GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS

INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

NO. 521 **29 MARCH 2019**

FINDINGS DOCUMENT AND POSITION PAPER ON AN INQUIRY INTO THE ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY

1. The Independent Communications Authority of South Africa ("the Authority") gave notice of its intention to conduct an inquiry into the role and responsibilities of the Authority in Cybersecurity in terms of section 4B of the Independent Communications Authority of South Africa Act, 2000 (Act No. 13 of 2000) ("ICASA Act"), as indicated in a Discussion Document published in Government *Gazette* No. 41944 of 28 September 2018.

2. The Authority has since received responses to the said Discussion Document on 30 November 2018 and held public hearings from 17 to 18 January 2019.

3. The Authority hereby publish the attached notice regarding the conclusion of the inquiry into the role and responsibilities of the Authority in Cybersecurity in terms of sections 4C (6) of the ICASA Act.

Dr. Keabetswe Modimoeng

Acting Chairperson

Date: 28/03/2019

GENERAL NOTICE

NOTICE ___ OF 2019

INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

FINDINGS DOCUMENT AND POSITION PAPER ON AN INQUIRY INTO THE ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY

1. On 28 September 2018, the Independent Communications Authority of South Africa ("the Authority") published a notice in the Gazette[1] of its intention to conduct an inquiry into the role and responsibilities of the Authority in Cybersecurity in terms of section 4B of the Independent Communications Authority of South Africa Act no. 13 of 2000 ("ICASA Act").

2. The Authority published a Discussion Document in the Gazette[2] inviting interested parties to make written representation within 45 working days.

3. The Authority received thirteen (13) written submissions in relation to the Discussion Document, of which seven (7) indicated their intention to make oral submission. There was no request for confidentiality in terms of Section 4D of the ICASA Act from the submissions received.

4. The Authority held public hearings on the Discussion Document from 17 to 18 January 2019.

[1] Government Gazette No. 41944 of 28 September 2018.
[2] *Ibid.*

5. The Authority has concluded the inquiry into the role and responsibilities of the Authority in Cybersecurity.

6. In summary, this is what the Authority has found with regards to its role and responsibility in Cybersecurity the Authority's findings on its role and responsibility in Cybersecurity are briefly outlined below-

   6.1 There were conflicting views on the role of the Authority in cybersecurity.

   6.2 Section 2(q) of the Electronic Communications Act 36 of 2005 ("ECA") does not provide sufficient mandate to the regulation of Cybersecurity by the Authority.

   6.3 Submitters ignored addressing the role of the Authority in relation to network reliability and information security instead focused on their internal networks.

   6.4 The Authority should work in collaboration with other organisations who deal with Cybersecurity to not duplicate their efforts.

   6.5 The Authority to amend its existing regulations to include Cybersecurity matters.

7. A copy of the Authority's Findings Document into the role and responsibilities of ICASA in Cybersecurity which includes also the Authority's position on this matter is available on the Authority's website (www.icasa.org.za) and at the Authority's head office library (Block C, 350 Witch-Hazel Avenue, Eco Point Office Park Eco Park, Centurion) during office hours (Mon-Fri from 09:00 to 16:30).

Independent Communications Authority of South Africa
350 Witch-Hazel Avenue, Eco Point Office Park
Eco Park, Centurion.
Private Bag X10, Highveld Park 0169

FINDINGS DOCUMENT AND POSITION PAPER ON INQUIRY INTO THE ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY

MARCH 2019

Table of Contents

ACKNOWLEDGEMENTS

WE THANK THE FOLLOWING ORGANISATIONS WHO MADE SUBMISSIONS

1. Cell C
2. Department of Justice ("DOJ")
3. FNB Connect
4. Information Technology Association of South Africa ("ITA")
5. Internet Service Providers Association ("ISPA")
6. Media Monitoring Africa ("MMA")
7. Mobile Telephone Networks Proprietary Limited ("MTN")
8. National Association of Broadcasters("NAB")
9. Research ICT Africa
10. Sentech
11. South African Communications forum("SACF")
12. Telkom
13. Vodacom

GLOSSARY OF TERMS

DoC - Department of Communications

DOJC - Department of Justice Cluster

ECA – Electronic Communications Act

GDP - Gross domestic product

ICASA – Independent Communications Authority of South Africa

ICT - Information Communications Technology

IT – Information Technology

IoT – Internet of Things

ITS - Information Technology Security

NCPF – National Cybersecurity Policy Framework

NCS - National Cybersecurity Strategy

ISACA - Information Systems Audit and Control Association

ISO - International Standards Organisation

1. INTRODUCTION

1.1 THE PURPOSE OF THE FINDINGS AND POSITION PAPER

The purpose of this Findings Document and Position Paper is to reflect the findings the Authority assembled from the inquiry, held in terms of section 4(B) of the Independent Communications Authority of South Africa Act, 2000 (Act No.13 of 2000) ("ICASA Act"), read in conjunction with sections 2(n) and(q) of the Electronic Communications Act, 2005 (Act No. 36 of 2005) ("ECA"), and to communicate its position regarding the role and responsibilities of the Independent Communications Authority of South Africa ("the Authority" or "ICASA") in Cybersecurity.

2. THE PUBLIC PROCESS

2.1. During the drafting stage of the Discussion Document, the Authority had one-on-one meetings with different government stakeholders to discuss the Authority's views on the matter and to ascertain the different roles played by these stakeholders in the Cybersecurity space. The views of these stakeholders were considered during the drafting stage.

2.2. After the consultations with the above government stakeholders, the Authority published a Discussion Document titled "Inquiry into the Role and Responsibilities of Independent Communications Authority of South Africa in Cybersecurity" on 28 September 2018, the closing date for submissions was 30 November 2018.

2.3. The Discussion Document was structured in the form of questions supported by explanatory and contextual discussion. Questions posed were not necessarily all encompassing. The Authority invited stakeholders to respond to the questions posed and to make input on issues related to Cybersecurity.

2.4. The Authority received thirteen (13) written submissions, of which seven (7) indicated their intention to make oral submission. Oral hearings were held on the 17th and 18th of January 2019 at ICASA Offices in Centurion.

2.5. A summary of the views expressed by interested parties and stakeholders, in written and oral submissions, are reflected below. This summary is not exhaustive and is merely reflective of some of the important arguments raised during the inquiry.

2.6. As part of the research methodology, the Authority conducted a desktop international benchmark to see how Cybersecurity is implemented.

2.7. All the written and oral submissions, including the full transcripts of the hearings, are available at the Authority's library and the website for public inspection.

2.8. The positions herein are guided by the Findings of the inquiry.

2.9. This document consists of two major sections:

- **Section A** deals with background;
- **Section B** deals with submissions received in response to the discussion paper and the Authority's findings and positions.

3. Section A: BACKGROUND

3.1 ICTs have become an indispensable part of our daily life. Today, these technologies support national security, they ensure economic stability and enable social interaction within countries.

3.2 Interconnected networks have encouraged investment and facilitated new consumption models that have driven global economic growth. IT has become a key driver behind economic growth.[3] A panel study with 25 Organization for Economic Co-operation and Development (OECD) countries covering the period 1996–2007 was carried out to estimate various broadband impacts and reported that for every 10% increase in fixed broadband penetration, the GDP will increase by 3.9%.[4]

3.3 The benefits brought about by these technologies intrinsically originates with vulnerabilities and the risk of exploitation. Cybercrimes such as phishing, spam, computer-related fraud and other similar offences are rapidly increasing and evolving in step with the development and adoption of new ICT services.[5] Due to these facts, Cybersecurity is a growing global challenge.

3.4 The evolution of technology has resulted in access to the cyberspace, no longer being through a single medium, that is, the personal computer. Telecommunication devices and networks which previously operated for voice access only, have now evolved to comprise access to all Internet services. The evolution is not, necessarily, taking place in an unregulated environment however, telecommunication regulators have been existing to regulate the technical, economic and social uses of these services.

---

[3] Suffolk, J. 21st century technology and security – a difficult marriage.

[5] Draft Background Paper on Cybersecurity: The Role and Responsibilities of an Effective Regulator ("The draft background paper"). The draft background paper was commissioned by the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division and Regulatory and Market Environment Division. The draft background paper was prepared by Eric Lie, Rory Macmillan and Richard Keck of Macmillan Keck (Attorneys and Solicitors), for the 9th ITU Global Symposium for Regulators held in Beirut, Lebanon (10-12 November 2009). Available on http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

In this respect, the technology evolution in the telecommunication sector imposes a need for evolution on the role of the regulators.

3.5 The rapid adoption in developing countries of new ICT infrastructures such as the Internet is creating opportunities for these countries and its citizens to participate in the international flow of information, ideas, and commerce.[6] "More than 2 billion users send more than 88 quadrillion emails annually, and they register a new domain name with Internet Corporation for Assigning Names and Numbers every second of every day".[7] It should be noted that while the Internet comes with many advantages, it has also introduced a new challenge to South Africa's national security.

3.6 During the initial emergence of the Internet, safeguarding its security was less of a concern, but in recent years, the Internet has undergone exponential growth and protecting security of consumers, businesses and the Internet infrastructure is key.

3.7 Section 2(q) of the ECA enjoins the Authority with an obligation to ensure information security and network reliability. ***Information security*** is a subset of a broader Cybersecurity scope that deals with the protection, integrity, availability and confidentiality of data. ***Cybersecurity***, in the broader sense, deals with the protection of internet connected systems including hardware, software and data from cyber-attacks.[8]

3.8 Cybersecurity ensures that the public continues to enjoy the benefits that ICTs bring by managing the vulnerabilities and the risk of exploitation. Government, regulators, private sector organisations and individual users all have a responsibility to make efforts in creating a safe cyberspace.

---

[6] Madon, S. (2000). The Internet and Socio-economic development: Exploring the interaction. Information, Technology and People. 13(2), 85–101.

[7] Rosenzweig, P 2013, Cyber Warfare: How conflicts in Cyberspace are challenging America and changing the world, e-book, accessed 19 September 2018, p.201 < https://books.google.co.za/books?id=-xNb99V6WWkC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>.

[8] https://searchsecurity.techtarget.com/definition/cybersecurity.

3.9 As cyber threats grow, security policy, technology and procedures need to evolve even faster to stay ahead of the threats. However, it has been observed that Cybersecurity standards often lag the state-of-the-art and generally lag, to some degree, the state-of-the-practice. Advanced threats evolve and innovate daily whereas the Cybersecurity framework takes months, if not years, to gain consensus and to finally be implemented into law.

3.10 Studies show that Cybersecurity concerns cannot be resolved solely by market forces or by regulation but require a novel mix of solutions.[9] As a result, ICASA took a decision to conduct an inquiry to ascertain what role, if there is any, it can play to assuage Cybersecurity challenges faced by South Africa.

[9]Anderson, R. (2001). Why Information Security is Hard–An Economic Perspective. Retrieved October 18,2007, from http://www.acsac.org/2001/papers/110.pdf.

4. SECTION B: SUBMISSIONS

4.1 Overview

The Authority posed several questions regarding its roles and responsibilities in Cybersecurity. Thirty-five (35) questions were posed, however, these were: categorised in the following themes:

- Regulation of Cybersecurity.
    - Legislative framework
    - Definitions
    - Technical standards
    - Consumer Education/Awareness
- Research and Development;
- Private sector cooperation and industry regulation; and
- Capacity building.

Below are the responses from the respective stakeholders.

4.2 Regulation of Cybersecurity

The Discussion Document posed questions to the public to comment on the Authority's role in the regulation of Cybersecurity. The questions focused on the legislative framework and empowering provisions of the ICASA Act and the ECA for the Authority to regulate Cybersecurity. The questions included, defining Cybersecurity considering the available definitions, and whether the Authority may develop technical standards as a regulatory tool in Cybersecurity and lastly what role can the Authority play in consumer awareness.

4.3 Legislative Framework

4.3.1 Section 2(q) of the ECA entrusts the Authority with an obligation to ensure information security and network reliability. The inquiry on ICASA's role and responsibilities in Cybersecurity lies squarely in understanding

information security and network reliability and its position within Cybersecurity space.

4.3.2 Many of the submissions argue that the sections of the ECA alluded to by the Authority in the Discussion Document, namely sections 2(q) and 2(i) are insufficient and do not justify the Authority's perceived role in Cybersecurity. However, the submissions did not go further in alluding to how the Authority should approach its mandate in relation to sections 2(q) and 2(i) of the ECA.

4.3.3 MTN submits that ICASA should not contradict the primary legislation (i.e. the ECA) with the regulations it intends to introduce. MTN's position is that, currently ICASA does not have the required capacity to regulate Cybersecurity. MTN is of the view that the current legislation does not consider the implications of access to information and data protection laws.

4.3.4 MTN's view is that access to information and data protection laws are entrusted to the Information Regulator which is responsible for the implementation of the Protection of Personal Information Act ("POPIA") and not ICASA as the regulation of Cybersecurity is technologically neutral and as a result reduces the obligation from ICASA and any other institution not mandated to regulate online activities.

4.3.5 ISPA argued that there is a plethora of legislation dealing with Cybersecurity *albeit* at different angles and regulation of Cybersecurity is not within ICASA's jurisdiction. These include the Cybercrime Bill being led by the Department of Justice, POPIA Act led by the Information Regulator and online content which falls under the jurisdiction of the Film and Publications Board.

4.3.6 Vodacom and Cell C are also of the view that the Authority does not have mandate to regulate Cybersecurity nor the internet. Vodacom is concerned that by purporting to regulate Cybersecurity the Authority is over reaching its mandate. Whereas, Cell C submits that the Authority's mandate as set out in the ECA does not include regulation of Cybersecurity, and to do so would result in unnecessary duplication and

waste of resources as the function is not directly related to ICASA but is already catered for in the mandates of other regulators.

4.3.7 MMA, on the other hand, argues that there are several laws and incomplete policy processes such as the Cybercrimes and Cybersecurity Bill(B6-2017). Cybercrimes Bill was tabled in Parliament in November 2018 dealing with cybercrime such as spam, phishing, denial of service Cyber-fraud and identifies more offences to include hacking, unlawful interception of data and cyber extortion. In addition to this, the Cybercrime Bill identifies two major players in combating cyber-offences these are the SAPS and the National Prosecuting Authority.

4.3.8 The Bill left out issues dealing with cyber security and as a result, this has created uncertainty in the sector because South Africa's position in respect of Cybersecurity at the regional and international levels is still unclear.

4.3.9 MMA submits that the NCPF 2015[10] and the current and proposed regulatory framework does not appear to foreshadow a role for ICASA to play in the realm of Cybersecurity. Further, MMA cautions against exacerbating this through the addition of further laws and policies to carve out a role for ICASA that does not presently exist.

4.3.10 Telkom further states that Information Security 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, cyber fraud, cyberthreat related to the concept of Cybersecurity.

4.4 Defining Cybersecurity

4.4.1 Research has shown that there is no universal definition of cybersecurity. Many stakeholders provided a proposed definition for cybersecurity.

4.4.2 ITA submits that the current definition of Cybersecurity as defined by the NCPF is sufficient and that the Authority should not define this role as the role of Cybersecurity is spread across several government departments.

[10] Government Notice No. 609 in Government *Gazette* No. 39475 of 4 December 2015.

4.4.3 MTN suggests the following inclusions be made in the definition: Information Technology Security (ITS); Legal or Law Enforcement; National Security; and Economic Perspective. Cybersecurity or ITS are techniques of protecting computers, networks, programs and data from unauthorised access or attacks that are aimed at compromising the computer, network, program or data.

4.4.4 MTN further outlines the difference between Cybersecurity and information security by stating that Cybersecurity is defined as a preservation of confidentiality, integrity and availability of information in the cyberspace. Whilst information security protects information from unauthorised access to avoid identity theft and to protect privacy.

4.4.5 MTN suggests that the "cybersecurity" definition must include reference to content related offences, copyright related offences, any offence relating to computer forgery and fraud.

4.4.6 Telkom stated that Cybersecurity operates within a highly technical environment and is often included under a generic 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 information technology("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.

4.4.7 Telkom proposes that the term "Cybersecurity" ought to 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 IoT products and services and provide protection against cyber-attacks which may cause damage and or interference to such products and systems.

4.4.8 Whilst Cell C defines Cybersecurity as the practice of defending computers, networks and data from malicious attacks, measures taken to

protect a computer or computer system against unauthorised access or attack and the organization and collection of resources, processes used to protect cyberspace and cyber-enabled systems.

4.4.9 Sentech submits that Cybersecurity is a subset of information security and that the two (2) terms are not interchangeable. Sentech supports the view that Cybersecurity is concerned with information or things impacted by the vulnerability of electronic communications. Cybersecurity also considers processes, technologies and practices deployed to store, analyse, transmit and secure information, including other things such as appliances, cars, road management systems.

4.4.10. Sentech supports the adoption of the definition as stated in the NCPF.

4.4.11. In its submission Vodacom argues that should the Authority decide to define cybersecurity, this should be based on the Cisco definition which reads as the "practice of protecting systems, networks and programs from digital attacks". Furthermore, Vodacom argues that the Authority should not reinvent the wheel in trying to define the term "Cybersecurity", however they propose that the definition by Cisco is more practical.

4.4.12. With regards to information security Vodacom argues that Information Security is a crucial part of cybersecurity, but it refers exclusively to the processes designed for data security. Cybersecurity is a more general term that includes information security. Research ICT Africa proposes that in defining Cybersecurity two perspectives should be borne in mind; technological and organisational perspective. Technological perspective refers to technologies developed to safeguard computer systems and the information stored on such systems; whereas organisational perspectives implies the technical and non-technical measures taken by an organisation to ensure the availability, confidentiality and integrity in its computers.

4.4.13. NAB attest to the fact that advancements in technologies have brought with it challenges since consumers engage in online platforms to access media content. However, NAB did not provide a view on the definition of Cybersecurity but raised a concerned that in relation to cybersecurity, broadcasters are more concerned with signal piracy as this undermines the ability of broadcasters to sell their products to foreign markets.

4.5 Technical Standards

4.5.1 The Discussion Document requested stakeholders to provide their understanding of information security and network reliability and whether the two terms can be used interchangeably.

4.5.2 MMA argues that ICASA must not be seen to be involved in the monitoring and surveillance of users and/or operators that uses the information provided to ICASA by licensees. They further caution ICASA against risks that may be involved in setting the standards should the Authority decide to do so, this may ultimately render the networks more vulnerable to interference by setting standards that are known and can therefore be targeted and breached.

4.5.3 Cell C submits that network security in the context of the ICT sector and ICASA's mandate, is confined to redundancy and type approval. Cell C further argues that it is the licensee's responsibility to secure its network in the manner that it considers most appropriate and as such the Authority should not be involved in prescribing standards.

4.5.4 Further, Cell C is of the view that ICASA has misconstrued its mandate in relation to technology and network integrity; and the content of data messages. It argues that ICASA does not have a mandate to regulate technology at all, but only the manner in which licensees may deploy networks and services. The ICT sector in South Africa is technology-neutral, and ICASA's role is limited to type approval of specified equipment, as set out in Chapter 6 of the ECA.

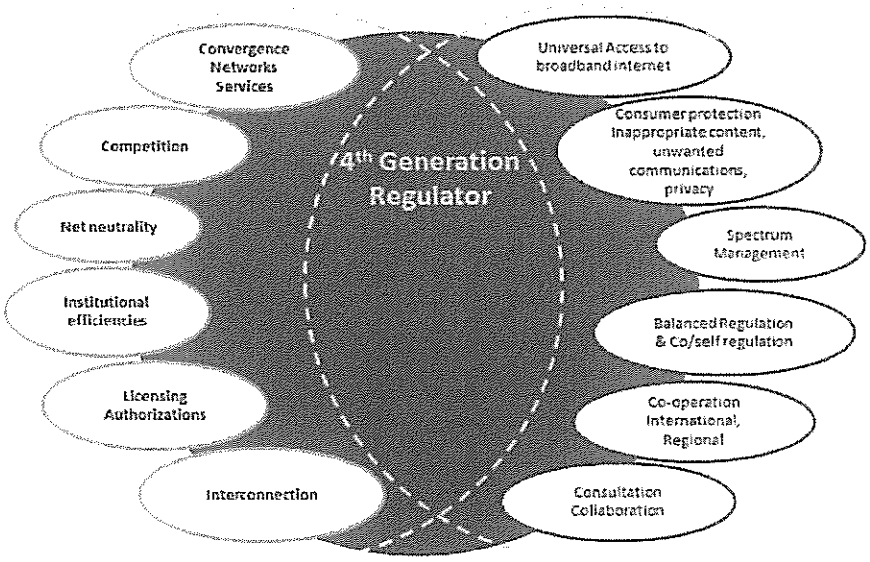
4.5.5 MTN submits that operators have already installed network security and integrity protocols which are in line with international best practices. MTN suggests that operators can partner with the Authority to define the minimum standards or requirements for network security and integrity standards.

4.5.6 MTN suggests that the implementation of proposed standards must not impair the use of computers and storage mechanism; and must not interrupt the services offered by operators to its customers; and must not place at risk the personal information of any customer.

4.5.7 Vodacom affirms its willingness to engage with the Authority on regulatory interventions in this regard. Vodacom will provide its views on specific regulatory interventions in the appropriate consultative processes.

4.5.8 Sentech agrees with the Authority that technology developments are evolving rapidly and as such regulators ought to adapt to this change. They attested to the fact that 4th Industrial Revolution brings opportunities for the sector and as a result, regulators need to adopt to this change and ought to become the *4th generation regulator*.

4.5.9 Sentech further states that the transformation creates a need for a 4th generation regulator whose task must be expanded beyond addressing traditional issues with regards to technology convergence and competition issues (inter-licensees and/or unlicensed operators). But also, to address socioeconomic issues of social growth, social inclusion, economic growth and social development as illustrated by the diagram below.



Source: ITU (adapted from Sentech's submission)

4.5.10. Telkom argues that should the Authority decide to develop the regulations on Cybersecurity standards, these should be subject to a

regulatory impact assessment to measure the impact of any proposed Cybersecurity measures on operators.

4.6 Consumer Education/Awareness

4.6.1 The Discussion Document requested stakeholders to comment on the extent to which the Authority should play a role in consumer education and outreach programmes.

4.6.2 SACF, MMA and Research ICT Africa state that the mandate of the Authority is to protect consumers. They further allude that the Authority should adopt a collaborative approach with other organisations in raising awareness with the threats pose by cyber space.

4.6.3 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, they are of the view that coordination role for Cybersecurity must reside with the National Cyber Security Advisory Council.

4.6.4 Vodacom argues that Cybersecurity awareness plays a crucial role in the creation of a Cybersecurity culture. If the Authority assumes a role in Cybersecurity awareness, it is important that:

- The Authority's role is in harmony with the NCPF;
- the Authority's objectives are clear;
- the Authority has the resources to perform the role well; and
- the role can be performed without compromising the Authority's ability to deliver on its core functions.

4.6.5 MTN supports the view that the Authority can play a role in consumer education and awareness in partnership with other entities. MTN suggests that ICASA must first develop awareness, skills and resources internally to manage Cybersecurity risk and advise the ICT industry.

4.6.6 Cell C is of the view that the Authority should not play any role in consumer education and awareness and argues that ICASA already has an extensive mandate and limited resources. Cell C suggests that the

Authority should liaise with the relevant entities who deal with Cybersecurity awareness programmes and publish their links on its website.

4.6.7 SACF argues that the role of ICASA in Cybersecurity is confined by the legislation. However, SACF argues that although ICASA's role is confined by legislation it is not precluded from playing a role *albeit* minimal. SACF further suggests that the role of ICASA should be that of consumer protection by hosting regular consumer awareness campaigns on topics related to cybersecurity.

4.6.8 MMA argues that building awareness and capacity on ICT-related matters that include, but extend beyond, cybersecurity, is an important and much-needed endeavour that ICASA may want to pursue further. However, MMA is of the view that given existing resource constraints, ICASA should be cautious about expanding its mandate until this is resolved.

4.7 The Authority's Finding and Position on the Regulation of cybersecurity

4.7.1 The Authority found that there are several legislative processes that are underway such as the Cybercrime and Critical Infrastructure Bills which relate to some aspects of Cybersecurity and might affect how this is dealt with in future. As a result, submitters propose that the Authority should await the completion of these processes prior to pronouncing on its role in the Cybersecurity space. Furthermore, the Authority cannot justify the application of sections 2(q), 36(1) and (2) of the ECA in ascertaining its role in Cybersecurity regulation.

4.7.2 In terms of section 2(q) most of the stakeholders disagree with the Authority's reliance on section 2(q), for its mandate regarding information security. However, most of those submissions (who disagree with the Authority's reliance on section 2(q)) focused on network reliability and not information security. The Authority is of the view that section2(q) of the ECA is sufficient enough and empowers the Authority to play a role in the Cybersecurity space.

4.7.3 It is further found that the transformation of technologies creates a need for a 4th generation regulator whose task can be expanded beyond addressing traditional issues regarding technology convergence and competition issues (inter-licensees and/or unlicensed operators).

4.7.4 There are several international standards already adopted by operators to protect their networks e.g. ISO27001; Cloud security Alliance, ISACA, etc. However, stakeholders expressed different views regarding whether the Authority ought to develop standards/guidelines/recommendations for Cybersecurity. On the one hand, stakeholders express that there needs to be collaborative approach in developing such standards and on the other hand, stakeholders are of the view that the Authority should not be involved in developing such standards for the industry since their standards are in line with the ITU general standards.

4.7.5 Cell C submits that there is no need for ICASA to develop standards as licensees are already committed to several international and domestic standards and requirements in relation to network security. However, ICASA may participate in research activities at the invitation of existing regulatory authorities or future authorities tasked with Cybersecurity and cybercrime.

4.7.6 Research ICT Africa argues that in fulfilling its mandate the Authority, as an implementation agent, should ensure that it not only protects information security and network integrity but also network reliability through setting technological standards which would protect the availability, confidentiality and integrity of IT equipment and networks.

4.8 The Authority's Position

4.8.1 The Authority's role regarding information security is provided by sections 2(q), 36 (1) and 36 (2) of the ECA and that based on the legislative framework, the Authority has a mandate in the Cybersecurity space even though it is only limited to network reliability and information security.

4.8.2 The Authority is aware of the state of different legislative framework relating to Cybersecurity in South Africa and it does not intend to duplicate the mandate of other entities dealing with the matter. However, the Authority is concerned with the public being safe on cyber space. It is

the view of the Authority that the legislation does not define information security as a result, this limit the Authority's role within cybersecurity.

4.8.3 In order to formulate a precise definition on cybersecurity, the Authority will be guided by the ITU and the completion of the country legislation around cybersecurity. The ITU defines Cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity
- Confidentiality

4.8.4 The Authority agrees with the stakeholders who argued that network security is more internally focused whilst Cybersecurity is external and looks at the conduct of consumers when engaging on the cyberspace.

4.8.5 With regards to setting standards, the Authority will facilitate collaboration with the DoC, DoJ and the industry to identify the most suitable standards for South Africa. These standards will be guided and informed by international standards as identified by the ITU and may include consumer protection issues such as giving consumer choice on whether location services should automatically be switched on, upon purchase of cell phone, etc.).

4.8.6 With regards to consumer protection, the Authority's view is that consumer protection is within the mandate of ICASA and that consumer awareness is important.

4.8.7 Through the Authority's Regional offices and consumer awareness and activations, the Authority will add Cybersecurity on its agenda. The Authority will also collaborate with the relevant entities and government departments who deal with Cybersecurity issues for purposes of collaboration and ensuring effective use of resources.

4.9 Research and Development

4.9.1 As technology continues to evolve rapidly, governments and regulators always lag. This challenge is due to both government and regulatory processes which take long to be completed. As a result, there is a time lag between policy and regulatory making in trying to catch up with technology and on the other hand Cybersecurity attackers are always a step ahead in infiltrating the security systems.

4.9.2 The Discussion Document requested stakeholders to comment if they think ICASA should be involved in research and development for home-grown Cybersecurity industry. These may be in policy and regulatory interventions including Cybersecurity standards.

4.9.3 MTN submits that the Authority has no power to formulate policy since this function rests with the legislature. However, the Authority, working with licensees, can make recommendations to the Cybersecurity policy.

4.9.4 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.

4.9.5 ISPA submits that the Authority should take its lead from the NCPF and forthcoming Cybersecurity legislation.

4.9.6 Research ICT submits that the Authority should facilitate an empirical, independent, and impartial Cybersecurity Maturity Assessment (CMA) in the country to identify the stage of maturity across several indicators related to Cybersecurity such as Cybersecurity policy and strategy; cyber culture and society; Cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organisations, and technologies.

Through the assessment it will be possible to identify specific points of policy intervention to effectively implement the National Cybersecurity Policy and the recently passed Cyber Crime Bill and Contribute to the drafting of a National Cybersecurity Strategy (NCS).

4.10 The Authority's Finding

4.10.1The Authority found that stakeholders were in support of it playing a role in research and development in collaboration with other entities.

4.10.2The Authority found that stakeholders are in support of the role it plays in consumer awareness and education, however, cautions the Authority to reassess its capacity.

4.11 The Authority's Position

4.11.1In adhering to section 2(i) of the ECA read with section 3(h) of the ICASA Act, it is therefore, the position of the Authority that it will participate in research and development within the ICT sector and partner with relevant institutions and government departments such as the National Departments of Communications and Justice, academic and research institutions.

4.11.2. Furthermore, from the research conducted the Authority will assume its advisory role to advise the relevant Minister of Communications as per section 4(1)(2)(a) of the ECA which empowers the Authority to make recommendations to the Minister on policy matters and amendments to ECA and its underlying statutes.

4.12 Private and Public-Sector Cooperation and Industry Regulation

4.12.1. The Discussion Document posed questions to the public to comment on the additional role that the Authority can play in Cybersecurity, considering the roles that are already being played by different stakeholders.

4.12.2. MTN suggests that ICASA should facilitate a multi-stakeholder engagement and cooperation on Cybersecurity matters and not take a lead in regulating Cybersecurity since this role is vested with the DoJC. In addition, MTN is of the view that the Authority can play a more active role

by leading and facilitating public awareness in respect of cyber-security. MTN suggests that the Authority should play an advisory role in incident management and promoting awareness.

4.12.3MMA submits a call for the establishment of an Interdepartmental Steering Committee (ISC) led by the Department of Justice on internet governance to address relevant matters, including cybersecurity. The objects should be broader than Cybersecurity alone, to reflect the broader internet governance mandate and the multi-disciplinary, cross-cutting challenges that these issues present.

4.12.4Further, MMA submits that ICASA should foster its role as a facilitator between public and private sector engagement. ICASA could arguably play a role in facilitating or participating in this coordinated effort, to the extent appropriate, with a view to ensuring that a holistic, streamlined approach is taken to matters of internet governance and ICTs, including cybersecurity. ICASA may also have a more active role to play in raising consumer awareness and digital literacy and protecting the rights of vulnerable users.

4.12.5Vodacom argues that although the collaboration between various governmental institutions and sectors will be of paramount importance to manage Cybersecurity related concerns, the Authority should guard against assuming functions and roles in relation to Cybersecurity which are being dealt with by other regulatory bodies.

4.13 The Authority's Findings

4.13.1The Authority found that there is a need to collaborate with public and private sector organisations and in collaborating with these organisations, the Authority may assume different levels of responsibilities in those collaborations.

4.14 The Authority's Position

4.14.1 The Authority will engage the relevant organisations dealing with Cybersecurity and continue to engage with the relevant regulators dealing with Cybersecurity to ensure that there is a clear demarcation of roles in relation to cybersecurity.

4.15 Capacity Building

4.15.1 The Discussion Document requested stakeholders to comment on ways in which ICASA can be involved in offering of professional Cybersecurity training to primary, secondary and tertiary institutions of learning. Moreover, whether the Authority can place requirements on licensees to capacitate and make consumers aware of cyber related threats.

4.15.2 MTN suggests that ICASA should not only assume the role of regulating Cybersecurity but it must first build capacity by advising the ICT industry on Cybersecurity and after it has accumulated the necessary skills it can then start regulating cybersecurity. Accordingly, MTN considers training as a more efficient way of capacity building.

4.15.3 MTN submits further that through engagement with NGOs and the private sector, ICASA can develop a pool of resources and experts to be utilised in its educational and awareness campaigns, because (according to MTN) ICASA does not possess the capacity and expertise to advise higher education. Furthermore, MTN cautions that ICASA must be mindful not to compartmentalise its resources as Cybersecurity incidents occur across all sectors and not only in the ICT sector.

4.15.4 Lastly, MTN affirmed its commitment to engage with the Authority and to participate in consumers' awareness programmes.

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

4.15.6 Telkom is of the view that industry associations such as ISPA may be best placed to collaborate with ICASA in this regard.

4.15.7 SACF is concerned with the perceived role of the Authority in capacity building and argues that ICASA may not be best placed to participate in Cybersecurity capacity building as the Authority is already resource constrained, financially and from a human resource perspective.

4.15.8 Vodacom submits its support for the Authority developing Cybersecurity competence and thought leadership as strategic skill for the future. The

Authority, according to Vodacom, needs to determine what skills are needed to contribute to Cybersecurity policy and accommodate this in its human resource plan.

4.15.9 Should the Authority assume a role of offering training, such role should be aligned to the NCPF, the Authority's objectives and resources to ensure that there is no compromise to the Authority's ability to deliver on its functions. Lastly, Vodacom does not believe the Authority has a mandate to place obligation on licensees to capacitate consumers of cyber related threats.

ISPA does not believe the Authority has the required expertise to perform the function of capacity building (providing training for primary education) in cybersecurity. The Authority must take a lead from the NCPF and forthcoming legislation.

4.15.10 Cell C submits that ICASA has a number of regulatory duties which it struggles to fulfil, partly because it claims to have limited resources. Licensees have no obligation to capacitate consumers regarding cybersecurity. Many of the other regulatory authorities are already dealing with this under existing and proposed legislation including the Cybercrimes Bill.

4.15.11 NAB agrees with Vodacom, Telkom and MMA that the Authority ought to adopt a collaborative approach and this should be shared between the Government and all other relevant players including the industry.

4.16 The Authority's Finding

4.16.1The Authority found that subject to capacity expertise and funding it may contribute to capacity building in the form of providing content from a research and development point of view.

4.17 The Authority's Position

4.17.1The Authority is of the view that citizens need to be educated on how to behave on cyberspace. The Authority will participate in capacity building

and partner with relevant institutions for Cybersecurity focused training such as Universities, Department of Education and Non-Governmental Organisations.

4.18. **4th Generation Regulator**

Sentech is of the view that the Authority needs to adapt to change by becoming the Fourth-Generation regulator. However, the Authority is of the view that based on the functions of "the 4th generation regulator", the Authority mandate covers most of the aspect raised in the diagram except for "Net-neutrality". Currently, the legislative framework is silent on "net-neutrality" and no policy framework has been developed to deal with this concept.

4.19. **Signal Piracy**

NAB raised a concern that broadcasters' challenge in relation to Cybersecurity is based on signal piracy but failed to expand on how Cybersecurity affect "on-line" or internet broadcasters. The authority is of the view that there needs to be a further engagement with the broadcasting industry in this regard.

5. CONCLUSION

5.1.1 The Authority would like to thank all participants for their input into this process. The Authority considered all submissions together with the current legislation and research conducted to produce the positions provided herein.

5.1.2 It is clear that regulating a safe Cyberspace is of public interest and such is the duty of the state and its agencies to ensure that South Africans are safe even on the cyberspace.

5.1.3 It is therefore the general position of the Authority that, Cybersecurity is a multi-facet concept and a multi-stakeholder approach and enabling legislation is required to clarify roles and avoid duplication of resources. The Authority will engage with relevant entities for the purposes of collaboration with regards to cybersecurity.

The Authority acknowledges and appreciates the current strides made by Government to understand and address cybersecurity.