*MOBILE TELEPHONE NETWORKS PROPRIETARY LIMITED*
*(Registration number:1993/ 001436/07)*
*216 14th Avenue, Fairland, 2195*
*Private Bag 9955, Cresta, 2118, South Africa*
*Tel +2711 912 3000 Fax +2711 912 4670*

**30 November 2018**

**The Independent Communications Authority of South Africa (ICASA)**
**350 Witch-Hazel Avenue**
**Eco Point Office Park**
**Eco-Park Estate**
**Centurion**
**0144**
**For Attention: Ms Violet Letsiri**
**Senior Manager: Social Policy for ICT Services**

**Via Email: VLetsiri@icasa.org.za**

**Dear Ms Letsiri,**

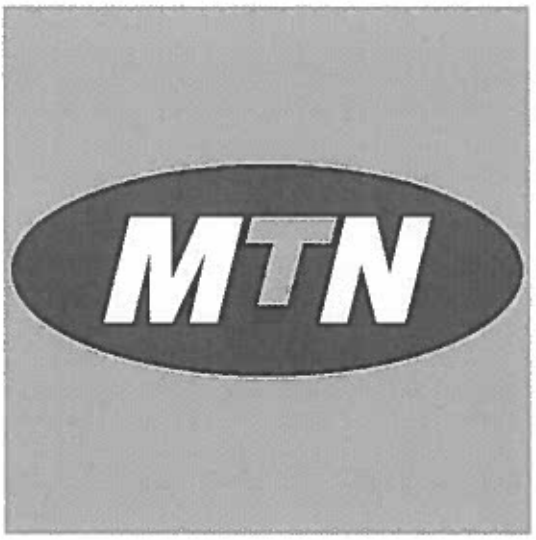
RE: **MTN's written Submission on the Inquiry into the Roles and Responsibilities of the Independent Communications Authority of South Africa in Cybersecurity**

Please find enclosed, MTN (Pty) Ltd (hereafter referred to as "MTN") submission on the Inquiry into the Roles and Responsibilities of the Independent Communications Authority of South Africa in Cybersecurity.

Mobile Telephone Networks Proprietary Limited ("MTN") welcomes the opportunity to make submissions to the Authority and look forward to participating in the public participation process.

Yours faithfully

**Moses Mashisane**
**General Manager: Legal and Regulatory Affairs**
**MTN (Pty) Ltd**




# MTN'S SUBMISSION TO THE INDEPENDENT COMMUNICATION AUTHORITY OF SOUTH AFRICA ("ICASA") INQUIRY INTO THE ROLES AND RESPONSIBILITIES OF ICASA IN CYBERSECURITY

**30 NOVEMBER 2018**

Contents

## 1. INTRODUCTION

On the 28th September 2018, the Independent Communications Authority of South Africa ("the Authority"), published its notice to conduct an inquiry in terms of Section 4B of the Independent Communications Authority of South Africa Act No 13 of 2000 (ICASA Act").

The purpose of the inquiry is to determine the roles and responsibilities that the Authority should play in relation to cybersecurity guided by the Electronic Communications and Transactions Act No. 25 of 2002 and the ICASA Act.

MTN's submissions is structured as follows:

- Part A: Background to the Cyber Security Bill and MTN's submissions;
- Part B: MTN's specific submissions relating to the questions posed by the Authority in relation to the Authority's role in relation to cyber security.

## 2. PART A: BACKGROUND TO THE CYBER SECURITY BILL AND MTN'S CONCERNS

MTN submitted written submissions to the Portfolio Committee on Justice and Correctional Services ("Portfolio Committee") on the 11th August 2017 on the proposed Cybercrimes and Cyber Security Bill published in the Government Gazette No. 40487 dated 09th December 2016 ("the Bill"). The submission focussed on General Submissions, Recommendations as well as Specific Submissions relating to the text in the Bill. In its submission on the Bill to the Portfolio Committee MTN raised objections in respect of the following key aspects of the Bill:

- The Standard Operating Procedures;
- The definition of various offences, in particular the definition of what constitutes "Cybercrime";
- The incongruence between the Bill and other legislation in respect of electronic evidence and integrity; and
- The onerous requirements placed on mobile network operators in respect of evidence preservation and disclosure.

While MTN welcomed the introduction of the Cybersecurity legislation, MTN was concerned with the impact that some of the requirements of the Bill would have on day to day operations within MTN and our subscribers' right to privacy.

It is against this background that MTN is responding to the section 4B inquiry. In terms of Section 4B it is critical to consider the Bill, which covers aspects of cyber security in detail.

## 3. PART B: MTN'S SPECIFIC SUBMISSIONS RELATING TO THE QUESTIONS POSED BY THE AUTHORITY.

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

With the rapid evolution of Information Communication Technologies (ICT) around the world and increase in demand for services and access to high speed broadband, the internet and mobile services have become indispensable. As a result of the continued use of the internet and associated services, the risks and dangers cybercrime such as fraud, identify theft, fake news, propagation of inappropriate content and hate speech (to name a few) has increased exponentially

Cybersecurity is a shared responsibility between Government, the private sector and individuals. In order to be successful in the fight against cybercrime a collective national cybersecurity effort is required. The collective effort should ideally aim at defining ways to achieve the objectives and to clarify the roles and responsibilities of the various stakeholders.

The specific objectives of the Cybercrimes Bill are as follows:

- It creates a uniform framework for the detection, combatting and prosecution of cybercrime;
- It promotes a cybersecurity culture in South Africa;
- It aims to create various structures to combat cybercrime and to develop the capacity and resources necessary to create a cybersecurity culture.

The Authority, as a regulator in the ICT sector, at this point does not have the requisite capacity to play an active role in respect of cybersecurity. It is also necessary for the Authority to ensure that regulations issued by the Authority in terms of its empowering provisions compliment and do not contradict primary legislation which deals with issues of cyber security for example the Electronic Communication's and Transactions Act no 25 of 2002 ("ECTA") and the Bill, once it becomes effective.

Even though the Authority will play a key role in cybersecurity initiatives, there has to be institutional improvements and various other changes that need to be made to ensure that

the Authority remains relevant in dealing with cybersecurity. There should also be a clear demarcation between criminal activities, the prevention of cybercrime and matters relating to cyber security. The department of Justice and Constitutional Development is best placed to deal with cybercrime and criminal activity, whilst the Electronic Communications and Transactions Act also covers cybercrime in Chapter XIII.

It is however MTN's submissions that the Authority in this respect must collaborate with other stakeholders and the ICT industry in particular to effectively manage cybersecurity.

For the Authority to manage its role in cybersecurity, it is imperative that the Authority develops awareness, skills and resources internally to manage cybersecurity risks and to advise the ICT industry as well as regulate appropriately within its mandate. In this regard, it is prudent to note that the Authority as an adviser would best position itself once it attains the requisite resources and skills due to the ever evolving nature of the ICT and associated technology.

Capacity building is crucial as it is a necessary component of ensuring cybersecurity awareness. This can be achieved by regular cybersecurity related training being made available to the ICT industry, Authority's stakeholders and members of the public.

To assume an effective role in respect of cybersecurity, MTN recommends that the Authority should assist its stakeholders with analysis and dissemination of global cyber threat information and to also assist in training and skills development on the various aspects of cybersecurity. It is also recommended that the Authority facilitate multi-stakeholder engagement and cooperation on matters of cybersecurity. It must however be noted that all of these roles are currently assigned to the Cyber Security Hub as referred to in the Cybersecurity Bill.

Due to the many technological changes in recent years, the role of the Authority has become more prominent, and it is envisaged that the Authority assumes a role where it promotes the ICT sector development.

Previously, the Authority's main focus was on traditional telecommunications, however the current dynamic converged environment requires a new approach on a technology neutral basis.

In conclusion, MTN submits that the Authority play a role with respect to cybersecurity by engaging with the ICT sector and providing technical and industry expertise. However, it would not be appropriate for the Authority to take the lead in regulating cybersecurity since the Department of Justice and Constitutional Development has initiated the Cybercrimes and Cyber Security Bill and is best placed to regulate such matters.

*Question 2: How would you define cybersecurity?*

MTN confirms and agrees with the inclusion of the following aspects in the definition of cybersecurity:

- The information technology security;
- Legal or law enforcement;
- National security; and
- Economic perspective.

MTN submits that cybersecurity or information technology security are the techniques of protecting computers, networks, programs and data from unauthorised access or attacks that are aimed at compromising the particular computer, network, program or data.

MTN submits that cybersecurity or cyberspace security within the context of MTN, is defined as the preservation of confidentiality, integrity and availability of information in the Cyberspace.

Cyberspace is defined as the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance.

Some basic techniques used for application security are Input Parameter Validation, User/Role, Authentication and Authorization, Session Management, Parameter Manipulation and Exception Management and Auditing and Logging.

Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are Identification, authentication and authorization of a user and critical infrastructure / systems and Cryptography.

Disaster recovery planning is a process that includes performing risk assessment, establishing priorities and developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include Anti-virus and Anti-spyware, Firewall to block unauthorized access to your network, Intrusion Prevention Systems (IPS) to identify fast-spreading threats, such as zero-day or zero-hour attacks, Virtual Private Networks (VPNs) and to provide secure remote access.

MTN accordingly proposes and a comprehensive definition of cybersecurity, in addition to the definition that is contained in the Cybercrime Bill, should include the following elements:

- Content related offences;
- Copyright related offence;
- Offences where the integrity and availability of computer systems and data have been compromised; and
- Any offence related to computer forgery and fraud.

*Question 3: Are there any other laws that the Authority should consider in determining its role with regards to Cybersecurity?*

MTN agrees with the Authority that the primary pieces of legislation which must be considered have been correctly identified by the Authority.

MTN, in its written submissions made to the Portfolio Committee on the Cybercrime and Cybersecurity Bill submitted that the current version of the Bill did not sufficiently harmonise with other pieces of legislation;

In this regard, it is submitted, and the Authority has correctly identified that the Bill in its current form did in fact create new obligations on electronic communications service providers, especially in relation to aiding law enforcement agencies with the investigation of cybercrimes

In particular MTN submits that the Bill does not consider the implications of access to information and data protection laws, particularly the extent to which the Bill voids obligations of confidentiality and privacy, as well as the licensing conditions of the electronic communications service providers. This is because the correct primary legislation and proposed legislation (such as the Protection of Personal Information Bill) were not considered when drafting the Cybercrime and Cyber Security Bill.

*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"*

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

Network Integrity and Information Security refers to the following core elements:

- Confidentiality – only those who are supposed to access the data can access it;
- Integrity – the data that is stored is only changed or accessed when it's supposed to be;
- Availability – the data can be accessed when it is needed;
- Authentication – the person who accesses the data is authorised to do so and is who he says he is;

- Authorisation – the person is authorised to access the data; and
- Accounting – means keeping a log of all access to the data.

Network Integrity is ensured by mechanisms that prevent data from becoming lost, garbled or modified without consent. These mechanisms are embedded within software protocols, drivers and network firmware. At an enterprise level, network integrity refers to the complete network as a whole with network discoverable resources.
Should there be any discrepancies, this would entail that there is a compromise in network integrity, whether by hardware failure, software failure, network intrusion or otherwise.

A network that is secure prevents intrusions like worms and trojans which deliver malware into the network as well as traffic anomalies which adversely affect the network and quality of service.

A network that is functioning properly will ensure the following:

- Applications and users receive adequate network availability;
- Applications and users receive sufficient bandwidth;
- Network security if effective; and
- Network management has complete control of the entire network.

The layered approach to network security and network integrity comprises of the following layers:

- Perimeter defence;
- Systems layer;
- Application gateway layer; and
- Host integrity layer

In respect of the role of the Authority in ensuring network security and network integrity, MTN submits that the Authority's role be expanded to include the following:

- Capacity Building in respect of network security and integrity;
- Create mechanisms for sharing, cooperation and collaboration of knowledge;
- Public awareness;

- Develop a concentrated strategy to communicate the importance of network integrity and security to consumers or licensees?

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

MTN submits that there must be a balance between the cybersecurity requirements nationally and the efficiency imperatives of business.
In this regard Network operators already have entrenched network security and integrity protocols in place. These protocols follow international best practise and industry standards.

Network operators can however partner with the Authority in terms of defining the minimum requirements in respect of network security and integrity standards, especially in view of its expertise and knowledge of its day to day operations. We caution against an inflexible-based approach in favour of a light touch following international best practise and industry standards bearing in mind the dynamic nature of technology and the ICT industry.

Additionally, and since cybersecurity must be viewed from both an economic and information security perspective, it is imperative that the Authority should facilitate collaboration together with the ICT sector and government institutions.

The Authority's mandate under the Objects of the Electronics Communications Act no 36 of 2005 ("ECA) is as follows[1]:

*"to… ensure information security and network reliability;"*

MTN is of the view that the Authority could enhance its approach by playing a more active role, especially in terms of public awareness relating to cybersecurity. This is predicated by the fact that cybersecurity remains the responsibility of everyone, including the private sector and individuals alike;

[1] Section 2(q) of the ECA

*Question 5: Section 36 (2) of the ECA provides that "standards must be aimed at protecting the integrity of the electronic communications network", kindly provide your understanding of this section.*

To answer this question, section 36 should be read as a whole. Section 36 states the following:

> *"(1) The Authority may, subject to the provisions of the **Standards Act, 2008 (Act No. 8 of 2008), [our emphasis]** prescribe standards for the performance and operation of any equipment or electronic communication facility, including radio apparatus.*
>
> *(2) Any such standard must be aimed at–*
>
> *(a) **protecting the integrity of the electronic communications network; [our emphasis]***
>
> *(b) ensuring the proper functioning of connected equipment or electronic communications facilities;*
>
> *(c) ensuring interoperability, interconnectability and harmonisation;*
>
> *(d) avoiding harmful interference with the electronic communications network…"*

MTN submits that its interpretation of section 36 is that the Authority may prescribe standards which must not conflict with the Standards Act, 2008 (Act No. 8 of 2008). Considering this, MTN is of the view that the Standards Act as well as international and best practise be considered in ensuring the protection of Network Integrity.

Section 24 of the Bill stipulates the standard operating procedure to be put in place, as well as the standards to be adhered to by ECSP's.

MTN submits that the implementation of standards should take into consideration the following:

- That such standards do not impair the function of a computer or storage mechanism;
- That these standards do not interrupt the services offered by an ECSP to its customers not implicated in an offence;
- That such standards do not place at risk the personal information of any customer of an ECSP.

In addition, it is imperative that the standards that are developed are in line with the operational requirements of the ECSP, and that they do not create additional costs to the ECSP by the implementation of standards that are not in line with the services offered by the ECSP.

The requirements in terms of Section 24 of the Bill purports to amend the requirements of the ECA, and there is currently no evidence to suggest that the provisions of the ECA will be amended so that it is in line with the requirements of the Cybersecurity Bill.

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

Any additional role that is to be played by the Authority will depend largely on the technical and industry expertise that exists.

The Cybersecurity Bill and the ECTA currently offer sufficient mechanisms to deal with cybersecurity.

MTN submits that the below key components should guide the authority in terms of any additional role that is envisaged:

- Advisory: by providing advice to ECSPs;

- Incident Management: by sharing cybersecurity threats with ECSP's;
- Promote awareness

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

MTN submits that the Authority actively participates in awareness and educational campaigns to highlight the risks related to cyber threats.

In this regard, the Authority can partner with its licensees and other stakeholders to educate members of the public.

*Question 8: Should the Authority strive to follow the same approach? What legislative powers are there to enable the Authority to implement this?*

MTN submits that the powers being referred to are fully included in the Cybersecurity Bill, and many functions and rights of licensees are referred to in the Bill.

*Question 9: Should the Authority, through the end user regulations also require licensees to limit or cut internet connectivity of users with less that required software protection forcing them to upgrade their existing programs or download new ones?*

MTN submits that this would be a curtail to the rights of consumers in so far as it relates to the freedom of choice, and that to cut internet connectivity would be an unjust administrative action in violation of the Promotion of Administrative Justice Act No 3 of 2000.

*Question 10: Should a legislative change be encouraged which will grant the Authority, the rights to suspend business or software companies, in the ICT sector, that fail to correct the vulnerabilities of their security programs?*

MTN submits that it will be imprudent to enable legislative changes, in the absence of any consultation with its licensees.

Additionally, and due to the lack of expertise within the Authority, the vulnerability of the security programs must first be assessed against international best practice and standards before any determination can be made in this regard.

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

It is submitted that in view of the fact that the Authority lacks the expertise and resources, it would not be prudent for the Authority to assume this function.

These functions are already assigned to the Cybersecurity Hub and the Cyber Centre.

*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?*

The current legislative framework does not specifically define spam resulting in the lack of anti-spam provisions in our law.
ECTA simply defines "Spam" as any "unsolicited commercial communication" and only applies to electronic communication and not paper-based communications.
ECTA requires that the sender of spam provide an opt-out with each message, which has been ineffective.

In terms of the Consumer Protection Act, the issue of spam is dealt with indirectly via the direct marketing provisions, where every consumer is afforded the right to request the sender to desist from sending direct marketing communications.

Section 69 of POPI also makes it unlawful for a direct marketer to market directly to a consumer unless the consumer has opted-in and provided permission. On its effective date, POPI will provide more protection against unwanted direct marketing messages.

Similarly, in terms of the European Union General Data Protection Regulations consumers must provide consent to receive messages from marketers on products and offerings, in that:

- Requests must allow individuals to consent;
- Consent to be documented;
- Provide consumers options to withdraw consent

In terms of self-regulation, the Internet Service Provider's Association of South Africa ("ISPA") deals with unsolicited communications as follows:

*"Unsolicited communications ("spam")*

*ISPA members must not send or promote the sending of unsolicited electronic communications and must take reasonable measures to ensure that their networks are not used by others for this purpose.*

*ISPA members must provide a facility for dealing with complaints regarding unsolicited electronic communications originating from their networks and must react expeditiously to complaints received."*[2]

The Wireless Application Service Providers Association ("WASPA") also self-regulates direct marketing in a similar manner providing for a compulsory opt-out opportunity[3]

However, as the Authority has correctly pointed out, spam is also used as a vehicle to generate BOT viruses that lead to attacks on critical information infrastructures, and in this regard, spam therefore becomes a major cybersecurity threat.

To address this issue, MTN has developed the following security measures to protect itself and its customers from spam:

- Partnered with the GSMA to exchange information relating to spam messages; and
- Regular campaigns to alert its customers to the risk of spam.

The Regulation of Interception and Provision of Communication Related Information Act 70 of 2002, places limitations on operators in that operators are prohibited from actively intercepting and monitoring messages and emails that are relayed via its network to identify spam messages.

The authority can in this regard play a pivotal role in the following manner if the Authority has the capacity to do so:

- Communicate with stakeholders on new spam messages;
- Identification of new BOT viruses;

[2] https://ispa.org.za/code-of-conduct/

[3] https://waspa.org.za/coc/15-9/ See rule 16 and 17.

- Collaboration with international regulators in terms of identifying new threats, phishing emails and spam messages, as well as steps taken to identify such threats.

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

Many consumers, despite being adept in the use of technology, remain critically vulnerable in respect of being exposed to cybersecurity threats. This is also as a result of consumers being ignorant and in some cases irresponsible (due to lack of knowledge on the issue of cybersecurity).

In this regard, it is only through continuous education and awareness that the consumers can learn to limit and avoid any exposure to cyber threats.
This applies more so to minors who participate extensively in online social platforms such as Facebook, twitter etc.

By virtue of this exposure in cyber space, these vulnerable consumers stand a higher risk of being exposed to cyber threats, BOTS, spam, malware, exposure to inappropriate content, cyber bullying and catfishing by sexual predators and other such incidents.
Additionally, with the rise in child pornography, and sexual predation online, minors open themselves up to having their personal details compromised and may suffer significant psychological trauma as a result.

By extending a rigorous and robust consumer awareness campaign, the risks can be mitigated, if not eradicated altogether. MTN believes that the Authority and the ICT industry as a whole bear the responsibility to educate consumers, especially children.

The Authority can assist by embarking on the following:

- Partner with the private sector to conduct awareness;
- Partner with the ICT industry including Broadcasters and operators to conduct educational and awareness campaigns;
- Collaborating with other regulators such as the Film and Publications Board; and

- Aide industry stakeholders in respect of communication, critical messages and crisis communications.

*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.*

The End-user and Subscriber Service Charter Regulations, 2016 requires operators to submit bi-annual reports on quality of service. Regulation 9 includes reports on network availability. Network availability is directly impacted by network outages and is an adequate measure.

*Question 14: Should the Authority set similar standards for licensees to ensure that customer's proprietary network information is protected from unauthorised disclosure*

Customers would not have proprietary network information. A more appropriate term would be personal information. MTN is obliged to keep customers personal information confidential in terms of regulation 3.1(g) (key commitments) of the Code of Conduct for Electronic Communications and Electronic Communications Network Licensees, 2007. Moreover upon its effective date, POPI provides detailed obligations on any party who collects, processes or stores personal information.

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

Network Security is the active process of taking physical and software-related preventative measures to protect the underlying networking infrastructure from unauthorised access, misuse, malfunction, modification, destruction or improper disclosure. This active process creates a secure platform for computers, users and programs to perform critical functions effectively and efficiently.

The Authority can assist in network security issues by collaborating with international and local bodies and regulators to advise on the minimum standards to be implemented by licensees. Such standards should take into account that the minimum standards should not be prescriptive and should only be a guideline; and should take into account that these functions have been assigned to the Cyber Security Hub in terms of the Cybersecurity Bill.

Additionally, the Authority can assist in compiling a pool of resources such as experts who can advise licensees of measures to implement to ensure network security.

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

Network reliability refers to the attribute of any computer related component (software, hardware or a network) that consistently performs according to its specifications. It is concerned with the capacity of a networks ability to offer the same services even during a failure.

Network Integrity relates to the various mechanisms in place to ensure the overall completeness, accuracy and consistency of data.

Information Security generally relates to the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection and destruction of information.

All three of the above differ significantly from network security in that network security is the platform by which reliability, integrity and security is managed.

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

The primary role of SITIC is to exchange information on cyber threats between the public and private entities; to operate as a public warning system to provide information on threats; to provide information and advice; and to compile and publish incident statistics.

A critical component of the Cybercrimes Bill is that it caters for the creation of Computer Security Incident Response Teams (CYBER SECURITY HUB) and Industry Cyber Security Hub.

The primary purpose of the Cyber Security Hub is to perform similar functions as those of SITIC.

In view of the above, it is submitted that should the Authority undertake to perform similar functions as those of Cyber Security Hub, then this would be a duplication of roles.

It is however submitted that there is no preclusion from the Authority acting as repository for information relating to cyber threats, and from assisting in creating awareness amongst its licensees.

*Question 18: What cybersecurity measures are in place by ISP's in South Africa to protect the consumers?*

MTN regularly posts information on its website advising customers on being proactive in terms of protecting themselves in cyber space.

This includes measures such as online security, general internet security tips, and advice on identity theft and the proper use of social networking.

In addition to the above, MTN has implemented measures to prevent the accessing of any child pornographic sites, in line with Section 72(A) of the Film and Publications Act.

Any site that is deemed to be inappropriate in terms of containing child pornography is blocked and access is restricted.

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

Network level filtering allows the user to block any web-based content that may be inappropriate for minors.

Such filters allow a consumer to manage access in their home to a range of internet services which includes inappropriate content.

MTN supports the filtering of all age inappropriate content, and the interest of minors remains paramount.

However, MTN does not advocate that the onus of offering network filtering services be placed on licensees for threats relating to malware and BOTS etc.
This is predicated by the fact that it then becomes the responsibility, even in circumstances where the user / consumer negligently downloads malware or spyware.

The Authority should be mindful of the limitation of liability clauses in the ECTA, and any regulation that is drafted should not seek to amend the rights as enshrined in the ECTA.

In these eventualities, the licensee can then be held liable for any malfeasance that occurs as a result of the consumer's negligence, and this creates an onerous obligation on the part of the licensee.

*Question 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?*

It is submitted that in terms of the Cybercrime Bill, this function is mandated to the National Cybersecurity Centre in conjunction with the Cyber Security Hub. Accordingly, there is no need for this role to be duplicated. The Authority can however assist in a collaborative effort by obtaining such details from the Cyber Security Hub and then to disseminate such information to its licensees and other affected parties, and to assist in public and consumer awareness.

*Question 22: Is POPI sufficient to deal with protection of Personal Information. What can ICASA do to help enforce POPI in the ICT Sector?*

MTN submits that the provision of POPI are adequate to deal with the protection of personal information. In terms of POPI, the Information Regulator has been assigned the roles of ensuring compliance and enforcement.
However, the Authority can engage with the Information Regulator and conduct awareness campaigns with its licensees, in order to coordinate efforts and ensure compliance in the ICT Sector.

MTN submits that the Information Regulator is the appropriate authority to deal with such incidents. The Authority can however, act by communicating the critical incidents to create awareness amongst its licensees.

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

MTN submits that it is critical for the Authority to involve itself in educational campaigns with regards to online protection to both parents and minors. MTN proposes that this be done in collaboration with the Film and Publication Board.

By virtue of the fact that the Authority is an independent regulator, the Authority can partner with the private sector, including its licensees and media houses from raising awareness. Such awareness campaigns can be done via print and social media.

MTN remains committed to support efforts to safeguard the public, especially minors, and will actively participate with the Authority in respect of any educational and awareness campaign in this regard.

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

The Authority can, through engagement with the private sector and NGO's, develop a pool of resources and experts who can be utilised in its educational and awareness campaigns.

These resources can also include international experts, who through inter government and inter agency relationships could offer their services in offering of the cybersecurity training. There are currently many NGO's and private sector entities who engage in, support and sponsor education and awareness. MTN submits that collaboration with such entities is key to deliver a common message.

The Authority must be mindful not to compartmentalise its resources and should focus on a pool of resources from across various sectors. This is by virtue of the fact that cybersecurity incidents occur across all sectors, and not only in the ICT sector.

*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 on each of the above category*

MTN submits that the standards cannot be prescriptive as in most instances, licensees may already have stringent standards in terms of its security protocols in place, and these standards consider the licensees own operational requirements.

MTN submits that in terms of the Cybersecurity Bill, the ability to conduct research should be left to the Cybersecurity Hub, more so in relation to the development of standards and international best practice. The Cybersecurity Hub currently has the capacity and resources to undertake research in the area of cybersecurity.

*Question 26: How can Mobile Operators partner with ICASA to teach children about safe internet practices?*

MTN assures the Authority that it will commit itself to partnering with ICASA in educating children on safe internet practices. MTN will aid the Authority to develop training material, both via print and online in order to alert children of the risks associated with online activity.

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

The Authority, if it does possess the capacity and expertise can advise higher education in the area of cybersecurity qualifications. However, should the authority not possess such skills, then it is submitted that industry experts and NGO's can advise tertiary institutions on appropriate and relevant course content that will be suitably recognised by the industry.

*Question 28: Is Integrity as written in ECA equivalent to Security? Please elaborate*

MTN submits that whilst the ECA refers to integrity, it does not equate with security. The definitions hereof have been discussed at length under Question 15 herein.

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

MTN welcomes the participation of the Authority in the process of defining the standards, but advises that in view of the provisions of the Cybersecurity Bill which caters for the creation of a Cyber Security Hub, that the Authority's role of developing standards and codes of conduct would be duplicated.

MTN recommends that the Authority act as an advisor to the Cyber Security Hub. The Authority, if it possesses the expertise and resources, will then be able to share its expertise with the Cyber Security Hub, and assist the Cyber Security Hub from an advisory perspective.

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

MTN has certified and trained personnel in respect of cybersecurity. In this respect, these personnel are experts in their relevant fields. The role of these personnel is to primarily ensure the following:

- Network and Information Integrity;
- Network and Information Security; and
- Network Reliability

The day to day functions of these personnel is to constantly ensure that services are not affected, and that consumer information is protected. A significant amount of resources is committed to identify threats on a constant basis, to scan the network for malware and spyware, as well as intrusion and detection.

In terms of the overall risk matrix, MTN conducts audits in line with international benchmarking and standards, in respect of all computer software and hardware to identify threats and vulnerabilities.

*Question 31: Should the Authority place requirements on licensees to capacitate and make consumers aware of cybersecurity threats? Please elaborate.*

MTN is committed to engaging with the Authority and to participate jointly with the Authority in making consumers aware of cyber related threats. The public-private partnership initiative is welcomed. However, MTN cautions against a rule-based approach in favour of a light touch approach.

*Question 32: What policy making role should the Authority play with regards to Cybersecurity?*

The Authority is a creature of statute with a specific mandate therefore the legislature is responsible for policy making, together with Parliament. ICASA is not empowered to set policy.

As a functionary of Government, the Authority can, in consultation with licensees, present the views of licensees in respect of policy decisions with regards to cybersecurity

In this respect, the Authority, by effectively utilising its expertise and pool of resources, can advise Government on the impact (if any) of any policy decisions on cybersecurity issues.

With the introduction of Next Generation Networks and the regulation thereof, it is imperative that the Authority partners with licensees in order to identify potential cyber threats to such networks.

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

The institutions established under the Cybercrime and Cybersecurity Bill are best placed to regulate cybersecurity. For ICASA to do the same would be a duplication of effort and resources.

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

MTN is in support of self-regulation. Cybersecurity and cybercrime incidents affect the ICT financially and cause reputational harm. It is in the best interest of the Industry to Self-Regulate. Furthermore, POPI and the Cybercrime and Cybersecurity Bill touch on these issues. The mandates of self-regulatory bodies such and ISPA can also be expanded to monitor compliance.

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

MTN iterates its position that the development of the standards according to the Cybersecurity Bill remains the prerogative of the Cyber Security Hub.

The Cybersecurity Bill creates an obligation for licensees to actively monitor its network for threats, and in this regard, places an obligation on licensees to report such threats to the Cyber Security Hub In terms of the Bill, it is an offence for a licensee to fail to take adequate steps to identify threats, and to report incidents to the Cyber Security Hub, and to take appropriate action.

MTN accordingly submits that the relevant provisions of the Cybersecurity Bill provide enough recourse and regulates the conduct of licensees, with the threat of sanctions being imposed.

## 4. CONCLUSION

MTN is aware of the real threat that is posed by cyber criminals. MTN is cognisant of the fact that more needs to be done to protect not only itself from cyber criminals, but to also protect its consumers.

MTN welcomes the role envisaged by the Authority in respect of cybersecurity. However, any interventions proposed by the Authority in this regard must be conceived within the current legislative prescripts and should be in line with what is proposed in the Cybersecurity Bill.

MTN urges the Authority to ensure that there is collaboration between the Authority and the licensees, so that a proper framework can be created in respect of the roles and responsibilities of all stakeholders, and that such roles and responsibilities is properly documented and aligned to the Cybersecurity Bill.

MTN commits to engaging with the Authority to ensure that the Authority's best efforts and resources are deployed to ensure that its consumers are protected by any cyber related threat.