SACF Comments: Inquiry into the Roles and Responsibilities of ICASA in CYBERSECURITY Regulation - DISCUSSION DOCUMENT

Submitted: 30 November 2018

SACF COMMENTS ON THE DRAFT ELECTRONIC COMMUNICATIONS AMENDMENT BILL

INTRODUCTION

1. The SACF is an industry association that represents a diverse group of members that participate throughout the ICT value chain and are therefore in a unique position, to bring considerable insights through the experience of our members – small and large across the ICT value chain.

2. The SACF welcomes the opportunity to comment on the section 4B Inquiry into in the Role of the Authority in respect of Cybersecurity.

3. Our submission is limited to three key themes, which we trust will contribute to ICASA's discussion in respect of its role on Cybersecurity.

4. The SACF would like to participate in oral hearings on the Cybersecurity Discussion Document, should there be any.

ROLE OF ICASA IN CYBERSECURITY

5. It is laudable that ICASA, has initiated an inquiry into cybersecurity given its growing importance as consumers are increasingly connected.

6. ICASA is a creature of statue and therefore derives its powers and mandate from legislation.

7. Therefore, ICASA's powers a confined to what has been prescribed in the applicable legislative framework.

8. ICASA draws its mandate from the Electronic Communications Act (ECA), Independent Communications Authority of South Africa (ICASA) Act and the Electronic Communications and Transactions Act (ECTA) from which ICASA draws its mandate.

9. On our reading none of the above legislation empowers ICASA to regulate licensees in respect of Cybersecurity.

10. Instead, the Cybersecurity and Cybercrimes Bill, provides for the role of regulating Cybersecurity to the Cybersecurity Hub which falls within the Department of Telecommunications and Postal Services (DTPS).

11. As long as ICASA has no legislated powers in respect of Cybersecurity, we are of the view, it cannot impose obligations or regulate on Cybersecurity.

12. However, that does not mean that ICASA has no role to play in respect of Cybersecurity.

13. A key area of ICASA's mandate is consumer protection, therefore, in our view the absence of a legislative mandate does not preclude ICASA from running regular consumer awareness campaigns on topics related to Cybersecurity.

RELATIONSHIPS WITH OTHER REGULATORS

14. We note ICASA's questions in respect of the implementation of POPI.

15. The Information Regulator has primary jurisdiction over the POPI Act.

16. The Cybersecurity Hub through the Cybercrimes and Cybersecurity Bill has primary jurisdiction in terms of Cybersecurity.

17. However, we are of the view that while, the Authority does not have primary jurisdiction in respect of Cybersecurity or in respect of POPI.

18. We are of the view that these relationships should be no different than that between ICASA and the Competition Commission. Accordingly, we would encourage ICASA to conclude a Memorandum of Understanding (MOU) with the Information Regulator and the Cyber Hub.

POLICY-MAKING ROLE

19. In the Discussion Document, ICASA poses a question as to whether it has a role in respect of policy making in respect of Cybersecurity.

20. Until the early nineties, the Minister or political head was responsible for setting policy, making regulations and being the operator of the state monopoly – a practice that was noted globally. Prices were not necessarily lower, service was less than ideal, and services were not ubiquitous. During the 90s because of global best practice most countries including South Africa embarked on processes which culminated in the separation of powers. The political head was responsible for policy, independent regulators were created, and the incumbent monopolist became an independent operator. Competition was introduced. Although, in South Africa, the State continues to hold a stake in more than one licensee and the Ministry of Telecommunications and Postal Services is the shareholder representative in Telkom and Broadband Infraco as examples.

21. The purpose of the separation of powers was that the political heads would determine policy which is underpinned or aligned to a specific political agenda. The need for an independent regulator with the ability to independently consider and accept or reject policy directions, is to maintain fairness. However, this is not absolute as regulation does not operate outside of overall national policy and legislative framework. Once the overarching policy has been set, the execution of regulations and licensing ought to be done independently and objectively.

22. It is important to note that the regulator's powers are confined to that which is bestowed upon it in law.

23. The responsibility and role of policy making lies with the relevant line Ministry. Therefore, we are of the view that ICASA has no legislative powers or mandate to make policy, including policy on Cybersecurity.

CAPACITY BUILDING

24. We laud ICASA for recognizing the growing importance of Cybersecurity and as a key growth area for the future of work and its intent to play a role in developing critical skills.

25. Despite, ICASA's noble intention to participate in capacity building towards developing cybersecurity skills, we are of the view that ICASA may not be best placed to participate in Cybersecurity capacity building.

26. As we understand it, ICASA is already resource constrained, financially and from a human resource perspective, as gleaned from ICASA's various submissions advocating for a self-funded model to alleviate its resource constraints.

27. We further understand that ICASA's budgetary allocation was reduced during the current financial year.

CONCLUSION

28. We would again like to thank ICASA for the opportunity to submit comments.

29. We would like to reiterate our views that ICASA does not have primary jurisdiction over cybersecurity and the protection of personal information. However, it does have a secondary role to play and more directly to cybersecurity in its ongoing awareness campaigns.