Telkom

Submission to the Independent Communications Authority of South Africa

THE DISCUSSION DOCUMENT ON THE INQUIRY INTO THE ROLE AND RESPONSIBILITY OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA ("ICASA") IN CYBERSECURITY PUBLISHED IN GOVERNMENT GAZETTE NO. 41944 DATED 28 SEPTEMBER 2018

30 November 2018

Table of Contents

1. EXECUTIVE SUMMARY

1.1 Telkom SA SOC Limited ("Telkom") welcomes the opportunity to submit its written comments on the inquiry into the role and responsibility of the Independent Communications Authority of South Africa (the "Authority") in Cybersecurity published in Government Gazette 41944 dated 28 September 2018 (the "Discussion Document").

1.2 Telkom recognises that under the Electronic Communications Act ("ECA") the Authority has a mandate to protect the interests of consumers, ensure information security and network reliability and protect the integrity of the electronic communications network.

1.3 The legal and regulatory framework governing the security of information, computers and computer systems, computer software programmes and the authentication of IoT devices and services involves various regulatory authorities, industry bodies and associations, including the Department of Telecommunications and Postal Services ("DTPS"), National Cyber Security Advisory Council, the Information Regulator, the State Information Technology Agency ("SITA"), the State Security Agency ("SSA"), Department of Justice and Constitutional Development ("DOJ"), the National Prosecution Authority ("NPA"), the South African Police Services ("SAP"), the Department of Defense and Military Veterans, the Department of Science and Technology, the Department of Higher Education, the Department of Public Service and Administration, the Presidential Infrastructure Coordinating Commission and Films and Publication Board.

1.4 Telkom agrees that the Authority can play a role in raising consumer awareness towards cybercrime, cybersecurity and research and development, subject to adequate resources. However, the coordination role for cybersecurity must reside with an entity such as the National Cyber Security Advisory Council. The Authority should further take into account existing regulations which regulate some of the aspects in the Discussion Paper, as set out in this document.

1.5 With regards to further regulation of Cybersecurity standards, any such proposed regulation must be subject to regulatory impact assessments ("RIAs") to measure the impact of any proposed cybersecurity measures on operators and follow an open and transparent consultative process where operators can make submissions. Furthermore, any additional regulation should be available for input and comment by industry. Telkom further proposes regulation which permits licensees to detect and

disconnect comprised electronic communications equipment which may be harmful to operators' networks.

1.6 In summary, Telkom supports a regulatory framework which promotes regulatory certainty with a clear delineation of roles and responsibilities between regulatory authorities with regard to identifying cybercrimes, protecting consumers against cybercrimes and response mechanisms.

2. SPECIFIC COMMENTS

This section will set out Telkom's responses to the specific questions in the Discussion Document.

2.1 Question 1: Does the evolution of technologies necessitate the evolution of the regulatory function of the Authority?

Telkom is of the view that the effect of technology evolution on information security issues is already addressed by various entities and does not necessarily require an evolution in the regulatory function of the Authority. As stated in the Discussion Paper, there are currently several government interventions in South Africa on cybercrimes and cybersecurity which are guided by the National Cybersecurity Policy Framework ("NCPF"), and a Cybersecurity Working Group was established by Government to identify gaps and challenges in the implementation of policies and or legislation.

2.2 Question 2: How would you define cybersecurity?

Cybersecurity operates within a highly technical environment and is often included under a generic Information Technology ("IT") or Information Security banner. The concept of Information Security covers three main threat areas: accidental, environmental, and adversarial. Cybersecurity is a subset of Information Security that is concerned with the prevention, detection and mitigation of adversarial threats and attacks. It revolves around the use of IT to protect the confidentiality, integrity, and availability of information contained within or accessed by an IT or communications system or subscriber to such services. It aims to provide protection against criminal activities carried out by means of computer systems, computer technology or the Internet and a network. It is thus important to consider other concepts such as cybercrime, cyberfraud, cyberthreat related to the concept of cybersecurity.

The Memorandum on the objects of the Cybercrimes Bill, 2007 recognises that there is no general universally recognised definition of cybersecurity and proposes that the term "cybersecurity" can more readily be defined as "technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer-systems, against cybercrime, damage or interference."

The National Cybersecurity Policy Framework of South Africa, 2012 defines Cybercrime to mean: “illegal acts, the commission of which involves the use of information and communications technologies”. A new definition of cybercrime proposed in the Electronic Communications and Transactions Amendment Bill of 2012 states that “cybercrime means any criminal or other offence that is facilitated by or involved the use of electronic communications or information systems, including any levels or the Internet or any one or more of them.” In terms of the Cybercrime Bill, 2018, a person is guilty of the offence of cyber fraud if such person “unlawfully and with the intention to defraud, makes a misrepresentation by means of data or a computer program; or through any interference with data or a computer program or interference with a computer data storage medium or a computer system as contemplated in section 6(2) (i) causes actual prejudice; or (ii) is potentially prejudicial, to another person…”

In light of the definitions above, Telkom is of the view that the definition of cybersecurity should also include the protection of electronic communications networks from any harmful or unlawful access and acquiring of data. The definition should also extend to smart devices (such as smartphones and smart televisions) that are increasingly being used to access electronic communications networks. Further, the definition of cybersecurity should be in as far as possible, future-proof in light of rapid technological developments.

We propose that the term “cybersecurity” be defined as the application of technologies, measures and practices designed to maintain the integrity of electronic communication systems which protect data, computer programs, computer data storage mediums or computer-systems, electronic communications networks and Internet of Things (“IoT”) products and services and provide protection against cyber-attacks which may cause damage and or interference to such products and systems.

IoT products and services include smart devices, wearable health trackers, connected home automation and alarm systems and safety related products such as smoke detectors. It also includes the digital services linked to IoT devices from for example mobile applications, cloud computing / storage and third-party Application Programming Interfaces (APIs). We are of the view that it is not necessary for the definition to specifically reference national security aspects or economic harm, which may serve to limit the definition of cybersecurity.

2.3 **Question 3: Are there any other laws that the Authority should consider in determining its role regarding Cybersecurity?**

The Authority's mandate is set out in the ICASA Act. In considering the type-approval of electronic communications equipment and facilities, however, ICASA can consider the Code of Good Practise for Consumer IoT Security[1] published in October 2018 by the UK government Department for Digital, Culture, Media and Sport. This Code of Practice sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. This information can be used by ICASA in relevant awareness campaigns regarding cybersecurity as the guidelines in this Code of Practice can contribute to protecting consumers' privacy and safety, whilst making it easier for them to use their products securely. It will also mitigate against the threat of Distributed Denial of Service ("DDoS") attacks that are launched from poorly secured IoT devices.

Furthermore, the Cisco Code of Practice[2] sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer information form unlawful access and or interception. Implementing its guidelines is likely to contribute to information security and network integrity whilst making it easier for consumers to use their IoT devices securely. These guidelines bring together what is widely considered to be good practice in IoT security. They are outcome-focused, rather than prescriptive, giving organisations the flexibility to innovate and implement security solutions appropriate for their products.

Telkom would also like to emphasise the importance of the alignment of all relevant legislation on cybercrime in order to promote regulatory certainty, as well as the need for clarity regarding the mandate and jurisdiction of relevant departments and regulatory agencies with regards to different aspects of cybercrime. We further submit that any proposed operating procedures which govern the right of the SAP to access or seize any computer, data, computer program etc in the investigation of cybercrimes must be drafted in consultation with industry.

[1] https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
[2] https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

2.4 **Question 4: Section 2(q) of the ECA provides that one of the objects of the ECA is to "ensure information security and network reliability".**

2.4.1 ***Question 4.1: What is information security and network integrity and what is your understanding of the Authority's mandate in this regard?***

Information security refers to the protection against or measures taken to achieve protection against the unauthorised access, use, disruption, disclosure or destruction of information, especially electronic data. It focuses on the protection of the confidentiality, integrity and availability of data. It aims to ensure data integrity, i.e. maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle and ensuring that information can only be accessed and modified by those authorised to do so. In the context of computer systems, integrity refers to methods of ensuring that data is real, accurate and safeguarded from unauthorised user modification. In simple terms, what is inserted at one point of a communication network system is 100% transmitted and received at another point of communication network system.

While information security is also a crucial part of cybersecurity, information security refers exclusively to the processes designed for data security, whilst cybersecurity is a more general term that includes information security. There are different types of information security[3]:

- **Application security:** covers software vulnerabilities in web and mobile applications and APIs, which vulnerabilities may be found in the authentication or authorisation of users, integrity of code and configurations, and mature policies and procedures.
- **Cloud security:** focuses on building and hosting secure applications in cloud environments and securely consuming third-party cloud applications.
- **Cryptography:** Encrypting data in transit and data at rest helps to ensure data confidentiality and integrity, and digital signatures are commonly used in cryptography to validate the authenticity of data.
- **Infrastructure security:** deals with the protection of internal and extranet networks, labs, data centers, servers, desktops, and mobile devices.

[3] https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

- **Incident response:** monitors for and investigates potentially malicious behavior. There should be an incident response plan for containing the threat and restoring the network.
- **Vulnerability management:** the process of scanning an environment for weak points (such as unpatched software) and prioritising remediation based on risk.

The Authority has a mandate to approve electronic communications equipment and facilities under section 35 of the ECA. Accordingly, Telkom supports such type-approval, where necessary, in order to contribute towards ensuring network reliability and integrity.

2.4.2 ***Question 4.2: Is the mandate to ensure network integrity and information security currently being fulfilled by the Authority?***

Current regulations may fall short of fully addressing cyber vulnerabilities resulting from the use of IoT devices which connects to electronic communication networks as issues of cybersecurity keeps evolving as technologies evolve. Please further refer to response to question 9 below.

2.5 **Question 5: Section 36(2) of the ECA provides that "standard[s] must be aimed at protecting the integrity of the electronic communications network", kindly provide your understanding of this section.**

Telkom understands that technical standards by the Authority for the performance and operation of electronic communication equipment and facilities must have the object of protecting the integrity of the electronic communications network. The relevant technical standards would depend on the equipment involved, and which part of the network needs what protection from which potential harm, as cyberattacks exploit network vulnerabilities and target individual or organisational data at different layers of the network. For example, phishing and password attacks happen via different technologies and on the different parts of the electronic communications network.

2.6 **Question 6: Taking into account the roles that are being played by different stakeholders, what additional role should the Authority play in Cybersecurity?**

The Authority can play a role in conducting an RIA on the effect cybersecurity measures on operators, to ensure it does not increase the cost to communicate. It For example,

the Bill calls for audits re compliance with the Bill, but the content of these audits is unclear and could lead to high costs for operators. The preservation of data when operators become aware of an offence and the preservation of real-time communications may increase cost on operators. Reporting requirements and provision of data evidence to relevant structures could impose a heavy administrative burden on operators. The Authority can further assist in developing a legislative framework to provide regulatory certainty re the jurisdiction of various entities.

2.7 **Question 7: What role, if any can the Authority play with regard to Cybersecurity awareness?**

The Authority can play a role in creating awareness among consumers regarding relevant legislation on data privacy, as well as protection of their devices against cyberthreats.

2.8 **Question 8: The KCC and the Korea Internet and Security Agency (KISA) planned to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers. Should the Authority strive to follow the same approach? What legislative powers are there to enable the Authority to implement this?**

Telkom is of the view that it is not advisable or practical for operators to monitor the security levels of the computers and other devices used by customers. It will furthermore increase the cost of compliance on operators and ultimately increase the cost to communicate.

2.9 **Question 9: Should the Authority, through the end-user regulations also require licensees to limit or cut internet connectivity of users with less-than- required software protection forcing them to upgrade their existing programs or download new ones?**

Telkom supports licensees having the right to disconnect compromised equipment completely from the network. This will however require careful regulation in light of technological advances as well as loss of subscription revenue by operators, the risk of faulty disconnections etc. Any regulations must be open for public scrutiny and comment by operators.

2.10 **Question 10: Should a legislative change be encouraged which will grant the Authority the rights to suspend the business of software companies, in the ICT sector, that fail to correct the vulnerabilities of their security programs?**

Telkom advises against this, as it would seem to assign accountability solely to companies, where such companies may have been the victims of hacking or cyberattacks despite updated security software. This also interferes in the commercial sphere and affects the revenue of operators. Any such proposed legislative change must be open for public comment and involve industry participation.

2.11 **Question 11: Should the mandate of the Authority be extended to software and internet regulation?**

ICASA's mandate focuses on licensees and should therefore not extend to regulating software. It is unclear what ''internet regulation'' refers to.

2.12 **Question 12: What regulatory/legislative or self-regulatory measures are in place in the regulation of spam in South Africa? What role, if any can the Authority play in this regard?**

The regulation of spam in South Africa is regulated by several data protection / privacy laws wherein recipients of unsolicited electronic communication can opt out of future communications, including the Electronic Communications and Transactions Act, 2002 (ECTA), the Consumer Protection Act, 2008 (CPA) and the recently promulgated Protection of Personal Information Act, 2013 (POPIA or POPI).

- Section 45 of ECTA provides that recipients of unsolicited communications can opt-out of future communications and may request information from the sender where their contact details were obtained. (Section 69 of POPI (on commencement) will replace section 45 of ECTA with regards to the regulation of unsolicited commercial communications to consumers).

- Section 11 of the CPA provides that a consumer may (a) refuse to accept; (b) require another person to discontinue; or (c) in the case of an approach other than in person, pre-emptively block any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.

- The CPA also provides for a “do-not-contact registry” (DNCR) meant to allow customers to permanently opt out of all unsolicited marketing communications.

The Authority can possibly provide for a website where SPAM can be reported or aid in consumer awareness regarding rights under legislation with regard to SPAM.

2.13 **Question 12 *[please note there are two questions 12 in the Discussion document]:* To what extent should the Authority play a role in consumer education and outreach programmes?**

The Authority can actively promote digital literacy and alert consumers of cyber security threats as well as consumers’ rights under relevant legislation. In this regard, it should collaborate with regulators such as the Information Regulator as well as the Consumer Protection Commission.

2.14 **Question 13: Should the Authority, through its end-user regulations require licensees to submit network outage reports to identify trends in network disruptions and as such make a report available?**

Sub-regulation 16.1 of the End-User and Subscriber Service Charter regulations already makes provision for licensees to report Impossibility of Performance. It states that ‘’in the event that a Licensee fails to provide end-users with service due to circumstances beyond its control for a period more than two (2) hours:

a) a licensee must notify the authority in writing and issue a public notice to affected end-users
b) indicate timeframes within which end-users should expect the service to be restored
c) submit a report to the Authority detailing the events that led to the impossibility of performance.’’

It is suggested that additional regulation is not necessary. Additional regulation would further create an overlap with the propose framework under the Cybersecurity Bill which requires operators to report incidents to Computer Security Incident Response Teams (“CSIRTs”).

2.15 **Question 14: In the US, the draft Cybersecurity Act also requires telecommunications carriers to take steps to ensure that CPNI is protected from unauthorised disclosure and in this regard, the Act obliges licensees to abide by standards set by the Federal Communications Commission. Should the Authority set similar standards for licensees to ensure that customers proprietary network information is protected from unauthorised disclosure?**

Telkom is of the view that regulation 3.8 of ICASA's Code of Conduct Regulations already provides that licensees are required to provide customer information and protect the confidentiality of consumer information and further regulation is not necessary.

2.16 **Question 15: What is your understanding of networks security and how can the Authority ensure network security?**

Please see responses to questions 2 and 4 above.

2.17 **Question 16: In your understanding, how is it different from network reliability, network integrity and information security?**

Please see responses to questions 4 above.

2.18 **Question 17: Should the Authority assume some functions done by SITIC and if so, how should the Authority be resourced?**

The Authority should not assume the functions performed by the Swedish IT Incident Centre ("SITIC"). Please refer to our response to question 1 re the current framework to address cybersecurity issues.

2.19 **Question 18: What cybersecurity measures are in place by ISPs in South Africa to protect the consumers?**

Telkom has internal policies protecting customer confidential information. We further adhere to relevant regulations such as the Authority's Code of Conduct, as well as legislation with regards to data protection and privacy.

2.20 **Question 19: Should the Authority require licensees to offer new and/or all customers 'family-friendly network-level filtering[4]?**

ICASA must conduct a study to assess end-users' interest in such filtering before imposing any regulations. Any such provision should be by means of regulation which is open for public comment as it may interfere with the commercial operations of licensees and increase the cost of compliance. It must further be tested against privacy laws which prohibit access to private information. It cannot be a mandatory or default service. Filtering may also have unintended consequences such as over-blocking and under-blocking of content which is not correctly classified and violation of privacy laws relating to content.

2.21 **Question 20: Can Botnet Tracking and Detection help in threats on the network in South Africa? If yes, who must do it and how? How can the Authority get involved in this?**

Telkom is of the view such tracking and detection will be of assistance and the Authority can liaise with accredited cybercrime institutions and research institutions in this regard. Operators already have measures in place to protect their network.

2.22 **Question 22: Is POPI sufficient to deal with protection of Personal information. What can ICASA do to help enforce POPI in the ICT sector?**

POPI is in our view sufficient. The mandate to enforce POPI resides with the office of Information Regulator. The Authority can possibly assist by providing info to the Information Regulator on cybersecurity attacks reported to the Authority, should the Authority make provision for the reporting of same on the Authority's website.

2.23 **Question 23: Should ICASA be involved with Online Child Protection? If so, how?**

The Authority can be involved by raising consumer awareness and providing avenues for reporting of illicit content. In this regard, it should collaborate with other regulators and consider the provisions of all relevant legislation which criminalises online child pornography in South Africa. Cybersecurity deals with the integrity and transmission of

content, while the content itself may be regulated in relevant legislation. The regulation of content does not in our view fall within the existing purview of the Authority under the ECA.

2.24 **Question 24: How can ICASA be involved in offering of professional cybersecurity training to primary, secondary and tertiary institutions of learning?**

Telkom is concerned that ICASA may not be capacitated to attend to various training functions in addition to its existing mandates and would suggest that ICASA rather play a collaborative role in ensuring that other entities attend to training programmes.

2.25 **Question 25: Do you think ICASA should be involved in Cybersecurity standards, research and development and/or home-grown cybersecurity industry? If yes, please elaborate how on each of the above category**

Please see response to question 5 above. ICASA can play a role in research and development subject to adequate capacity.

2.26 **Question 26: How can Mobile operators partner with ICASA to teach children about safe Internet practices?**

Telkom is of the view that industry associations such as ISPA may be best placed to collaborate with ICASA in this regard. Such training and awareness may however lead to cost and capacity constraints on both ICASA and operators.

2.27 **Question 27: How can ICASA partner with tertiary institutions to help them provide accredited cybersecurity qualifications?**

Subject to capacity, expertise and funding, ICASA may contribute to content from a research and development point of view.

2.28 **Question 28: Is integrity as written in ECA equivalent to security? Please elaborate**

Please see response to question 4 above.

2.29 **Question 29: Do you agree with the proposed regulatory interventions?**

Telkom agrees with the Authority's consultation of industry in assessing the Authority's role in cybersecurity. We emphasise that an RIA is imperative should additional obligations be imposed on operators, to ensure these measures do not increase the cost to communicate.

2.30 **Question 30: What measures do licensees have in place to capacitate the consumer on issues of cybersecurity awareness?**

Telkom has sent communications to its customers regarding cybersecurity, including measures taken by Telkom to enhance the security of customers' Internet connections by updating their usernames and passwords and educating customers about Self Help Functionalities and cybersecurity. Telkom further distributed communications to customers on how to protect themselves from phishing and spam.

2.31 **Question 31: Should the Authority place requirements on licensees to capacitate and make consumers aware of cyber related threats? Please elaborate**

It is unclear how licensees must capacitate consumers in this regard. Additional obligations on licensees increase the regulatory cost of compliance and the cost to communicate.

2.32 **Question 32: What policy-making role should the Authority play with regards to Cybersecurity?**

Policy-making should reside with the Minister of the DOJ. This is to ensure that national policy is consistent.

2.33 **Question 33: What cybersecurity standards should the Authority require licensees to comply with?**

Cybersecurity and information security is a complex and involved field and the Authority should first conduct a regulatory impact assessment to assess the impact of further regulation, then publish draft regulations for comment by licensees.

2.34 **Question 34: Is self-regulation sufficient in the area of cybersecurity? How is this implemented? How is it monitored?**

This would require a study on which entities self-regulate and whether such self-regulation is successful. Cybersecurity issues occur on various communication network systems as well as end user devices and software. Each area should be considered on its merits to assess whether self-regulation is sufficient. Self-regulation can exist together with official regulation and legislation.

2.35 **Question 35: Are there any other issues that the Authority should be aware of in relation to ICT regulators and cybersecurity?**

No - please see content of submission.

END OF SUBMISSION