INQUIRY INTO THE ROLES AND RESPONSIBILITIES OF THE IDEPENDANT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY.

FEEDBACK – FNB CONNECT

1) ***Does the evolution of technologies necessitate the regulatory function evolution of the Authority? Elaborate.***
   Yes. With the evolution of technologies, new barriers of entry, and threats tend to surface and without the evolution of the authority, governance and regulation cannot be depended upon in the interest of national safety Question 2: How would you define cybersecurity?

2) ***How would you define cybersecurity?***

   It the secure protection of a user or an organisation from threats arising from cyber activities.

3) ***Are there any other laws that the Authority should consider in determining its role with regard to Cybersecurity?***.
   Yes. RICA and FICA. Currently, there is a mis-alignment between RICA and FICA with regard to Customer verification. However, FICA offers greater protection than RICA on the basis that FICA uses stronger measures than RICA.

4.1) ***Section 2(q) of the ECA provides that one of the objects of the ECA is to "ensure information security and network reliability. What is information security and network integrity and what is your understanding of the Authority's mandate in this regard?***
Information Security and network integrity looks at the protection of information and the necessary steps that an organisation takes to secure information and to provide a reliable and integral network. The Authority should provide guidance on the minimal

measures to be put into place a secure network infrastructure. The Authority’s current role should be expanded to touch on infrastructure as well as information security.

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

No. The Authority currently has limited focus in terms of network breaches. Organisations are unable to engage with Authority on details support and guidance. To date we have not seen active involvement by the Authority in managing network integrity and info security.

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.***

36(2) of the ECA. Organisations need to confirm to the stipulated standards as per Section 36(2). Our understanding is that each organisation must maintain a set of standards Irrespective of the standard set by the authority an organisation must conform to Section 36(2).

6) ***Taking into account the roles that are being played by different stakeholders; what additional role should the Authority play in Cybersecurity?***

The Authority should have the powers to enforce penalties and provide guidance on what measures need to be undertaken by any organisation should any breach in security take place.

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

Need to run necessary public and industry awareness campaigns and host a cite whereby all organisations are made aware of current and latest threats that the country and the world is being exposed to. Remedial measures should be provided to rectify the threats and breaches that may occur. The authority should be actively involved with National Intelligence Agency and Military Intelligence Agency.

8) ***Should the Authority strive to follow the same approach? What***

legislative powers are there to enable the Authority to implement this?

Yes. RICA.

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?***

No. It would limit user's rights

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?***

Yes. Should the business provide software to the market and it is unsupported national beaches ma y occur to high degrees which breaches cannot be rectified.

11) ***Should the mandate of the Authority be extended to software and internet regulation?***

Yes with limited scope so that the market is still regulated but has the freedom to operate accordingly.

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?***

There is no single governing body managing or regulating spam in the entire ICT industry however there are controlled institutions such as WASPA and ISPA. The authority should be the centralised controlling body for all spam related bearers.

12) ***To what extent should the Authority play a role in consumer education and outreach programmes?***

They must exercise a majority role. Further they must play an active role on social media platforms and follow a similar approach to SABRIC.

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?***

Yes. The greater viability of the reports helps reduce end user frustration and negates churn In the industry. The advantage of such out rep helps identify trends in problematic environments thus enabling entities to adopt suitable solutions.

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

Yes.

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

Network security refers to the safety and protection of network equipment and prevention of associated breaches. The Authority must have advanced tools such as NIA and MIA to infiltrate and intercept communications on networks. The Authority should have set minimum standards.

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

Network reliability and integrity speaks to the stability of the network. Information security makes ref to the data content that traverses across the network.

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

The Authority should adopt the mode of ops as SIDIC. Resourcing can be done by key entities contributing to a common platform. The platform that the Authority can adopt can be an open access solution whereby various industry champions participate and contribute resources and technical solutions.

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

There are no known cybersecurity measures in place to protect consumers. The Authority should ensure that measures are in place to protect consumers. Penalties and obligations should be imposed for non-compliance on ISP's.

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

Yes. The offering should give customers opportunity to select or discard the filtering solution without any costs incurred.

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. Centralised body will be instrumental and should be licenced to offer this. Use of algorithms and incorporate artificial intelligence coupled with large data lakes and remedial measures. The Authority can establish a forum to initiate a forum and steering committee with industry champions that will drive the agenda forward.

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

Yes. ICASA can introduce more awareness campaigns on POPIA and they can constantly remind the ICT sector of the minimal threshold requirements. Enforcement cannot be done by ICASA but they can promote the Act and its requirements through awareness campaigns.

23) ***Should ICASA be involved with Online Child Protection? If so, how?***

Yes. When child has access to online. Then second when a child goes missing, then can utilise ICASA's services for tracing purposes. Measures can be put in place in order to police this.

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

Roadshows, communications, awareness campaigns. ICT staff at Department of Education can be trained.

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***

Yes. ICASA can take learnings from other countries by developing a framework on international standard based on deployment internationally. A centre of Excellence should be developed focusing on potential threats and heave simulated attacks on industries.

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

They can introduce zero rated APN's so that the targeted content can be easily accessed by children. ICASA can create a portal for information dissemination.

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

ICASA can contribute or sponsor programmes with tertiary institutions to provide these qualifications. Also appoint representatives to attend open days at universities to provide students/prospective students with information on cybersecurity qualifications. ICASA can also assist institutions by providing access to latest frameworks and standards as applied internationally.

28) ***Is integrity as written in ECA equivalent to security? Please elaborate***

Integrity is the quality of the network infrastructure and security refers to the safety and protection of the data traversing the infrastructure.

29) ***Do you agree with the proposed regulatory interventions? Please elaborate***

No. The proposed regulation relates mainly to the promotion of frameworks and standards however it does not detail action plans for implementation and guidelines for remediation of cybersecurity threats.

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

There are currently no measures in place pertaining specifically to cybersecurity awareness.

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

Yes. They should make it compulsory for licensees to raise awareness on a regular and minimum basis thus enabling the Authority to monitor and track the licensee’s ability and efficiency of consumer awareness.

32) ***What policy-making role should the Authority play with regards***

to Cybersecurity?

The role of the authority should be that of enforcement. The role should also include the setting of standards, governance and framework.

33) ***What cybersecurity standards should the Authority require licensees to comply with?***

These standards cannot be explicitly contained. The standards need to be defined with regard to a structured framework, hence to enforce licensees to comply, the framework and standards must be defined.

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

No. There needs to be a Regulatory Body that facilitates the implementation of cybersecurity controls. Regular audits can be implemented to determine the effectiveness and efficiency of the implemented cybersecurity defence measures.

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

The Authority needs to fully encompass and embrace GDPR . Stricter penalties for non-compliance and non-compliant Regulators need to be identified on a specific forum.