sabric
Making South African banking safe, secure and fraud free

Sabric House,
Hertford Office Park,
90 Bekker Street,
Vorna Valley, Midrand
PO Box 3682, Halfway House, 1685 Tel: 011 847 3000 • Fax: 086 240 9838
Website: www.sabric.co.za

8 September 2017

Your Ref:
File Ref.
Direct Tel No: (011) 847-3106
Direct Email: kalyanip@sabric.co.za

The Honourable Dr. Mathole Motshekga MP
Chairperson
Portfolio Committee on Justice and Correctional Services,
3rd Floor, 90 Plein Street, Cape Town,
8000

Attention: Mr V Ramaano
Committee Secretary: Portfolio Committee on Justice and Correctional Services
National Assembly

Per e-mail: vramaano@parliament.gov.za

Dear Dr. Motshekga,

RE: SABRIC Comments on the Cybercrimes and Cybersecurity Bill [B6 – 2017]

The South African Banking Risk Information Centre (SABRIC) is a Not for Profit Company formed by the four major Banks to assist the Banking and Cash in Transit industries combat organised crime. We aim to be Africa's trusted financial crime risk information centre, leveraging on strategic partnerships and currently have 19 banks as our members. More information on SABRIC can be found on our website www.sabric.co.za.

SABRIC is appreciative for the opportunity to comment on the above-mentioned Bill and believe that our comments will be beneficial to the Committee when assessing whether the Bill will achieve its objectives.

SABRIC plays a role in coordinating cybercrime and cybersecurity initiatives for the banking industry. We also act as the nodal point for the banking industry in collaboration with local and international stakeholders including law enforcement and the Cybersecurity Hub. Noteworthy initiatives currently underway include, amongst others:

- Creating consumer awareness for cybersecurity.
- Hosting the Banking Industry CSIRT for information sharing across participating banks.

- Development of a cybersecurity skills framework and lobbying for recognition of cybersecurity as an occupation.

With respect to this version of the Bill, as introduced in Parliament and referred to your respective Committee, we have consulted with our members who have mandated SABRIC to submit this proposal on their behalf. In addition to participating and making our submissions to the Expert Working Committee on the Bill, we would like to put forward the following additional comments for consideration:

Investigation and Prosecution of Cybercrimes:

- Current legislation dealing with cybercrime is fragmentary and inadequate. Bringing all related provisions into one piece of legislation not only assists with identification of possible gaps but also provides a practical framework for enforcement.
- The Bill criminalises cybercrimes comprehensively and substantially in line with international precedents. We submit that the offences will enable prosecution of perpetrators who previously could not be addressed, due to the lacunae in our legislation. A shortcoming in the Bill is, however, the failure to criminalise offences relating to identity theft. We are of the view that the current provisions in POPIA are insufficient to address identity theft adequately and that this aspect requires attention.
- Current legislation does not provide adequate sentences for cybercrime. The Bill prescribes proportionate penalties for these offences.
- Specialised procedures, which did not previously exist to investigate cybercrimes, are proposed in order to facilitate the investigation of cybercrimes. A welcome addition would be the Standard Operating Procedures that needs to be enacted in order to regulate cyber investigations. If this is done in accordance with international standards, it will positively contribute to the admissibility of electronic evidence in courts of law.
- The Bill also proactively, and in line with the international benchmarks, specifically empowers the SAPS to make use of private forensic investigators. This may to some extent, help to alleviate the current skill shortages in the SAPS to deal with the investigation of complicated cybercrimes. However, it is submitted that the SAPS should continue to focus attention on obtaining the necessary expertise to independently investigate cybercrime.
- To the best of our knowledge, South Africa has not ratified any international convention, which specifically deals with cooperation in cybercrime matters. It is submitted that the Bill will facilitate international cooperation, since the Bill is substantially in line with international benchmarks and specialised procedures are included in the Bill to facilitate international co-operation, pending formal request for international co-operation.
- Due to the nature and extent of cybercrime, which is escalating, it is submitted that Government as well as the private sector must ensure that the necessary knowledge and skills are obtain to deal with cybercrime and cybersecurity. The establishment of the various structures within Departments as well as the private sector may help to focus attention on these aspects.

Critical information Infrastructure

We agree that the protection of critical information infrastructure of a country is essential. The Bill aims to address this aspect, which we support. Of concern, is that the implementation of the

cyber initiative for South Africa will seemingly be placed under control of Government only. We submit that both the public sector and the private sector have an interest in the protection of critical information infrastructures and a secure cyberspace. The implementation of the cyber initiative of the Republic may be expedited if Government and the private sector work together. Given the vast experience and expertise within the private sector, we believe that valuable contributions to policy decisions that may affect them, can be made. We propose that consideration be given to incorporating a structure into the Bill whereby private sector industry leaders can engage with Government on cybersecurity related issues.

CSIRTS

The creation and recognition of private sector CSIRTs is critical to ensuring that authorised participants are informed of cybersecurity incidents and that necessary steps are taken to address identified vulnerabilities. The flow of information across CSIRTS and between public and private sector CSIRTS is equally important. Whilst the Bill recognizes the Cybersecurity Hub as the nodal point between Government and private sector CSIRTS and grants the Department of Telecommunications and Postal Services the powers to issue regulations on what CSIRTS should comply with, we would like to caution that over regulation of CSIRTS would not necessarily translate into improved cyber resilience for the country. We submit that two-way information flows will encourage collaboration that will ultimately improve the country's resilience. The provision in the Bill enabling information sharing is long overdue and critical for the prevention and detection of cybercrimes.

International Collaboration

In our experience, cybercrime and cybersecurity incidents are seldom launched and executed from within South Africa only. Most incidents have an international perspective to them and this is exploited by criminals, who seem to think that jurisdictional challenges will ensure that there are little or no consequences for their actions. International collaboration to stay informed and understand the cybercrime and cybersecurity landscape is critical. From a private sector perspective, great effort is made to engage on cybercrime and cybersecurity matters at a global level. We urge that that similar initiatives be implemented within Government so that South Africa is an active participant in global efforts to address cybercrime and in so doing, make our jurisdiction less attractive to transnational organized criminals.

Skills Development

The effectiveness of this Bill is dependent on successful implementation. It is acknowledged that there is a skills shortage in both the public and private sectors currently and thus skills development on all fronts is critical. We propose that Government collaborates with the private sector for skills development and that a series of strategic initiatives be adopted to fast track capacity building. While responding to cybercrime is a high priority, cybersecurity within Government is equally important and the private sector could share lessons learnt in this regard. We submit that it is of utmost importance that special training programs, to obtain the necessary knowledge to deal with cybercrime and cybersecurity, are adopted across the private and public sectors.

Conclusion

SABRIC once again thanks the Committee for the opportunity to provide comments on this Bill. We trust that our comments and proposals will be taken into consideration as the Committee undertakes its processes and deliberations on this Bill.

Yours faithfully

Kalyani Pillay
CEO
SABRIC