



Independent Communications Authority of South Africa
350 Witch-Hazel Avenue
Eco Point Office Park,
Eco Park, Centurion.

By email: VLetsiri@icasa.org.za

30 November 2018

Dear Ms Violet Letsiri,

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 (ICASA) published a notice inviting comments on the inquiry on its role and responsibilities in cybersecurity. Interested persons were given until 30 November 2018 to submit their written input.
2. The National Association of Broadcasters (NAB) is a leading representative of South Africa's broadcasting industry, representing the interests of all three tiers of broadcasters. Our members include the public broadcaster, commercial radio media groups; Primedia, Kagiso Media, Tsiya Group, AME, MSG Afrika, as well as independents, Classic FM, Kaya FM, YFM, Smile FM, and LM Radio; all the licensed commercial television broadcasters e.tv, Multichoice, M-Net, and StarSat-ODM; a host of community radio broadcasters and community television broadcaster, Faith

Postal Address: P.O.Box 412363, Craighall, 2024, South Africa

Tel: +27(11) 326 2444 | **Fax:** +27(11) 326 3086

info@nabsa.co.za | www.nab.org.za

The NAB is a voluntary industry association funded by its members





Terrestrial. The NAB membership also extends to training institute, NEMISA and the broadcast signal distributors, Sentech and Orbicom.

Background context

3. It is the NAB's understanding that this inquiry is conducted pursuant to section 4B of the ICASA Act 13 of 2000, as amended. It is the NAB's further understanding that the objective of this inquiry is to solicit views and information that will assist with determining the role that ICASA ought to play in relation to matters pertaining to cybersecurity within the ambit of ICASA's enabling legislation, namely the ICASA Act and the Electronic Communications Act 36 2005, as amended.
4. Rapid advancements in technology have presented the broadcasting industry with new opportunities for growth and development mainly through new distribution platforms. These developments have also necessitated a review of the current legislative and policy framework to ensure regulatory certainty whilst also creating an enabling policy environment for the development of the broadcasting industry. To this end we are encouraged that ICASA and the Department of Communications have begun the process of developing a policy framework for digital sound broadcasting. The NAB also notes the efforts made towards completing the digital migration process.
5. Unfortunately, advancements in technology have not been without their drawbacks. As consumers begin to increasingly engage online and access media content through online platforms, cybersecurity has become central to ensuring a secure online environment, both in the interests of the consumer and media content distributors.



Cybersecurity threats facing the broadcasting industry

6. Currently, one of the biggest cybersecurity threats facing the broadcasting industry is signal piracy. Signal piracy can take a physical form through the unauthorised recording of broadcasts on video tapes, DVDs or USB sticks. Signal piracy can also be virtual through the unauthorised redistribution of signals over the air or online, and also through hacking into encrypted pay TV signals using equipment which is specially designed to circumvent the security measures which are built into set top boxes.¹
7. Signal piracy is a grave concern as it undermines the ability of broadcasters, including the public broadcaster to sell their local content in foreign markets, particularly where viewers in those foreign markets already have illegal access to the media content. Revenue generated by broadcasters is directly proportionate to their ability to invest in content development, and broadcasters also make significant investments in order to acquire exclusive rights over content and the broadcasting of sporting events. Consequently, the financial losses incurred as a result of signal piracy impede broadcasters from investing further in the acquisition, production and transmission of diverse local content.
8. South Africa has also grappled with signal piracy and this was brought to the fore in 2011 in the matter between a broadcaster and a signal distributor, where the broadcaster sought a court order directing the signal distributor to change its signal encryption system after it had been intercepted. As cited in the case, signal piracy also results in a significant loss of advertising revenue.

¹<http://www.wipo.int/pressroom/en/briefs/broadcasting.html>



Recommendations

9. The inquiry document highlights some of the approaches which have been adopted in various countries. Notably, a majority of the cited countries have highlighted the increasing importance of consumer education and awareness, as well as capacity building which is the shared responsibility of both government and the industry. The NAB submits that ICASA must encourage licensed entities to promote cyber safety through their respective public education campaigns.

10. Cybersecurity challenges will continue to evolve as technology continues to develop. Therefore, in order to effectively promote cybersecurity, the NAB submits that a co-ordinated approach across various government departments, including law enforcement is essential. Offences relating to cybercrimes often transcend national borders which requires coordination with other law enforcement and regulatory agencies in foreign jurisdictions.

11. The NAB notes that although the international rules and consequently, the national legislative provisions, have not been adequately updated to address these emerging challenges, the World Intellectual Property Organisation through its Standing Committee on Copyright and Related Rights has begun working towards developing an international treaty in response to these concerns. We trust that such international conventions will be implemented through national legislation, once they have been finalised and ratified, guided by the constitutional principles of freedom of expression and access to information. Furthermore, these international instruments will serve as guidance on *inter alia* the technical considerations and standards to be adopted.



Conclusion

12. In conclusion, the NAB thanks ICASA for the opportunity to make this submission and we look forward to further engagements.

Yours sincerely,

A handwritten signature in black ink, consisting of several overlapping, fluid strokes that form a cursive name.

Nadia Bulbulia
Executive Director

