Deloitte.

Private Bag X6
Gallo Manor 2052
South Africa

Deloitte & Touche
Registered Auditors
Risk Advisory
Building 7
Deloitte Place
The Woodlands
Woodlands Drive
Woodmead Sandton
Docex 10 Johannesburg

Tel: +27 (0)11 806 5000
Fax: +27 (0)11 806 5202
www.deloitte.com

10 August 2017

Honourable Dr Mathole Serofo Motshekga
The Chairperson of the Justice and Constitutional Development Portfolio Committee
C/o The Secretary
3rd Floor
90 Plein Street, Cape Town
8000

Attention: *Mr V Ramaano*
Per email: *vramaano@parliament.gov.za*

Dear Dr Motshekga

WRITTEN SUBMISSION ON THE CYBERCRIMES AND CYBERSECURITY BILL (B6-2017)

We write to you on behalf of Deloitte Risk Advisory in relation to the latest Cybercrimes and Cybersecurity Bill (B6-2017) ("**Cyber Bill**") currently under consideration by the National Assembly. We thank you for this opportunity to submit a written submission to the Justice and Constitutional Development Portfolio Committee ("**the Committee**") regarding the Cyber Bill in response to your call for comments as published on www.justice.gov.za on 3 July 2017.

Of late, visibility of cyber risk has gained significant momentum as a result of the global headlines relating to repeated cyber-attacks. Cyber threats engender the most concern among business executives, as no business is immune against cyber-attacks, which can impact a company's reputation, threaten its bond with customers, and open it up to lawsuits and regulatory scrutiny.

We welcomed the changes that were made to the 2015 draft version, however in our view, there still remain some concerns and/or need for clarification, particular with regard to the following key points:

- **Section 1 – Definitions**

1. **"Computer":** We make the following suggestion for the definition of "computer" to ensure adequate inclusion of operational technology such as medical devices, self-driving automobiles, automotive automation, aviation automation, Internet of Things devices, home-automation, building management systems and automation, industrial control systems, etc.:

   "computer" means any electronic programmable device used, whether
   by itself or
   as part of a computer system or any other device or equipment or any part thereof
   to perform predetermined arithmetic, logical, routing, processing or storage operations or physical actions in accordance with set instructions and includes all—
   (a) input devices;
   (b) output devices;
   (c) processing devices;
   (d) computer data storage media; and
   (e) other equipment and devices that are related to, connected with or used with such a device;

2. **"Public available data"**: We suggest that the grammatically correct form for data that is available in the public domain is "*publicly available data*" and the opposite is "*non-publicly available data*".

- **Section 2 – Unlawful securing of access**

We appreciate the fact that this clause intends to criminalise individuals who get access to data or devices without permission, however the wording of the clause does not provide for instances where an individual may gain access and misuse another individual's data or device negligently versus the intentional misuse by an unauthorised person.

- **Section 17(2)(d)**

The subsection states that a data message is harmful when "it is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons". It is put forward that the requirement of the data message being false in nature should be sufficient for the data message to be harmful and the remainder of the elements should not be required.

- **Section 18**

It is submitted that negligence be included in subsection 18(1), as the there is a likelihood that persons may negligently make available, broadcast or distribute, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his consent. The requirement of intention provides a higher standard of proof, whereas negligent behaviour in this regard should be addressed.

Further, it is submitted that the definition of "intimate image" is narrow and should be extended to avoid misinterpretation or parties intentionally creating defences for possessing intimate images which contain elements which fall outside of the current definition.

- **Section 22**

It is a submitted that a minimum fine in respect of non-compliance with all sections would be more impactful.

- **Section 37**

It is submitted that section 37(1)(e) be amended to include that information shall not be disclosed during the course of investigation of criminal proceedings and not only in the institution of criminal proceedings to extend the protection of the information during the investigation phase.

- **Section 52 – Obligations of electronic communications service providers and financial institutions**

Section 52(1)(a) requires that an electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any cybercrimes as defined in the Bill, "without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service". It is submitted that "feasible" be defined as it is unclear and could lead to the requirement being ineffective as it contradicts the requirement for reports to be made within 72 hours.

Although non-compliance with the clause is criminalised, it is not very clear how the R 50 000 fine stated in section 52(3) will be attributed. Will an electronic communications service provider or financial institution be fined R 50 000 per category/class of offence OR per offence which it fails to report timeously?

- **General - Overlap with the Protection of Personal Information Act ("POPI")**

Our submission is by no means exhaustive and does not set out to provide a detailed technical or legal analysis of the current draft Cyber Bill. As an interested party, we rather aim to highlight certain key points which we believe need further discussion and clarification to ensure that everybody's right to cybersecurity is adequately protected and that there is a proper balance between our rights to privacy, freedom of expression and access to information.

We trust that our submission will assist the Committee in its deliberations around finalising the Cyber Bill.

Although we do not intend to address the Committee in person, we will be available to elaborate on our submission should the Committee deem this appropriate.

Yours sincerely

Candice Holland
Director
Deloitte & Touche
Tel/Direct: +27 (0)11 209 8598
Cell: +27 (0)82 330 5091
caholland@deloitte.co.za