PO Box 1560, Parklands, 2121 • Tel +2711 788 1278 • Fax +2711 788 1289
Email info@mma.org.za • www.mediamonitoringafrica.org
Promoting human rights and democracy through the media since 1993

30 November 2018

TO: **Ms Violet Letsiri**
Senior Manager: Social Policy For ICT Services
Independent Communications Authority of South Africa
By Email: VLetsiri@icasa.org.za

INQUIRY INTO THE ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY: SUBMISSIONS BY MEDIA MONITORING AFRICA ON THE DISCUSSION DOCUMENT

For more information, please contact:

WILLIAM BIRD, Director of MMA
E-mail: williamb@mma.org.za
Tel: +2711 788 1278

THANDI SMITH, Head of Policy Programme
Email: thandis@mma.org.za
Tel: +2711 788 1278

MMA was assisted in the drafting of these written submissions by ALT Advisory:
https://altadvisory.africa

CONTENTS

LIST OF ACRONYMS

CCB	Cybercrimes and Cybersecurity Bill
DoC	Department of Communications
DTPS	Department of Telecommunications and Postal Services
ECA	Electronic Communications Act 36 of 2005
ECTA	Electronic Communication and Transactions Act 25 of 2002
FPAB	Films and Publications Amendment Bill
ICASA	Independent Communications Authority of South Africa
ICTs	Information and communications technologies
ISC	Inter-departmental Steering Committee
MMA	Media Monitoring Africa
MTEF	Medium-Term Expenditure Framework
PCJCS	Portfolio Committee on Justice and Correctional Services
POPIA	Protection of Personal Information Act 4 of 2014
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

INTRODUCTION

1. Media Monitoring Africa[1] (MMA) welcomes the opportunity to provide written submissions to the Independent Communications Authority of South Africa (ICASA) on the discussion document regarding the roles and responsibilities of ICASA in cybersecurity (the Discussion Document). MMA would also welcome the opportunity to present further oral submissions at the appropriate time as this inquiry continues.

2. MMA strives towards an internet that is both safe and open for all users. However, MMA has certain concerns with ICASA expanding its role into the realm of cybersecurity, given existing challenges, the level of regulatory uncertainty, and the intended functions of ICASA as set out in section 4 of the ICASA Act 13 of 2000. Accordingly, this submission is structured as follows:

    2.1. First, an overview of MMA and our work on cybersecurity;
    2.2. Second, the issue of resource constraints of ICASA;
    2.3. Third, the existing legislative landscape and state of regulatory uncertainty; and
    2.4. Fourth, the functions of ICASA.

3. We briefly deal with each in turn below, and are available to provide any further information to ICASA on request.

ABOUT MMA

4. MMA is a non-profit organisation that promotes democracy and a culture where media and the powerful respect human rights and encourage a just and fair society. MMA acts in a watchdog role to promote ethical and fair journalism that supports human rights.

5. MMA's vision is a just and fair society empowered by a free, responsible and quality media. Through a human rights-based approach, MMA aims to promote the development of:

    5.1. Media that is transparent, diverse, ethical and accountable to its audiences;
    5.2. Critical and constructive communications by the powerful; and
    5.3. Informed, engaged and connected citizenry.

[1] MMA was assisted in the drafting of these written submissions by ALT Advisory: https://altadvisory.africa.

6. MMA aims to contribute to this vision by being the premier media watchdog in Africa to promote a free, fair, ethical and critical media culture. MMA has 25 years of experience in media monitoring and direct engagement with media, civil society organisations and citizens. MMA is the only independent organisation that analyses and engages with media according to this framework. In all of its projects, it seeks to demonstrate leadership, creativity and progressive approaches to meet the changing needs of the media environment.

7. MMA has previously engaged on the Cybercrimes and Cybersecurity Bill (CCB) (now known as the 'Cybercrimes Bill') in the following instances:

    7.1. Providing written submissions to the Portfolio Committee on Justice and Correctional Services (PCJCS) on 8 August 2017;
    7.2. Presenting oral submissions in Parliament to the PCJCS on 21 September 2017; and
    7.3. Providing supplementary written submissions at the request of the PCJCS on 5 October 2017.

8. MMA recognises that cybercrimes and cybersecurity are increasingly becoming central to the changing needs of the media environment. As such, this falls squarely within the mandate of MMA.

RESOURCE CONSTRAINTS FACED BY ICASA

9. Before any additional roles and responsibilities are assumed by ICASA, it is imperative that ICASA is appropriately capacitated in terms of its financial, technical and human resources as a matter of urgency.

10. It is of serious concern that in ICASA's presentation to the Portfolio Committee on Communications on 18 April 2018 regarding the 2018/2019 Annual Performance Plan,[2] ICASA indicated that "budget cuts left [ICASA] with a huge budget deficit which will have a negative impact of the implementation of the Mandate". As a result of the challenges indicated by ICASA, it noted that it would not be able to afford the following over the Medium-Term Expenditure Framework (MTEF) period:

> **"1. Operational Costs**
>
> - Regional office relocation and tenant installation cost
>
> **2. Equipment and Projects**
>
> - Procurement and critical equipment required for:

[2] Accessible at https://www.ellipsis.co.za/wp-content/uploads/2018/04/ICASA_Annual_Report_Presentation_2018_19.pdf.

- Procurement of NATJOINTS Test Equipment
- Procurement of Quality of Services (QoS) Equipment
- Elections Monitoring Equipment
- SKA project"

11. There is no apparent indication that there is a plan in place to resolve the existing resource constraints being faced by ICASA. Notably, ICASA already has a expansive and important mandate that it is required to fulfil, that is being severely hampered by these constraints.

12. Accordingly, MMA would strongly caution against ICASA looking to expand its mandate before addressing the current resource constraints that it faces in fulfilling its existing mandate as it stands at present.

THE LEGISLATIVE LANDSCAPE AND STATE OF REGULATORY UNCERTAINTY

13. There are currently a plethora of laws – or proposed laws – that seek to address different matters of cybersecurity. However, the different stages of finalisation and implementation of these laws has given rise to significant regulatory uncertainty.

14. We note in this regard, for instance, the following:

    14.1. The Protection of Personal Information Act 4 of 2013 (POPIA) has been signed into law, but the substantive provisions have not yet been brought into force. As such, the requirements regarding appropriate technical and organisational safeguards required by POPIA are not yet in force. Even once the substantive provisions of POPIA are brought into force, responsible parties will still have at least a one-year grace period before they are required to comply.

    14.2. The Cybercrimes Bill, as adopted by the National Assembly, has now separated out the cybersecurity provisions. It is unclear at this stage when the Cybercrimes Bill will be finalised, or whether there is an intention to re-introduce the cybersecurity provisions at a later stage.

    14.3. Other proposed laws and amendments that implicate cybersecurity are the Critical Infrastructure Protection Bill, the Protection of State Information Bill (POSIB), the Defence Amendment and the Films and Publications Amendment Bill (FPAB). There is no certainty in respect of any of these by when they will be finalised.

14.4. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) is the subject of an extensive constitutionality challenge, with allegations that RICA has been abused to conduct unlawful surveillance in the country.

15. Furthermore, South Africa has signed – but not ratified – the Convention on Cybercrime of the Council of Europe.[3] South Africa has neither signed nor ratified the African Union Convention on Cyber Security and Personal Data Protection.[4] It is therefore unclear what South Africa's position in respect of cybersecurity is at the regional and international level.

16. We note in this regard that the existing and proposed regulatory framework that currently exists does not appear to foreshadow a role for ICASA to play in the realm of cybersecurity. This is similarly true in respect of the National Cybersecurity Policy Framework published in the Government Gazette on 4 December 2015.

17. Given the existing state of flux that the regulatory environment is currently in, and the high levels of regulatory uncertainty that persist in respect of cybersecurity, MMA would strongly caution against exacerbating this through the addition of further laws and policies in an effort to carve out a role for ICASA that does not presently exist. While these laws are certainly complex and nuanced, and require adequate time for appropriate public consultation processes to be engaged, there is an urgent need to resolve the existing state of regulatory uncertainty. Further uncertainty would only add to the regulatory malaise.

THE NEED FOR BETTER COORDINATION AMONGST ROLE-PLAYERS

18. Linked to the regulatory uncertainty in the country, there is also an existing conflation of roles amongst various role-players in the realm of cybersecurity that are facing significant structural and institutional challenges. We note in this regard, for instance, the following:

18.1. The State Security Agency has been plagued with allegations of abused of power, and is currently under an investigative review.

18.2. The Information Regulator, established under POPIA, is yet to be empowered to begin its substantive work, and is currently hamstrung in its mandate by

[3] Accessible at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=nvBhOL7G.
[4] Accessible at https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf.

the fact that the substantive provisions under POPIA have not yet been brought into force.

18.3. The Ministry of Telecommunications and Postal Services has now been combined with the Ministry of Communications.

18.4. The Cybersecurity Hub remains in a pilot stage of implementation, and it is unclear whether the Cybersecurity Advisory Council continues to exist or operate.

18.5. The National Prosecuting Authority (NPA) has been besieged with challenges, and is currently without a permanent National Director of Public Prosecutions.

19. In MMA's submissions on the CCB, MMA has previously noted its concerns on the lack of any overarching internet governance policy on how current and proposed legislation that deal with information and digital rights regulation is to be managed by the different role-players, including in respect of cybersecurity, or accordingly a lack of coordination amongst the various role-players. In the absence of a clear government internet governance policy and legislative guidance, an unduly complex structure of oversight is in the process of being created.

20. The result is that that people in South Africa, civil society organisations, and members of the media, among others, need to navigate an overly complex regulatory landscape in order to make submissions, conduct their business, and, ultimately, defend and protect their information rights. Additionally, this poses significant challenges to government's coordinated and effective implementation of the existing regulatory provisions, and may result in overlapping mandates or aspects not being assigned or accounted for by appropriate functionaries. Further, with rapid technological developments, including the development of technologies used to perpetrate cybercrimes, the complex governance structures created by the various pieces of legislation dealing with internet governance may not be amenable to swift and effective responses to cybercrimes and technological developments by the state which, in turn, may lead to a derogation by the state of its constitutional obligation to respect, protect, promote and fulfil the rights in the Bill of Rights.[5]

21. A further constitutional consideration relates to cooperative governance and intergovernmental relations. In terms of section 41(1)(c) of the Constitution "[a]ll spheres of government and all organs of state within each sphere must provide

[5] See section 7(2) of the Constitution.

effective, transparent, accountable, and coherent government for the Republic as a whole" and the must "co-operate with one another in mutual trust and good faith by coordinating their actions and legislation with one another".[6]

22. Accordingly, MMA has called for the establishment of an Interdepartmental Steering Committee (ISC) on Internet Governance to address relevant matters, including cybersecurity, in which ICASA could also play a role. It is proposed that the ISC be led by the Department of Justice, and also comprise representatives from the following role-players:

    22.1. Department of Defence;
    22.2. Department of Home Affairs;
    22.3. Department of International Relations and Cooperation;
    22.4. Department of Justice and Constitutional Development;
    22.5. Department of Science and Technology;
    22.6. Department of Telecommunications and Postal Services;
    22.7. Financial Intelligence Centre;
    22.8. National Prosecuting Authority;
    22.9. National Treasury;
    22.10. South African Police Service;
    22.11. South African Revenue Service;
    22.12. State Security Agency;
    22.13. Information Regulator;
    22.14. Two representatives from opposition parties represented in the National Assembly;
    22.15. Two teachers of law, or members of the attorneys' or advocates' profession, with knowledge of internet governance laws, appointed following a public call for nominations;
    22.16. Two technical experts in internet governance following a public call for nominations;
    22.17. Two members of civil society organisations working on internet governance following a public call for nominations.

23. We emphasise that:

    23.1. The objects should be broader than cybersecurity alone, to reflect the broader internet governance mandate and the multi-disciplinary, cross-cutting challenges that these issues present.

[6] See section 41(1)(h)(iv) of the Constitution.

23.2. Reporting by the ISC should be to Parliament, not to the Joint Standing Committee on Intelligence (JSCI), to ensure greater transparency, and cognisant that the JSCI typically holds its meetings in closed sessions.

23.3. We propose adding representatives from opposition parties represented in the National Assembly, members of the legal profession, technical experts and civil society representatives, to ensure accountability, a diversity of views, and the requisite technical expertise.

24. At the crux of our submission in this regard, in our view it will not be helpful to add ICASA as another ad hoc role-player to the existing landscape, that performs a tangential role to the existing role-players. Rather, what is urgently needed is coordination. ICASA could arguably play a role in facilitating or participating in this coordinated effort, to the extent appropriate, with a view to ensuring that a holistic, streamlined approach is taken to matters of internet governance and ICTs, including cybersecurity.

THE FUNCTIONS OF ICASA

25. Lastly, we wish to highlight sub-sections 4(3) and (4) of the ICASA Act that set out ICASA's functions. Importantly, these sub-sections state respectively that ICASA "is independent, and subject only to the Constitution and the law, and must be impartial and must perform its functions without fear, favour or prejudice" and that ICASA "must function without any political or commercial interference".

26. In determining any role that it may wish to play in the realm of cybersecurity, ICASA must be sure not to compromise on these provisions. The independence of ICASA from interference from the public or private sector is paramount to it being able to fulfil its mandate.

27. As cybersecurity is typically seen as a principally state-led function, ICASA must be cognisant not to traverse this line to the effect that it is seen as a state functionary. ICASA must also ensure that its role does not in any become – or appear to become – one that involves the monitoring and surveillance of users or operators, or that uses the information provided to ICASA by licensees to facilitate monitoring or surveillance activities. In our view, it is further not ICASA's view to engage in activities that are tantamount to regulation of the internet or online content.

28. It is also necessary to be cognisant of the exigencies of South African society. ICASA should avoid unduly increasing barriers to entry for new entrants to the market or new users by imposing standards that may be prohibitive. Furthermore, while ICASA may

see a role to be played in developing industry standards, ICASA must also have regard to the risks that may be involved in the setting of such standards that may ultimately render the networks more vulnerable to interference by setting standards that are known and can therefore be targeted and breached.

29. In our view, ICASA should foster its role as a facilitator between public and private sector engagement. Furthermore, ICASA may also have a more active role to play in raising consumer awareness and digital literacy, and protecting the rights of vulnerable users. Building awareness and capacity on ICT-related matters – that include, but extend beyond, cybersecurity – is an important and much-needed endeavour that ICASA may want to pursue further. We re-iterate, however, that given existing resource constraints, ICASA should be cautious about expanding its mandate until this is resolved.

CONCLUSION

30. MMA recognises the dynamic and evolving nature of ICTs and cybersecurity globally, and the need for all relevant role-players to be responsive in the face of emerging opportunities and challenges. However, in doing so, it is important to be duly cognisant of the existing landscape and shortcomings, and ensure that these are addressed before engaging in new endeavours.

31. MMA appreciates the opportunity to provide its input through this submission, and would welcome the further opportunity to make oral submissions as this inquiry progresses.

MEDIA MONITORING AFRICA
Johannesburg, 30 November 2018