INQUIRY INTO THE ROLES AND RESPONSIBILITIES OF ICASA IN RELATION TO CYBERSECURITY (*GAZETTE* 41944 OF 28 SEPTEMBER 2018)

Cell C Limited (Cell C) agrees with ICASA that cybersecurity is an important and necessary area for regulation. However, in our view, it is not an area that ICASA needs to become involved in, nor is it appropriate for ICASA to become involved here. Cell C has set out its response to this inquiry in the paragraphs that follow.

1. Introductory remarks

1.1 Paragraph 6.13 of the Inquiry Document states it is not ICASA's intention to duplicate any role resulting in possible resource waste, however ICASA aims to focus its strength where it is mandated by law. It is Cell C's considered view that ICASA's role as mandated in law, is to regulate the electronic communications, broadcasting and postal sectors and not to regulate cybersecurity, and that to do so would in fact result in unnecessary duplication and waste of resource.

1.2 Cell C is concerned that over many years ICASA has complained regularly about its lack of adequate funding in order to properly carry out its primary mandate as set out in the Electronic Communications Act, 2005 (ECA) and ICASA Act, 2000 (ICASA Act). ICASA is a creature of statute, initially anticipated in section 192 of the Constitution as an independent entity to regulate broadcasting in the public interest, which mandate was later extended to electronic communications and postal services. Its scope of authority, powers and duties are clearly prescribed as relating to the regulation of these sectors. It is inappropriate for ICASA to take on other functions that are not only not directly related to its functions, but that are already catered for by a plethora of other authorities. It would be wasteful of ICASA's already limited resources to extend itself into cybersecurity.

1.3 This is more so the case because ICASA has not fulfilled its mandate under these existing laws, because there are actions that remain outstanding and have been outstanding since 2006 when the ECA came into effect, and since 2014 when amendments were made to it. These actions include, among others:

a. A review and definition of "essential facilities" under section 43(7) of the ECA;
b. The definition and review of numerous so-called priority markets under section 67 of the ECA;
c. The approval and publication of reference interconnection offers under Chapter 7 of the ECA;

d. The publication of regulations regarding rapid deployment under Chapter 4 of the ECA;
e. The conclusion of regulations under section 4(3)(k) of the ICASA Act in relation to broad-based black economic empowerment as regards ownership of equity in licensees (despite 3 separate inquiries into ownership and control of various sectors), and the repeal of the Regulations regarding Ownership in Telecommunications;
f. The translation of the Minister's targets for universal service and universal access in each sector as set out in the Determination by the Minister of Communications (as it then was) in 2010;
g. The completion of a review of the broadband value chain which was carried out at significant cost but never completed;
h. The completion of the review of Sentech's role as signal distribution in South Africa, which was begun but never completed; and
i. The conclusion of numerous outstanding inquiries lodged with the CCC, a committee of the Council of ICASA.

1.4 Furthermore, ICASA has misconstrued its mandate in relation to technology and network integrity; and the content of data messages. It 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. As for content, the ECA specifically excludes content from the ambit of ICASA's functions in section 1 in the definitions of each of electronic communications, electronic communications services, electronic communications networks, electronic communications network services, and broadcasting. To date the only entity that has had power to deal with content in limited forms, is the Film and Publications Board (FPB), in terms of the Film and Publications Board Act, 1996.

1.5 At the time when ICASA published the Inquiry Document, the national law, then called the Cybercrimes and Cybersecurity Bill, had not yet been passed by Cabinet. However, on 28 November 2018, the National Assembly assented to this Bill, changing its name to Cybercrimes Bill. Cell C and other licensees made an extensive submission to the Department of Justice, which is the originating department for the Bill, on 10 August 2017. Not one licensee suggested that any of the functions within that Bill might be more properly situated within ICASA's mandate, because it is not appropriate to do so. All comments made on the Bill were made to the relevant Department.

1.6 In the ICASA Conclusion to the Inquiry Document, ICASA claims to be "well-positioned in terms of mandate, resources and experience to deal with current and emerging cybersecurity challenges". Cell C does not believe that the Inquiry Document or the facts can support this statement.

1.7 Finally, we also wish to note the number of competition problems that the broadcasting and electronic communications sector suffer from, which have been enumerated by Cell C to ICASA on countless occasions. The market is clearly skewed in favour of MTN Pty Ltd and Vodacom Pty Ltd, who together hold more than 80% of the total revenue market share in the electronic communications market. The HHI[1]of the sector has also been calculated at over 4,000 – when any HHI greater than 2,000 is indicative of significant market failure. ICASA has a mandate under section 2(f) the ECA, to promote competition in the sector. To this end, there are several useful interventions that ICASA could embark on that would improve competition in the electronic communications and broadcasting markets, with resulting benefits for consumers and industry, rather than extending itself into an area where there are already a number of initiatives and national agencies engaged in developing and implementing a national approach.

In the balance of this submission, we attempt to answer ICASA's specific questions, but these answers should be seen in the context of this general response.

2. Response to specific questions

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

No, for the reasons set out in paragraphs 1.4 and 1.5. Evolution of technology emphasizes the importance of "judgement-based" decision making around evolving cyber risk, based on the evolving threat landscape and sophistication of the cybercrime. In short, this means looking beyond compliance with the letter of regulation. There are many complex aspects to this. ICASA does not have the necessary expertise to regulate this area.

Question 2: How would you define cybersecurity?

We do not believe it is necessary to define this as the national law put to the National Assembly deals with the concept. For ICASA to attempt a separate definition would put it at odds with national law. In any event, we are not sure what the relevance of a definition is to the inquiry, since ICASA would have to amend primary law to include this within its mandate.

[1] The Herfindahl-Hirschman Index or HHI is a common measure of market concentration used to determine whether a market is competitive or not.

Question 3: are there any other laws that ICASA should consider in determining its role in relation to cybersecurity?

No. ICASA should not have such a role in our view, as set out in section 1 of this submission. ICASA correctly summarises the way in which this issue is dealt with in other laws. ICASA has not correctly captured the concept under either the ECA or ICASA Act, and it is not possible for ICASA to do so since neither Act refers to or implies that ICASA should extend its mandate to this area. It is patently clear from section 5 of the Inquiry Document that there are several entities already legally mandated to address cybersecurity.

Question 4: What is information security and network integrity and what is your understanding of ICASA's mandate in this regard? Is the mandate to secure network integrity and information security currently being fulfilled by ICASA?

Security controls have to be applied to ensure that data (information) is trustworthy, consistent and accurate according to predetermined network integrity objectives. Security controls have to be applied to ensure that data (information) is trustworthy, consistent and accurate. These matters do not fall within the mandate of ICASA.

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.

Please see the answer to question 4.

Question 6: Considering the role that are being played by different stakeholders, what additional role should the Authority play in cybersecurity?

For the reasons set out in paragraphs 1.2, 1.3 and 1.6, Cell C does not believe that ICASA has a role in the regulation of cybersecurity – this would tend to create unnecessary overlap and possible inconsistency and uncertainty, in addition to those concerns already discussed. However, as a stakeholder in the ICT industry, it would be appropriate for ICASA to attend any meetings of other regulatory bodies (such as those listed in the Inquiry Document), as part of its research mandate.

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

ICASA can request that information provided by cybersecurity regulators be distributed to ICT sector stakeholders.

Question 8: Should the Authority strive to follow the same approach [as South Korea]? What legislative powers are there to enable the Authority to implement this?

As set out in section 1 of this response, Cell C does not consider it appropriate or within ICASA's mandate to regulate any aspect of cybersecurity. There are multiple regulatory authorities already tasked with various aspects of this area. ICASA is a creature of statute – its founding statutes would have to be amended to create powers for it that it does not need. ICASA is correct to ask this question of itself.

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?

ICASA's mandate in relation to end users flows from section 69 of the ECA. It is very specific as to its general purpose, which is to deal with customer contracts and minimum standards for end user and subscriber charters, in accordance with the objects of the Act in section 2(m) and (n). When considered within the framework of the ECA in general, it is clear that ICASA's focus should be directed to matters that pertain to the use of electronic communications and broadcasting services and the relationship between the providers of these services and consumers. It would be entirely inappropriate to purport to now regulate the way in which consumers use those services through a charter that is intended to be applied to licensees, even if ICASA had the power to do so, which Cell C does not believe it has.

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?

The role of ICASA is limited by law. It is not ICASA's role to determine which of the multiple numbers of security software programmes are appropriate to implement in a business – this is not its competence. ICASA's competence lies in type approval and the regulation of radio frequency spectrum. For all the reasons set out in paragraphs 1.3 to 1.7 above, Cell C does not consider any such change to be appropriate, necessary or advisable.

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

No, as set out above; ICASA has a large scope of work already, and limited resources. There are other matters that require ICASA's attention. In addition, the area of cybersecurity is so broad that ICASA would have to in essence, become another type of regulator. The "threat landscape" in this area consists in Adversarial Threat, Accidental Threats, Environmental Threats (accidents, hacking, fraud); IT Theft, Terrorism, User Error, Espionage, Vandalism,

Organised Crime, System Theft, Identity Theft, Malware (for example there are over 230 000 new types of malware software launched per day). These matters are already dealt with by the Global State of Information Security protocols and organisations who are experts in these areas.

Question 12.1: 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?

Regulation of spam in South Africa was introduced by the Electronic Communications and Transactions Act, 2002 (ECTA) and bolstered by the Consumer Protection Act, 2008 (CPA) and the recently promulgated Protection of Personal Information Act, 2013 (POPIA). Industry bodies such as WASPA and ISPA have been addressing these matters for decades. There is no role for ICASA in this area. ICASA is not a content regulator.

Question 12.2: To what extent should the Authority play a role in consumer education and outreach programmes?

ICASA already has an extensive mandate and limited resources. If it were to play any role at all which we submit it should not, then if it were to make resources from the relevant parties available to consumers through a link on its website, that would be sufficient.

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?

No, for the reasons set out above. ICASA should not have any role in this area so requiring licensees to provide reports on these matters is not required.

Question 14: Should the Authority set similar standards for licensees to ensure that customers proprietary network information is protected from unauthorised disclosure?

No. That is neither ICASA's nor licensees' role. Users must adopt and maintain their own security measures and ICASA does not have any mandate in this regard, nor should it.

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

Network security in the context of the ICT sector and ICASA's mandate, is confined to redundancy and type approval. It is the licensee's responsibility to secure its network in the manner that it considers most appropriate. It is not in licensees' interests to operate a network that is not secure. Accordingly, all licensees already have IT departments that address these

operational issues. Licensees' choice of security options is entirely within their own competence.

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

These are operational matters that affect consumers and licensees to differing degrees. Network reliability is an obviously core part of every licensee's business. However, it is wrong to link these concepts together as if they are the same things or should be dealt with in the same way by the same regulator. Licensees have obligations to disclose consumer information to law enforcement under various laws. Network integrity is not about cybersecurity but redundancy and operational uptime, physical security of property, and privacy. Security in this sense is limited to maintaining a network that is safe to use. Licensees will have and do have obligations under other laws in relation to personal data, security, and cybersecurity. These are not ICASA's competencies nor within its mandate.

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

No. We have already dealt with ICASA's resourcing in section 1 of this response. ICASA should focus on its existing and large mandate and concentrate on fulfilling these functions.

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

ISPA has been at the forefront of self-regulation of internet service providers for decades. ISPs have committed to a code of practise in this regard, see https://ispa.org.za/press_releases/ispa-to-launch-cyber-security-code-in-south-africa/

Q19: Should the Authority require licensees to offer new and/or all customers 'family-friendly network-level filtering?'

No. This is available for free from the hardware and software manufacturing companies (e.g. Apple, K9 etc). See answer to Q13-16 and our introductory comments.

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?

Yes, they can assist but operators already do this as part of best practise in operating networks. This is not ICASA's role.

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

Yes, it is sufficient. It was drafted by the legislative arm of Government and enacted by Parliament after extensive consultation. It is not ICASA's role to enforce POPI. There are an adequate number of specialist regulatory authorities including those created under POPI without ICASA unnecessarily extending its sector-specific mandate.

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

No. This is not ICASA's role. There are already several regulatory bodies and law enforcement agencies committed to this task.

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

Again, this is not ICASA's role. ICASA should fulfil its current mandate.

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.

No, unless ICASA participates in research activities at the invitation of existing regulatory authorities or future authorities tasked with cybersecurity and cybercrime. Our submission explains ICASA's role and why it should not be extended. We do not understand why ICASA would seek to become involved in this way.

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

ICASA has a number of regulatory duties which it struggles to fulfil, partly because it claims to have limited resources. We have listed out some of the activities that ICASA has not undertaken or fulfilled, in section 1. Although there is nothing wrong with the concept of more education particularly in relation to children and the internet, this is misplaced in the circumstances. ICASA needs to focus on its existing functions.

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

See answer to question 26.

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

No. Network integrity concerns the uninterrupted performance of a network i.e. the constant quality provision of services over electronic communications facilities. It also concerns the integration of different facilities with one another.

Information regarding network performance is not provided to customers – it is the information that informs operators about network performance, capacity, traffic, and this all affects design and maintenance, upgrades of equipment and expansion. This is not the same as cybersecurity.

"integrity" is mentioned in section 2(t) of the ECA in relation to broadcasting and specifically the public broadcasting service. It is also mentioned in section 36(2)(a) in relation to the prescription by ICASA of "standards for the performance and operation of any equipment or electronic communications facility, including radio apparatus" which standards must be aimed at "…protecting the integrity of the electronic communications network". The context in which this is written is clearly not security-related but performance-related.

Question 29: Do you agree with the proposed regulatory interventions? Please elaborate.

No. Paragraph 8.1 of the Inquiry Document sets out a number of interventions that would significantly extend ICASA's mandate without justification. Industry members are already engaged in discussions with relevant bodies that are dedicated to cybersecurity and related matters and industry members are already subject to national laws in this regard. For ICASA to become involved as well would simply duplicate existing structures with the risks outlined above, such as inconsistency and unnecessary cost. This is undesirable in itself, but more so because ICASA has other duties that it should be focussing on to maximise its existing resources.

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

Licensees are already committed to several international and domestic standards and requirements in relation to network security. However, 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.

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

No. This is not ICASA's role and there are already numerous entities involved in this exercise.

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

ICASA has no role in relation to policy except to advise the relevant Minister (of Telecommunications and Postal Services, or Communications, as the case may be) about policy initiatives that may be required. The executive arm of government, through the relevant Minister, is the policy-maker. There is no need for ICASA to assume any such role. Its mandate is clearly spelt out in the ECA and ICASA Acts.

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

None, for all the reasons already set out.

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

If self-regulation were sufficient then it is doubtful that the legislature would have drafted a Bill in this regard. It is clearly a matter of national concern. However, it is not ICASA's role to deal with it. Many different national initiatives have been launched and are in progress, as ICASA has mentioned in the Inquiry Document.

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

No. ICASA has chosen a selection of regulatory authorities which are responsible for cybersecurity in other countries. However, not one of those authorities is a telecommunications sector-specific regulator. The reference by ICASA to the Dutch regulatory authority, OPTA, in paragraph 7.2 simply confirms that they have a role in relation to spam. However, spam is already dealt with in South Africa under the Electronic Communications and Transactions Act, 2002, and through WASPA and ISPA. Furthermore, paragraph 7.2.4 of the Inquiry Document purports, incorrectly, to link the Dutch regulatory position with a broader statement regarding spam being linked to cybersecurity. OPTA is not responsible for cybersecurity. This paragraph should not be included here as it misrepresents the position in this country.

The Nigerian example does not indicate that the Nigerian regulatory authority is responsible for cybersecurity; the Malaysian example misstates the position which is similar in South Africa where the Regulation of Interception of Communications and Provision of Communications-Related Information Act, 2008 (RICA) deals with interception and this is not ICASA's domain. It is also clear that the police are responsible for enforcement action in relation to cybercrimes.

The other examples provided only serve to illustrate that the national regulatory authorities for telecommunications in other countries have all adopted different approaches depending on their national approach to the regulation of cybersecurity. In the UK, the focus is on protecting children from accessing harmful online content, for example – in South Africa this is already dealt with by the FPB. This does not mean that ICASA should be tasked with this. Our regulatory history and legal framework for the sector have a different history.

ICASA has yet to fulfil many of its primary functions, rather than taking on yet more functions that are not core to its mandate, when there are already a number of national entities in South Africa that deal with cybersecurity and related matters.

Cell C requests an opportunity to present if ICASA decides to hold oral hearings.