Vodacom's written submission in response to ICASA's inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity

[Government Gazette Number: 41944, Notice Number 1017 of 28 September 2018]

1 INTRODUCTION

Vodacom (Pty) Ltd ("Vodacom") welcomes the opportunity to participate in the "Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity" (the Inquiry") as published by ICASA ("the Authority") in Government Gazette No. 41944, Notice Number 1017 of 28 September 2018.

Vodacom confirms its willingness to participate in any further consultative process, which the Authority may undertake in this regard.

- Our submission is comprised of two parts:
- Part A: Vodacom's response in principle to the Inquiry;
- Part B: Vodacom's answers to the questions posed in the Inquiry.

2 Part A: In Principle Comments

Vodacom shares the Authority's view that the regulatory functions of the Authority have to evolve as technologies evolve. However, the evolution of technology in and of itself is unlikely to provide sufficient insight or guidance into why and how the Authority's regulatory functions have to evolve. The evolution of technology is one of the many factors that necessitates a re-evaluation of the Authority's regulatory functions.

The Authority may want to contemplate the implications of an essentially borderless ICT ecosystem compromised of multiple actors, most of whom do not fall under the Authority's jurisdiction or within its regulatory competence or mandate, as it pursues its public interest objectives and mandates. The challenge faced by national regulators worldwide is that the majority of the most influential actors in the ecosystem, who also create or facilitate the most value for consumers, tend to be beyond their direct and/or effective control.

Vodacom respects the challenge faced by the Authority as it considers how to adapt to a changing ICT ecosystem and Vodacom has no easy answers to offer. However, the Authority should be mindful that "command and control" interventions by national regulators are unlikely to be effective in borderless ICT ecosystems where many of the players in the value chain are unlicensed. Indeed, heavy-handed interventions may have unintended adverse outcomes in the form of depriving users of applications and content and constraining innovation.

Considering the potential impact and challenges from a legal perspective, any regulatory intervention in relation to cybersecurity cannot be approached on an ad hoc basis but must be addressed on a holistic basis.

To this end, the Cybersecurity Response Committee has been established in terms of the South African National Cybersecurity Policy Framework as a dedicated policy, strategy and decision-making body to identify and prioritise areas of intervention and focussed attention regarding cybersecurity related threats. The Cybersecurity Response Committee has also been tasked with the co-ordination of the promotion of cybersecurity measures by all role players (State, public, private sector and civil society and special interest groups) in relation to cybersecurity threats, through interaction with and in conjunction with the Cybersecurity Hub.[1]

[1] See the National Cybersecurity Policy Framework for South Africa, published on 4 December 2015 in the GG39475.

Although the collaboration between various governmental institutions and sectors will be of paramount importance to manage cybersecurity related concerns, the Authority should guard against assuming functions and roles in relation to cybersecurity which are being dealt with dealt with by other regulatory bodies.

3 Part B: Answers to Inquiry Questions

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

Vodacom is of the view that the regulatory functions of the Authority have to evolve as technologies evolve, however, the evolution of technology in and of itself is unlikely to provide sufficient insight or guidance into why and how the Authority's regulatory function has to evolve.

The evolution of technology is one of the many factors that necessitates a re-evaluation of the Authority's regulatory functions. Certainly, the practically complete transition from analogue to digital technology has changed the electronic communications ecosystem in profound ways.

The most important change has arguably been the move from rigid tightly integrated telecommunications networks and services (Telephony, Facsimile, telex, ISDN), to a modular, flexible and dynamic ICT ecosystem compromised out of technology agnostic broadband and over the top applications and content. This has enabled the borderless Internet that has become an almost indispensable part of modern society with all its benefits and risks among which cybersecurity looms large.

The Authority's current mandate aligns broadly with ITU best practice and includes the following core functions:[2]

- Implementing the licensing or authorization framework;
- Promoting competition;
- Interconnecting networks and facilities;
- Implementing universal service/access mechanisms;
- Managing radio spectrum;
- Establishing sufficient safeguards to ensure that consumers are protected against harmful business practices; and
- Minimizing the burden and cost of regulation and contract enforcement.

[2] ITU-infoDev ICT Regulation Toolkit www.ictregulationtoolkit.org/toolkit/1.2

These core functions remain relevant, although in some cases a re-evaluation of how to regulate in a converged ICT ecosystem may be required.

Question 2: *How would you define cybersecurity?*

Vodacom is weary of reinventing the wheel by proposing a novel definition of cybersecurity. Instead Vodacom offers its understanding of the term based on established definitions extracted from the National Cybersecurity Policy Framework, and Cisco based on its practical experience.

Cisco offers the following practical definition of cybersecurity:[3]

> *"Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes."*

Cisco observes that:

> *"Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative."*
>
> *"A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks"*

Cybersecurity is defined in the National Cybersecurity Policy Framework as:

> *"the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them".*

The Memorandum on the objects of the Cybercrimes and Cybersecurity Bill, 2017 defined cybersecurity as:

[3] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

"technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or computer systems against cybercrime, damage or interference"[4].

The above definitions reflect the reality experienced by cybersecurity practitioners for the Authority's consideration:

1. Effective cybersecurity is challenging because number and variety of devices (and programs and networks) that can be attacked;
2. Attackers are innovating all the time to find and exploit security weaknesses. Technology alone is not enough to protect and defend against cyberattacks and people, processes, and technology must all complement one another to create an effective defence from cyber-attacks.

The ITU's 2018 Guide to Developing a National Cyber Security Strategy affirms these practical insights when it identifies risk management as one of the principles of Cybersecurity:

"As with other types of risk, cybersecurity risk cannot be entirely eliminated but they can be managed and minimised.

To address that challenge, the Strategy should encourage entities to prioritise their cybersecurity investments and to proactively manage risk. Depending on an entity's risk appetite, a balance has to be maintained between security measures and potential benefits, considering the dynamic nature of the digital environment. The Strategy should also recognise the need for continuous risk management and facilitate a coherent approach across interdependent entities.

The focus on risk management will also prepare stakeholders for potential security incidents, ensuring the resilience of economic and societal activity in the country. With that in mind, the Strategy should encourage the adoption of business- continuity measures, which include incident and crisis management, as well as recovery plans."[5]

[4] It should be noted that a new version of the Cybercrimes and Cybersecurity Bill [B 6B-2017] was published on 7 November 2018, which is titled "The Cybercrimes Bill 2017". In the Cybercrimes Bill, Chapter 10 titled "Structures to deal with Cybersecurity" has been removed. According to the report of the Portfolio Committee on Justice and Correctional Services, cybersecurity will be dealt with at a later stage in a separate Bill.

[5] the International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity.* Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

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

The Authority lists the following laws:

- The constitution of the Republic of South Africa, 1996 (No 108 of 1996) ("the Constitution");
- The Protection of Personal Information Act, 2013 (4 of 2013) ("POPIA");
- The Electronic Communications and Transactions Act, 2002 (25 of 2002) ("The ECTA");
- The Promotion of Access to Information Act, 2000 (. 2 of 2000) ("PAIA");
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (70 of 2002) ("RICA");
- The Electronic Communications Act (36 of 2005) ("ECA");
- The ICASA Act (13 of 2000); and
- The Cybercrimes and Cybersecurity Bill [B6- 2017][6]

Vodacom believes that in addition to the above, the Authority should also consider the following legislation that may or may not be relevant for ICASA's purposes:

- The Film and Publication Amendment Bill, which is currently before the National Council of Provinces;
- The Consumer Protection Act (No 68 of 2008) ("CPA");
- The Child Justice Act No.75 of 2008;
- Protection of Constitutional Democracy against Terrorist and Related Activities Act (No. 33 of 2004);
- Criminal Procedure Act (No. 51 of 1977);
- Criminal Law Amendment Act (No. 105 of 1997); and

[6] As stated above, this Bill has been replaced by the Cybercrimes Bill [B 6B-2017].

- Criminal Law (Sexual Offences and Related Matters) Amendment (No. 32 of 2007)

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"*

Vodacom notes that question 4.1 and question 4.2 refer to "network integrity". In the context of section 2(q) of the ECA, Vodacom presumes that this is an error and that the Authority's intention is to inquire about "network reliability" as opposed to "network integrity".

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

Cisco[7] defines **Information security** as:

> *"Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection"*

Cisco distinguishes between information security and cybersecurity. Information Security is a crucial part of cybersecurity, but it refers exclusively to the processes designed for data security. Cybersecurity is a more general term that includes Information Security.

In its 2014 report, ITU-D Study Group 1 explained information security's role in cybersecurity as follows[8]:

> *"The important aspect of National Cybersecurity is to preserve the confidentiality, integrity and availability of a national's information. Loss of one or more of these attributes, can threaten the continuity of many Agencies and Organisations.*

[7] https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

[8] Final Report ITU-D Study Group 1, Question 22-1/1 Securing Information And Communication Networks: Best Practices For Developing A Culture Of Cybersecurity, 5th Study Period 2010-2014 Telecommunication Development Sector

Confidentiality: Assurance the certain information are shared only among authorised organisations. The classification of the information should determine is confidentiality and hence the appropriate safeguards.

Integrity: Assurance that the information is authentic and complete. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it).

Availability: Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them."

Network reliability relates to the availability and performance of networks.

In line with the extracts referred to above, Vodacom is of the view that information security should be understood to refer to the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. To this end, the integrity of information conveyed should be protected.

The Authority's mandate in respect of network reliability, as provided for in section 2(q) of the ECA, is aimed to ensure that that licensee's network is available and of a consistent and sufficient quality to meet subscribers needs.

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

In terms of section 4(1) of the ECA, the Authority is empowered to intervene and make regulations with regard to any matter which in terms of ECA and related legislation must or may be prescribed, governed or determined by regulation. The objects of the ECA do not, however, give ICASA an unfettered mandate to intervene and prescribe regulations with respect to information security.

There is no need for ICASA to regulate information security as this task is within the purview and remit of POPIA and the Information Regulator. The Authority has already to an extent addressed the protection of personal information of consumers in terms of the Regulations in respect of the Code of Conduct for Electronic Communications and Electronic Communications Network Services Licensees, which provides consequences for non-compliance by a licensee.

With respect to network reliability, the Authority fulfilled its mandate by means of the Quality of Service regulations in the End-User and Subscriber Service Charter of 2016[9].

Question 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.*

Section 36 of the ECA relates to equipment and electronic communications facilities. Equipment and facilities cannot be stretched to include the complete scope of cybersecurity.

Technical equipment standards deal mostly with hardware and firmware, whereas cybersecurity is to a large extent a holistic software and application and network challenge. In other words, interventions in type approval standards, will provide limited protection from cyberthreats.

In Vodacom's opinion, the Authority's mandate with respect to section 36(2), if it has a cybersecurity mandate, does not extend beyond hardening standards for electronic equipment.

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

The Authority should position and orient its role within South Africa's 2015 National Cybersecurity Policy Framework ("NCPF")[10] .

The danger at this point in time is that the Authority inadvertently takes on a role that is also the responsibility of another government agency. The potential for unintended consequences, inconsistencies and irrationalities arising as a result of one regulator encroaching on the territory of another is self-evident.

[9] Independent Communication Authority of South Africa, notice number 189 of 2016, Government Gazette Number 39898 published on 1 April 2016

[10] State Security Agency, notice number 609 of 2015, Government Gazette Number 39475 published on 4 December 2015

Vodacom recommends the Authority considers the guidance on institutional and organisational coordination in the 2009 ITU draft background paper on Cybersecurity[11]:

> *"The institutional organization and coordination of government institutions for cybersecurity is a vital element of a successful cybersecurity effort. In the context of the role and responsibility of government, it typically involves the organization and coordination of cybersecurity roles and responsibilities among appropriate government institutions in order to carry out the actions that are required to meet cybersecurity objectives. A detailed organization and cooperation framework is essential in order to avoid institutional gaps in the national cybersecurity effort as well as to avoid overlaps in responsibilities which can prove just as damaging. Where overlaps in responsibilities exist, there is often either a tendency towards passiveness by the institutions concerned, or at the other extreme, a potential for the introduction of conflicting regulations and approaches."*

Although Vodacom accepts that the possibility of gaps in the National Cybersecurity Framework remains, such gaps are not readily apparent. Therefore, the first logical step is to analyse South Africa's Cybersecurity Framework and related legislation against international best practice. The next logical step is to assess if any gaps that are identified fall within the Authority's mandate and if the Authority is the agency that is best positioned to fill such gaps. In this regard, it should be noted that the various statutes identified by the Authority in the Discussion Document already creates a legal framework to address some aspects relating to cybersecurity. In Vodacom's view, any additional role that the Authority may play in relation to cybersecurity, if at all, can only be assessed at the stage when cybersecurity is dealt with by the Department of Justice and Correctional Services.

[11] Draft Background Paper on Cybersecurity: The Role and Responsibilities of an Effective Regulator ("**The draft background paper**"). The draft background paper was commissioned by the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division and Regulatory and Market Environment Division. The draft background paper was prepared by Eric Lie, Rory Macmillan and Richard Keck of Macmillan Keck (Attorneys and Solicitors), for the 9th ITU Global Symposium for Regulators held in Beirut, Lebanon (10-12 November 2009). Available on http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on- cybersecurity-2009.pdf.

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

Refer to Vodacom's answer to question 6. The Authority's role in cybersecurity is not clear at this stage. Nevertheless, cybersecurity awareness plays a crucial role in the creation of a cybersecurity culture. In the event that the Authority assumes a role in Cybersecurity awareness, it is important that:

- The Authority's role is in harmony with the NCPF;
- the Authority's objectives are clear;
- the Authority has the resources to perform the role well; and
- the role can be performed without compromising the Authority's ability to deliver on its core functions.

The KCC and the Korea Internet and Security Agency (KISA) planned to have Internet service providers, such as Korea Telecom, monitor the security levels of the computers and other devices used by their customers.

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

Vodacom notes that the KISA example dates from 2009, which is long ago in the fast-evolving world of cybersecurity. It is not clear if:

- the intervention was implemented;
- if it achieved is objectives: and
- if it is still in force.

Bearing in mind that there are more connected devices than people in South Africa, and the vast variety of operating systems and versions, it is clear that the proposed approach will present significant practical challenges and may not be technically feasible. Furthermore, it is not clear that monitoring computer and device security levels will be an effective cybersecurity defence measure.

In Vodacom's opinion monitoring the security levels of computers and devices risks violating end-users' expectations of privacy. Furthermore, POPIA and RICA restrain Network Operators and Internet Service Providers from inspecting the software on connected devices.

The practice of interrogating device and software security levels may well be beyond the scope of Electronic Communication Services ("ECS") as defined in the ECA:

> *""**electronic communications service**" means any service provided to the public, sections of the public, the State, or the subscribers to such service, which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services"*

Question 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?*

Refer to Vodacom's answer to question 8.

This proposal raises serious practical and legal concerns. It is unclear whether the constitutional dispensation in South Korea is similar to that in South Africa, more specifically whether the right to freedom of expression, including the right to receive and impart ideas, and the scope and ambit of such right enjoys the same constitutional protection in South Korea as in South Africa. Vodacom therefore submits that the approach identified cannot be adopted without careful scrutiny.

The practical concerns with this proposal are so severe that Vodacom finds it difficult to imagine that such a proposal was implemented. The Authority should contemplate the following questions:

- What happens if limiting or cutting internet connectivity results in damages or loss of life?
- What happens if the end-user has to pay for a software upgrade?
- Who pays for the data required to download software upgrades?
- What happens if the end-user device cannot run the approved software protection?
- What happens if end-users do not know how to upgrade or download the required software?
- What happens if end-users download malware by accident?
- Who is liable when end-users complain that they do not get the ECS they paid for?

Vodacom urges the Authority to resist the temptation to intervene in end-users' freedom of choice and autonomy by imposing intrusive end-user regulations on licensees. This may infringe upon the consumer's rights to utilise services for which it has paid. Internet connectivity is essential in today's fast paced society and essentially punishing a consumer for not being able to upgrade its software would not be in compliance with South Africa's consumer protection laws, considering the extent of protection that consumers receive in South Africa.

In any event, it would be ultra vires the powers conferred upon the Authority in section 69 of the ECA:

- To require licensees to limit or cut internet connectivity of users with less- than-required software protection; and/or
- To force users to upgrade their existing programs or download new programmes.

The stated purpose of the end-user regulations is recorded in regulation 2 and in broad terms aims to empower and protect consumers and it appears that the Authority may not have taken into account the likely impact of such proposal on users.

Question 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?*

Vodacom is opposed to legislative changes to 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.

Firstly, most software and security programs in use in South Africa are not developed in South Africa. In cases where these businesses are not based in South Africa, the Authority has no mandate or jurisdiction to intervene.

Some software is developed by opensource communities under creative commons licenses. Other software is developed by individuals in their personal capacity. In these cases, there is no business to suspend.

That leaves the small minority of South African software companies alone and vulnerable to their business being suspended by the Authority. Vodacom anticipates at least two perverse outcomes:

1. ICT software innovation in South Africa will freeze. No new ventures will be embarked upon and existing companies will look for ways to relocate outside the Authority's reach.
2. South African software companies will have strong incentives to hide and deny security vulnerabilities. Such a measure could therefore compound the harm which the Authority seeks to prevent and may mean that South Africa will not be able to defend effectively in the event of cyber-attacks.

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

It appears that the Authority accepts that it does not have a mandate to regulate software and the Internet. This means that the Authority would be acting outside of the powers conferred upon t in terms of legislation if it imposed regulations on licenced operators that amount to indirect regulation of the Internet and Software as proposed in questions 8 and 9.

Vodacom would oppose the extension of the Authority's mandate to software and Internet regulation. Vodacom concedes that the Internet poses challenges to regulators. It remains an open question if the Internet can be regulated effectively by national regulators, whether this can be done without inflicting harm on the digital economy and if so, how.

Before extending the Authority's mandate to regulate, Vodacom is of the view that four common sense thresholds should be met:

1. The concern sought to be addressed should be properly understood and defined;
2. The ecosystem must be sufficiently understood to predict the outcomes of regulatory interventions;
3. There must be a reasonable prospect of mitigating the concern through regulations, i.e. any regulatory interventions should be reasonably capable of addressing the concern; and
4. The benefits of regulation (mitigating the concern) must outweigh the direct and indirect cost of interventions (unintended consequences).

At this stage there is no compelling argument to extend the Authority's mandate, while there are substantial concerns about potential adverse unintended consequences, namely:

- Increased regulatory burdens are likely to stifle investment;
- Increased regulatory burdens are likely to stifle innovation and creativity;
- Over-regulation deprives consumers of the freedom to choose;
- Ill-considered regulation may increase the digital divide between South Africa and its international peers; and
- Ill-considered regulation may result in South Africa foregoing the opportunities presented by the Fourth Industrial Revolution.

Question 12 (1): *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?*

For the purpose of answering this question, Vodacom interprets the term "spam" to refer to unsolicited commercial e-mail, and unsolicited bulk e-mail.

Legal Measures

The ECTA, CPA, and POPIA deal with spam.

Section 45 of ECTA provides as follows:

> *"Unsolicited goods, services or communications*
>
> *(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer-*
>
> *(a) with the option to cancel his or her subscription to the mailing list of that person; and*
>
> *(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.*
>
> *(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.*
>
> *(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).*
>
> *(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)."*

From the above it is indicative that the ECTA does not outlaw spam, it merely provides the consumer or recipient with certain rights he or she may enforce against the sender. For example, the consumer may elect to opt-out of the messages. Should the sender continue with the spam messages, after being advised that the recipient no longer wants to receive such messages, the sender will be guilty of an offence.

The Consumer Protection Act ("CPA") deals indirectly with spam through its direct marketing provisions in section 16 (which overlap with spam). Section 16 provides as follows:

"Consumer's right to cooling-off period after direct marketing

It would therefore cover 'physical' spam (such as flyers left in postboxes) and telephone marketing. The CPA also follows an "opt-out" regime and provides every consumer with the right to ask direct marketers to desist from engaging in any direct marketing.

Direct marketing is also dealt with in section 69 of POPIA which has not yet been promulgated. POPIA makes it unlawful for a direct marketer to market directly to a person unless that person has given their prior consent or if they are an existing customer.

The legal position regarding direct marketing will accordingly be changed when section 69 is proclaimed in POPI, from opting out under the ECT Act and CPA to opting in.

Further, the Cybercrimes Bill includes provisions dealing with malicious communications.

Self-regulatory measures

The Internet Service Providers' Association ("ISPA") is the Industry Representative Body in terms of section 71 of ECTA. As such ISPA performs a self-regulation function for its members who subscribe to a Code of Conduct. This Code of Conduct address "spam" among other things. ISPA also deals with consumer complaints on behalf of its members.[12]

Vodacom submits that there are sufficient regulatory measures in place to protect consumers.

Question 12 (2): *To what extent should the Authority play a role in consumer education and outreach programmes?*

Refer to Vodacom's answer to question 6. The Authority's role in cybersecurity is not clear at this stage. Nevertheless, cybersecurity consumer education and outreach programmes can play an important role in the creation of a cybersecurity culture. In the event that the Authority assumes a role in cybersecurity consumer education and outreach programmes, it is important that:

- The Authority's role is in harmony with the NCPF;
- the Authority's objectives are clear;
- the Authority has the resources to perform the role well; and

[12] https://ispa.org.za/about-ispa/

- the role can be performed without compromising the Authority's ability to deliver on its core functions.

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?*

Regulations 9 ,16 and 17 of the EUSSC regulations[9] require licenses to submit network outage reports to the Authority. Vodacom is of the view that these regulations are sufficient to meet the Authority's mandate.

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

Vodacom believes that the standards set in POPIA are sufficient to ensure that customers proprietary network information is protected from unauthorised disclosure.

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

Network security relates to the proactive and reactive protection of networks against unauthorised access, misuse, modification and denial of service.

The Authority should bear in mind that a network cannot be completely secure. It is dangerous to assume that a network is secure. No-one, not even the Authority, can ensure network security. All networks should expect to be attacked, and should expect that some attacks will succeed The safe assumption is that all accessible networks are not secure.

Best practice is to protect networks as much as possible, while remaining vigilant, monitoring networks for security breaches, and taking measures to recover from attacks as fast as possible.

The Authority should further consider that there are many types of networks: international networks, public networks, commercial networks, government networks, private networks, personal networks etc. Some

networks are licensed and some networks are not. Many types of networks are beyond the Authority's mandate and jurisdiction.

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

Vodacom is of the view that the concepts of network security, network reliability, network integrity and information security are related but different concepts, although there may be some areas of overlap, as explained hereunder.

Network reliability relates to the availability and performance of networks. The availability and performance of networks can be influenced by many factors ranging from the weather, to natural disasters, to equipment failures, to sabotage and human errors. Among the factors that can affect network availability are cyber-attacks including denial of service attacks.

Network integrity relates to the loss or corruption of network traffic. The integrity of networks is influenced by many factors ranging from transmission errors, equipment interoperability, equipment errors, human errors and sabotage. Some cyber threats relate directly to network integrity. For example, unauthorized monitoring, insertion, modification, re-ordering, delay or replay of traffic.

As stated before, information security is a component of cyber security. **Information security** relates to the the confidentiality, integrity and availability of information. Network reliability can impact the availability and, to some extent, the integrity of information accessed by means of a network.

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

Vodacom submits that it is premature for the Authority to assume some functions done by SITIC, when cybersecurity will be dealt with at a later stage by the Department of Justice and Correctional Services. The Cybersecurity Hub.

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

Vodacom cannot answer for all ISPs in South Africa, therefore Vodacom's answer is limited to Vodacom's own practices.

Vodacom complies with all the applicable legislation, namely RICA, ECTA, POPIA, and the CPA. Vodacom is also a member of ISPA and subscribes to its code of conduct.

Vodacom has a dedicated cybersecurity office that drives cybersecurity across the company from the network to subscribers, to internal information systems. Vodacom has protection measures in place and also monitors cyberthreats to be able to respond proactively.

Typically, cybersecurity standards can incorporate directives, methodologies and programmes from the following relevant standards bodies around the world:

1. ISO27001;

2. NIST Cyber Security;

3. Cloud Security Alliance;

4. CREST;

5. ISACA.

Vodacom has adopted the ISO27001 framework. Vodacom has developed 48 key controls to secure its network, information systems, and its subscribers.

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

No, RICA does not permit licensees to inspect or monitor the content of communications without appropriate authorization. The implementation of network level filtering would be a contravention of section 14 of RICA.

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?*

In its 2014 report, ITU-D Study Group 1[8] summarised the findings from expert presentations and consultations on botnets as follows:

> *"Botnet compromise of end-user devices is a significant problem that affects all ISPs - large and small.*
>
> *– Botnet malware is rapidly proliferating into end-user devices.*
>
> *– A rapid increase in botnet infections and technological sophistication appears to have been driven by the funding of botnet technology by sophisticated criminal elements.*
>
> *– Botnet malware technology, infections, and the resulting impacts resulting from them are moving faster than ISP industry methods and technologies have, to date, been able to respond to.*
>
> *– Botnets are a complex issue involving both end-user and network issues.*
>
> *– ISP efforts to address botnets must include cooperation and information sharing among ISPs in order to fully address the problem.*
>
> *– There are existing Best Practices (including some IETF RFCs) that address certain aspects of botnets (e.g., concerning responses to spam), but no comprehensive approach has been identified or widely implemented (at least in United States networks).*
>
> *– Botnet detection methods raise issues of end-user privacy which need to be considered when developing approaches to the botnet problem.*
>
> *– The problem of botnets in end-user devices can be substantially improved by implementation of these Best Practices, as applicable, by ISPs serving consumers on residential broadband networks. "*

There are benefits to tracking botnets and information sharing can be helpful. However, end-user privacy issues have to be considered. Vodacom tracks and defends against Botnet activity related to denial of service attacks. However, Vodacom cannot identify and monitor content generating bots or botnets on its network, because of the restrictions imposed in terms of RICA on inspecting content, as referred to above.

Vodacom submits that the Cybersecurity Hub and/or the Cybersecurity Response Committee would be responsible for implementing Botnet Tracking and Detection. A representative of the Minister of

Telecommunications and Postal Services will be on the Cybersecurity Response Committee and can contribute in that regard.

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

Is POPI sufficient to deal with protection of Personal information?

The Protection of Personal Information Act, 4 of 2013 ("POPIA") prescribes a legislative dispensation which is aimed at promoting the protection of personal information processed by public and private bodies. In achieving this, section 2 of POPIA provides that the purpose of the Act is to:

- give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party;
- regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
- provide persons with rights and remedies to protect their personal information from processing that is not in accordance with POPIA ; and
- require all individuals, entities and particularly businesses, to establish new methods of operating with regard to the collection and/or dissemination of any personal information stored in any manner.

Importantly, Data Subjects are given a number of wide-ranging rights in section 5 of POPIA, which include rights to object to the processing of their personal information, rights to request details of any personal information held about them and information about third parties who have or have had access to that information and rights to correct or delete certain personal information.

Consequently, and in light of the above, Vodacom is of the view that POPIA provides the necessary and appropriate mechanisms to deal with the protection of personal information.

What can ICASA do to help enforce POPI in the ICT sector?

Vodacom is supportive of a single Information Regulator which can ensure a consistent approach to privacy and data protection across all sectors of the economy which are based on the founding principles listed in Chapter 3 of POPIA viz., fair and lawful processing, openness; collection limitation; purpose specification; disclosure limitation; data subject participation; data quality; security safeguards and accountability. Such consolidated approach will go a long way in providing guidance, clarity and consistency in the regulatory

and legislative environments pertaining to privacy and data protection. Importantly, this approach will create an overall stable and investment-friendly regulatory and legislative framework, benefiting the South African economy and its people. By implication, any duplication or overlap in jurisdiction with sector-specific regulatory authorities must be avoided, since it will simply result in "forum shopping" or inconsistent approaches in dealing with privacy and data protection matters. The Information Regulator has been tasked with enforcing POPIA. It is therefore unnecessary for the Authority to assume a similar role. Should the Authority nevertheless wish to play an active role in this regard, then the current legislation may have to be amended to clearly indicate how co-operation between the Information Regulator and ICASA will occur. An example of this is found in section 82 of the Competition Act, 89 of 1998 (as amended) which sets out a framework for concurrent jurisdiction between the Competition Commission and other regulatory authorities.

In light of what has been stated above, Vodacom is of the view that ICASA should not play a role in enforcing the provisions of POPIA in the ICT sector

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

Various legislative instruments and codes of conduct deal with Online Child Protection, for instance:

- The Film and Publication Amendment Bill;
- The Cybercrimes Bill; and
- Section 34 of POPIA, which provides for prohibition on processing personal information of children, which is a form of online child protection.

In terms of the NCPF, the Department of Police and SAPS shall be responsible for prevention, investigation and combatting of cybercrime in South Africa which includes the development of cybercrime policies and strategies and should give operation priority to the fight against child sexual/physical abuse material on the internet. There are also a number of society and special interest groups active in this sphere.

Given that Online Child Protection deals with content related matters the Authority's role is limited, and licensees' ability to implement technical countermeasures is limited by RICA and protection of privacy constraints.

If the Authority decides to play are role in Online Child Protection awareness, education outreach programmes. It is important that:

- The Authority's role is in harmony with the NCPF;
- the Authority's objectives are clear;

- the Authority has the resources to perform the role well; and
- the role can be performed without compromising the Authority's ability to deliver on its core functions.

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

The Authority's role in cybersecurity is not clear at this stage. Nevertheless, Vodacom supports the Authority developing its cyber security competence and thought leadership as strategic skill for the future.

It is unlikely that the Authority has sufficient cybersecurity skills and insight at this point in time. A first step would be to determine what skills the Authority needs contribute to South Africa's cybersecurity policy and capacity building. Should the Authority decide to contribute to cybersecurity this should be accommodated in its strategic human resource plan.

In the event that the Authority assumes a role in offering professional cybersecurity training to primary, secondary and tertiary institutions of learning it is important that:

- The Authority's role is in harmony with the NCPF;
- the Authority's objectives are clear;
- the Authority has the resources to perform the role well; and
- the role can be performed without compromising the Authority's ability to deliver on its core functions.

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 how on each of the above category*

South Africans like Mark Shuttleworth and Entersekt have been world leaders is cybersecurity solutions. However, South Africa should be mindful not to forgo the benefits of the best the world has to offer.

It is unlikely that the Authority has sufficient cybersecurity skills and insight at this point in time. A first step would be to determine what skill the Authority needs contribute to South Africa cybersecurity policy and

capacity building. Should the Authority decide to contribute to cybersecurity this should be accommodated in its strategic human resource plan.

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

Vodacom affirms its openness to partner with government within the National Cybersecurity Policy Framework.

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

The question appears to be premature. The Authority should first confirm that it has the requisite core competencies.

It is unlikely that the Authority has sufficient cybersecurity skills and insight at this point in time. A first step would be to determine what skill the Authority needs contribute to South Africa cybersecurity policy and capacity building. Should the Authority decide to contribute to cybersecurity this should be accommodated in its strategic human resource plan.

Question 28: *Is integrity as written in ECA equivalent to security?*

Refer to Vodacom's answer to question 4.1 and question 16.

Vodacom is of the view that integrity as referred to in the ECA is not equivalent to security.

To recapitulate, **Network integrity** relates to the loss or corruption of network traffic. The integrity of networks is influenced by many factors ranging from transmission errors, equipment interoperability, equipment errors, human errors and sabotage. Some cyber threats relate directly to network integrity. For example, unauthorized monitoring, insertion, modification, re-ordering, delay or replay of traffic. Security is one of the multiple factors that can impact network integrity.

There are also many cybersecurity threats, originating from people, applications, software and computers that do to impact the integrity of electronic communications network and electronic communications services as defined in the ECA.

Therefore, integrity as written in the ECA is not equivalent to security.

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

Vodacom's general views on regulatory interventions by the Authority have been set out above, however, Vodacom affirms its willingness to engage with the Authority on regulatory interventions. Vodacom will provide its views on specific regulatory interventions in the appropriate consultative processes.

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

Vodacom runs cybersecurity awareness campaigns from time to time. Recent examples include:

- Tips for holiday cybersecurity;
- Cybersecurity in the fourth industrial revolution;
- How to safely sell goods online;
- How to make your enterprise cyber-resilient;
- Keep your smartphone and mobile data secure; and
- 5 cybersecurity trends affecting business.

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

Vodacom does not believe the Authority has a mandate to place these obligations on licensees and such requirements may also exceed the Authority's powers in terms of the ECA. Vodacom is further of the view that this falls within the scope and mandate of the Cybersecurity Response Committee and/or the Cybersecurity Hub.

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

The Authority may position and coordinate its efforts within the National Cybersecurity Policy Framework.

However, Vodacom remains of the view that the Authority should focus on policy issues with proximity to its core mandates. In any event, at this stage, the Authority's policy-making role with regards to cybersecurity is unclear.

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

There are a number of cybersecurity standards. These can take the form of directives, methodologies and programmes from the following relevant standards bodies around the world:

1. ISO27001;

2. NIST Cyber Security;

3. Cloud Security Alliance;

4. CREST;

5. ISACA;

This list is not comprehensive and there are many other standards that organisations may adopts. Vodacom's principled position is that organisations should have discretion to adopt and customise cybersecurity standards according to their needs.

Vodacom's general views on the Authority's role with regard to cybersecurity standards have been set out above, however, Vodacom affirms its willingness to engage with the Authority on regulatory interventions in this regard. Vodacom will provide its views on specific regulatory interventions in the appropriate consultative processes.

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

Vodacom notes that the Cybercrimes bill was passed by the National Assembly on the 27th of November 2018. According to the report of the Portfolio Committee on Justice and Correctional Services, cybersecurity will be dealt with at a later stage in a separate Bill. Vodacom intends to provide its views on self-regulation in the anticipated parliamentary process.

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

Vodacom has nothing to add at this point in time.

END