have a cyber element.</p> <p>One of the five principles which underpin these procedures is that “any deviation from these principles should be explained”.</p> <p>In the context of data held as electronic evidence, the duty to take care is particularly high due to the difficulty associated with maintaining the integrity of such evidence.</p> <p>Any established SOP should emphasise the risks associated with handling electronic evidence (such as remote and anonymous accessibility) and how even the slightest irregularities may affect their admissibility in court.</p>	<p>Communications and Transactions Act, 2002 (Act 25 of 2002).</p>
Clause 27(1)(a)(ii)	<p>In Clause 27(1)(a)(ii) part of the criteria for the issue of a search warrant, namely an article “being used or is involved in the commission of an offence” is already incorporated in the definition of “article”.</p>	<p>This clause should be redrafted in line with the redrafted clause 28(4)(a)(ii).</p>
Clause 50	<p>There is general support for the establishment of a 24/7 Point of Contact at the SAPS. This body should be adequately resourced or it runs the risk of being ineffective.</p>	
Clause 50 (5) (b)	<p>Unlike other Acts referenced more than once in the Bill, the National Strategic Intelligence Act (Act No. 39 of 1994) is not defined in section 1.</p>	<p>Provide a definition for the Act in section 1.</p>
Clause 52(3)	<p>This clause determines that the electronic communications service provider or financial institution that does not comply with the obligations set out in subclause (1) is guilty of an offence and is liable on conviction to a fine of</p>	<p>It is proposed that the penalty provided for in clause 52(3) be revisited.</p>

	<p>R50 000.</p> <p>This penalty appears disproportionately low when compared to the penalty provided for in clause 37(3) read with clause 37(1).</p> <p>It is submitted that the maximum penalty provided for in clause 52(3) of a nominal amount of R50 000 will not sufficiently prompt service providers or institutions to comply or fulfil their obligations provided for in subclause (1).</p>	
Clause 53	<p>Provision should be made for provincial level representatives on the Cyber Response Committee.</p>	
Clause 57(3)	<p>It is noted that provision is now made for consultation with the Premier of a Province in the circumstances listed in subclause (3)(b). Hence, the Cabinet member responsible for State security will be required to consult with the relevant Premier before he or she declares as a critical information infrastructure, an information infrastructure <i>"under the functional control or administration of a Provincial Government"</i>, which <i>"relates to or is incidental to a functional area listed in Schedule 4 or 5 of the Constitution"</i>, or in respect of <i>"any matter outside the functional areas listed in Schedule 4 or 5 to the Constitution that is expressly assigned to the province by national legislation"</i>.</p>	<p>In light of the impact on, and the Constitutional mandate of provinces in the listed matters, the consultation requirement in this clause should be amended to require the <u>concurrence</u> of the Premier in the Province concerned.</p>
Clause 57 (11)	<p>Clause 57(11) authorises the Cabinet member responsible for State security to take the steps specified in a notice issued under clause 57(9) in the event that the owner or person in control of the Critical Information Infrastructure fails to</p>	<p><i>"subject to section 100 of the Constitution"</i> should be inserted at the beginning of clause 57(11).</p>

do so. This on the face of it appears to allow for the possibility of the Cabinet member taking such steps on behalf of a province where information held by a province or municipality is declared as a Critical Information Infrastructure under clause 57(3).

Any such steps would in these circumstances need to be taken in accordance with section 100 of the Constitution. Hence "*subject to section 100*" of the Constitution should be inserted at the beginning of clause 57(11).