queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

30 November 2018

ICASA
Attention: Ms. Violet Letsiri, Senior Manager: Social Policy for ICT services
VLetsiri@icasa.org.za

INQUIRY INTO THE ROLES AND RESPONSIBILITIES OF ICASA IN CYBERSECURITY

1. ISPA refers to the Discussion Document initiating an inquiry into the roles and responsibilities of the Authority in relation to cybersecurity and sets out below its submissions.

GENERAL SUBMISSIONS

The Authority's mandate

2. The Discussion Document references various sections of the ICASA Act and the Electronic Communications Act ("**the ECA**") as constituting a basis for it having a role and/or responsibilities to play in cybersecurity. These are provisions which empower the Authority to make regulations and are by their nature broad in scope. ISPA notes that:

   2.1. Cybersecurity is not directly related to convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors.

   2.2. Cybersecurity is not a function of the price, quality or the variety of electronic communications services.

   2.3. It is doubtful that provisions relating to type approval of physical electronic communications equipment set out in section 36 constitute a basis for intervention in cybersecurity.

3. ISPA does not believe that the Authority has a clear mandate at all in respect of cybersecurity.

The National Cybersecurity Policy Framework

4. We refer the Authority to the National Cybersecurity Policy Framework ("**NCPF**") as approved by Cabinet on 7 March 2012 and as canvassed in the Discussion Document.

5. ISPA submits that – in the absence of finalised cybersecurity legislation (currently under development) – the NCPF is the legally authoritative document in respect of cybersecurity matters in South Africa.

6. Section 16 of the NCPF sets out in some details the roles and responsibilities of the State regarding cybersecurity.

   6.1. The Department of Justice and Constitutional Development ("**DOJ&CD**") and the National Prosecuting Authority ("**NPA**") have an overall responsibility for facilitating cybercrime prosecution and court processes in accordance with the applicable laws.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

6.2. The Ministry of State Security and the State Security Agency ("**SSA**") has overall responsibility and accountability for coordination, development and implementation of Cybersecurity measures in the Republic as an integral part of its National Security mandate.

6.3. ISPA draws the attention of the Authority to the following specific provisions (our emphasis):

"16.2.1 The Ministry of State Security and SSA shall, amongst others, be required to perform the following key roles and responsibilities in relation to cybersecurity in the Republic:

……

(d) Have an overall responsibility for the development and formulation of National Cybersecurity in Republic and in consultation with stakeholders. This includes reviewing and amending existing Cybersecurity policies as well as prescribing regulations on information and communications technology security for the Republic in order to advance the National Security interests of the Republic.

(e) Provide information assurance and secure information and communications technology infrastructure of National importance in support of national security; This should include the development of State capacity to provide threat monitoring, alerting, co-ordination and response for information communications technology related incidents pertaining to National Critical Information Infrastructure of the State;

(f) Prescribe a regulatory framework for the control by the State of the provision and application of cryptographic solutions, development of National strategy and regulations for the protection of National Critical Information Infrastructure, and prescribe information communications technology security technical standards to which the electronic communications security products and services of organs of State must comply;

16.2.2 The implementation of these responsibilities by SSA shall include aspects of developing and implementing regulations, collecting intelligence both locally and internationally, conducting necessary Cybersecurity investigations and reporting on South Africa's Cybersecurity situation."

7. There is a single mention of ICASA in section 15 of the NCPF, which defines the role of the Authority in the following terms:

"15. Technical and Operational Standards Compliance

15.1 The NCPF also promotes:

a) The recognition of and compliance with appropriate international and local technical and operational Cybersecurity standards. The Minister of Communications shall enforce compliance

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

with such standards where appropriate and in consultation with the National Cybersecurity Advisory Council;

b) The continuous monitoring, review and assessment of regulatory frameworks that support Cybersecurity; and

c) The development and/or adoption of standards by the South African Bureau of Standards in consultation with relevant Government Departments, ICASA and industry. This will ensure a safe and secure cyberspace environment that will enable the growth of e-commerce and an inclusive information society."

8. This should provide authoritative guidance to the Authority on its roles and responsibilities relating to cybersecurity.
9. It should further be clear from the above and submissions below that the Authority should use inter-governmental mechanisms and consult widely with, *inter alia*, the Department of State Security and the Department of Justice and Correctional Services before attributing to itself roles and responsibilities relating to cybersecurity.

The state of cybersecurity legislation and frameworks in South Africa

10. As noted above, the Cybercrimes Bill [B6-2017] was adopted by the National Assembly on 27 November 2018.
11. It is important to note that – subsequent to the analysis of this Bill set out in the Discussion Document – a decision was taken by the Portfolio Committee for Justice and Correctional Services to remove the provisions of the Bill relating to cybersecurity and to rename the Bill from the "Cybercrimes and Cybersecurity Bill" to the "Cybercrimes Bill".
12. We are informed by the Department of Justice and Correctional Services that cybersecurity-specific legislation is under development. This legislation when finalised will determine the institutional structure that will be established to drive cybersecurity objectives and the roles and responsibilities of various role players.
13. We also note that the Critical Infrastructure Bill [B22-2017] is currently before the National Council of Provinces and that this will also determine certain cybersecurity structures, mechanisms and obligations.
14. ISPA has a relationship with the Virtual Cybersecurity Hub situated at the DTPS and has noted the various presentations made by the Hub in Parliament which indicate that it, by its own admission, is in a very early stage of establishing itself and functionality.
15. In the circumstances ISPA submits that it is premature for the Authority to be assessing its roles and responsibilities regarding cybersecurity.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

16. Note that the Cybercrimes Bill sets out the following in respect of "electronic communications service providers" – we ask that the Authority take particular note of the emphasised portion.

> ***"CHAPTER 8***
>
> ***REPORTING OBLIGATIONS AND CAPACITY BUILDING***
>
> ***Obligations of electronic communications service providers and financial institutions***
>
> *54. (1) An electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must—*
>
> *(a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and*
>
> *(b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.*
>
> *(2) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must by notice in the Gazette, prescribe—*
>
> *(a) the category or class of offences which must be reported to the South African Police Service in terms of subsection (1); and*
>
> *(b) the form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service.*
>
> *(3) An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000.*
>
> *(4) Subject to any other law, or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic service provider or financial institution to—*
>
> *(a) monitor the data which the electronic communications service provider or financial institution transmits or stores; or*
>
> *(b) actively seek facts or circumstances indicating any unlawful activity.*
>
> *(5) This Chapter does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989."*

ICASA's jurisdiction and the practicality of regulation of licensees

17. It is trite that ICASA only has jurisdiction over licensees but that cybersecurity measures are the responsibility of both licensees and non-licensees.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

18. ISPA requests that the Authority assess the impact of applying a specific regulatory regime regarding cybersecurity on licensees only and whether this will distort competition.
19. It is further the case that there is a wide diversity of considerations, standards and sets of best practise which will apply to the range of entities which hold service licensing under the ECA. Cybersecurity forms part of a different value and service-delivery chain and is of itself an incredibly broad and complex subject involving numerous linked role-players with overlapping responsibilities.
20. It will simply not be possible to apply sufficiently nuanced regulation to cover this diversity and that the Authority should not attempt to do so.

Cybersecurity in the ISP industry

21. Network security is an absolute fundamental for any ISP operating in South Africa or anywhere else. If an ISP cannot run a secure service, it will soon be out of business.
22. Security breaches have become big media items, creating reputational damage. In an industry which is as competitive as the ISP industry, this can lead to massive customer loss.
23. A substantial amount of the time and the resources of an ISP are spent on security. It is a critical business function and competitive issue.
24. ISPA has a Security Working Group – one of only three active working groups currently – which meets monthly to further cybersecurity and cybercrime related issues and objectives.
25. ISPA has formed an ISP industry CSIRT, which is open to non-members.
26. ISPA has constructive working relationships relating to cybersecurity and cybercrime with:
    - 26.1. The Department of Justice and Correctional Services;
    - 26.2. The Department of Communications (as announced by the President in the most recent restructuring of government departments);
    - 26.3. The Virtual Cybersecurity Hub;
    - 26.4. SAPS, including its cybercrimes resources;
    - 26.5. The Financial Intelligence Centre;
    - 26.6. The Film and Publication Board; and
    - 26.7. SABRIC.
27. ISPA has developed and delivered a training programme for SAPS officials which will be further rolled out during 2019. ISPA would be happy to extend the offer of such training to the Authority.

28. On 20 May 2009, ISPA was formally recognised by the Minister of Communications as an Industry Representative Body (IRB) in terms of section 71 of the Electronic Communications and Transactions Act (Act 25 of 2002). This recognition gives the members of ISPA special recognition and limited liability for Internet content.

29. In order to obtain this recognition and to maintain it from year to year, ISPA is required to ensure that:

    29.1. its members are subject to a code of conduct;

    29.2. membership is subject to adequate criteria;

    29.3. the code of conduct requires continued adherence to adequate standards of conduct; and

    29.4. the representative body is capable of monitoring and enforcing its code of conduct adequately.

30. The Minister has published Guidelines for the Recognition of Industry Representative Bodies under Chapter 12 of the Electronic Communications and Transactions Act which set out the standards with which a code of conduct of a representative body must comply. These include provisions relating to security and child online safety.

31. ISPA reports annually to the Minister in this regard.

32. ISPA's Code of Conduct is available from https://ispa.org.za/code-of-conduct/ and includes the following provisions relevant to this Inquiry:

    "***Cyber crime***

    18. ISPA members must take all reasonable measures to prevent unauthorised access to, interception of, or interference with any data on that member's network and under its control.

    H. Protection of minors and vulnerable persons

    19. ISPA members must take reasonable steps to ensure that they do not offer any paid services to minors without written permission from a parent or guardian.

    20. ISPA members must provide Internet access customers with information about procedures and software applications which can be used to assist in the control and monitoring of minors' access to Internet content. This requirement does not apply to corporate customers where no minors have Internet access.

    21. ISPA members must have processes in place to respond to directives issued by a court in terms of any applicable legislation, including but not limited to:

    - *the Protection from Harassment Act (No. 17 of 2011); and*
    - *the Maintenance Act (No. 99 of 1998)*

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

22. *ISPA members must have processes in place to ensure that they comply with the requirements set out for ISPs in the Films and Publications Act (No. 65 of 1996) as amended."*

33. In accordance with its recognition as an IRB, ISPA operates a take-down notice process on behalf of its members. This process allows for unlawful content hosted by ISPA's members to be reported, and, where necessary, acted upon. This process facilitates the removal of phishing and fraud sites from the South African Internet.

34. ISPA publishes information on take-down statistics in South Africa at https://ispa.org.za/tdn/statistics/.

35. General information on take-down notices and online forms are available from https://ispa.org.za/tdn/.

36. ISPA develops and distributes information on cybersecurity and cybersafety and requires its members to do so under the ISPA Code of Conduct. Resources available on https://ispa.org.za/safety/ include posters made available to schools and other public facilities and which are free to download, such as the below.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

37. ISPA has developed and is implementing the icode initiative - www.icode.org.za – which is an industry-driven initiative to identify infected machines, inform affected consumers that they may be at risk, provide support to enable those consumers to disinfect their machines, and reduce their risk of re-infection.

38. The objectives of the icode are:

    38.1. to instil a culture of cyber security within South African ISPs and their customers;

    38.2. to provide a consistent message in plain language to customers, in order to raise awareness of cyber security risks, educate users on steps that they can take to better protect themselves online, and to assist customers who may have infected machines;

    38.3. to encourage ISPs to identify compromised computers on their networks;

    38.4. to develop mechanisms for ISPs to share information and collaborate on cyber security concerns affecting South Africa ISPs; and

    38.5. to encourage ISPs to identify and report any cyber security issues that may affect South Africa's critical infrastructure or that may have a national security dimension.

39. The icode is voluntary for all South African ISPs and does not limit participation to members of ISPA. Non-ISPA members can participate fully in the icode. A trusted logo signifies to users that their ISP complies with the icode.

40. ISPA submits that the above indicates that industry takes security extremely seriously and is actively working with government and other stakeholders on cybersecurity and cybercrime issues.

The Authority should not be seeking to expand its mandate

41. In ISPA's view – taking into consideration the pressing demands to which the Authority is subject – the Authority should not involve itself in a matter which is, at best, tangential to its mandate.

42. As noted above, cybersecurity is a complex issue and we do not believe that the Authority has the expertise to enter into this arena.

RESPONSES TO QUESTIONS

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

As a matter of broad principle, the answer is self-evidently yes. This does not establish a case or basis for the involvement of the Authority on cybersecurity matters. ISPA notes that the desktop comparative research presented in the Discussion Document does not provide material support for regulators in other jurisdictions having the broad roles and responsibilities in cybersecurity proposed in the final section of the Discussion Document.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

Question 2: How would you define cybersecurity?

ISPA submits that defining this term is not within ICASA's jurisdiction and it should take its lead in this regard from the NCPF and forthcoming cybersecurity legislation.

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".

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

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

ISPA submits that defining these terms is not within ICASA's jurisdiction and it should take its lead in this regard from the NCPF and forthcoming cybersecurity legislation.

ISPA submits that the Authority has sought to achieve the objectives set out in section 2(q) through the End-User and Subscriber Service Charter Regulations (as amended).

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.

ISPA's understanding is that this section relates to certification of hardware to ensure that it can be safely operated, is compliant with technical standards and does not cause damage to electronic communications networks. It does not relate to cybersecurity.

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

In paragraph 6.13 of the Discussion Document it is noted that it is not the Authority's intention "to duplicate any role resulting in possible resource waste, however the Authority aims to focus its strength where it is mandated by the legislation". As noted above the Authority will be required to consult within Government before it can attribute roles and responsibilities relating to cybersecurity to itself.

The definition of these roles and responsibilities will be an output of cybersecurity legislation and the further activities of the Departments of State Security and Justice and Correctional Services.

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

The Authority could seek to engage with consumers on online safety issues when on its roadshows and other activities.

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?

ISPA refers the Authority to its submissions relating to its icode initiative set out above.

ISPA does not support the Authority being involved in such activities or that it is within its mandate or jurisdiction to do so.

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?

ISPA refers to its previous response.

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?

Absolutely not. ISPA does not believe that there is a need for such forms of regulation as the market will soon expose such a service provider. Further, if such a need was established, we do not believe the Authority would be the correct entity to implement and enforce such a measure.

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

No. Internet regulation is the province, currently, of the Film and Publication Board.

The Authority is a communications regulator. Not a content regulator.

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?

ISPA does not see a role for the Authority in this regard and refers the Authority to the Consumer Protection Act and POPI as well as the National Consumer Commission and the Information Regulator.

ISPA has a long history of fighting spam in South Africa as this is an important issue for ISPs. Resources are available at https://ispa.org.za/spam/.

Question 12(2): To what extent should the Authority play a role in consumer education and outreach programmes?

The Authority should include online safety as a topic.

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?

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

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

This falls under POPI and the jurisdiction of the Information Regulator.

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

ISPA submits that defining this term is not within ICASA's jurisdiction and it should take its lead in this regard from the NCPF and forthcoming cybersecurity legislation. For reasons set out above, ISPA does not support the Authority playing a role in this regard.

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

ISPA submits that defining these terms and the relationship between them is not within ICASA's jurisdiction and it should take its lead in this regard from the NCPF and forthcoming cybersecurity legislation.

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

ISPA does not support the Authority having such functions or that there is a basis for this in the NCPF.

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

See submissions above on cybersecurity in the ISP industry.

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

The Authority is a communications regulator: not a content regulator. This falls within the mandate and jurisdiction of the Film and Publication Board and is being specifically investigated by the South African Law Reform Commission as part of its Project 107.

[No questions 20,21]

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 legislation developed over many years specifically addressing the protection of personal information and it is to be hoped that it is sufficient for this purpose. Given that POPI is not yet in force it is difficult to make any firm assessment in this regard.

Licensees – like everyone else – will be subject to POPI when it comes into force. It is the role of the Information Regulator, not ICASA, to enforce compliance with POPI.

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

Note that personal information is content and ISPA does not hold the view that the Authority holds jurisdiction over content.

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

This is more properly and explicitly the role and mandate of the Film and Publication Board under the Films and Publications Act of 1996 as amended.

As notes above, ICASA should involve itself through including this issue in its community outreach programmes.

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

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

ISPA refers the Authority to subsection 55(1) of the Cybercrimes Bill as adopted by the National Assembly on 27 November 2018:

> ***"Capacity to detect, prevent and investigate cybercrimes***
>
> *55. (1) The Cabinet member responsible for policing must—*
>
> *(a) establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes;*
>
> *(b) ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes; and*
>
> *(c) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the South African Police Service primarily involved with the detection, prevention and investigation of cybercrimes.*
>
> *36 (2) The Cabinet Member responsible for policing may make regulations to further regulate any aspect referred to in subsection (1)."*

ISPA does not believe that the Authority has the required expertise to perform this function.

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

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

queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

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

ISPA does not represent mobile operators *per se*.

CONCLUSION

43. We trust that this above is of assistance to the Authority in its further deliberations.

Regards

ISPA REGULATORY ADVISORS