CYBERSECURITY POLICY

OF

SOUTH AFRICA

August 2009

TABLE OF CONTENT

1. INTRODUCTION

1.1. Context

1.1.1 The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The objective of the first phase in Geneva was to develop and foster a clear statement of political will and take concrete steps to establish foundations for an Information Society for all, reflecting all the different interests at stake. The objective of the second phase in Tunis was to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the field of internet governance, financing mechanisms, and follow up and implementation of the Geneva and Tunis documents. The WSIS Action line C5 identifies the need to build confidence and security in the use of ICT's.

1.1.2 The Tunis World Summit on the Information Society mandated the ITU to assist in further developing the Global cybersecurity Agenda (GCA), a High-Level Experts Group on cybersecurity (HLEG) was established to support the Secretary General to assist countries to develop cybersecurity intervention identified the following key pillars: organisational structures, legal, technical and procedural measures, international collaboration, and national partnership of stakeholders.

1.1.3 South African does not have a coordinated approach to dealing with cybersecurity in South Africa. Whilst various structures have been established to deal with cybersecurity issues, the structures are inadequate to deal with cyber security issues holistically.

1.1.4 There are various legal provisions addressing cybersecurity in South Africa. However these provisions do not adequately address the legal challenges South Africa faces to effectively deal with cybercrime.

1.1.5 Securing our cyberspace also requires international collaboration given the global interconnection of ICT's. South Africa's does not have extensive international collaboration with other countries to support its cybersecurity initiatives to secure South African cyberspace.

1.1.6 The development of interventions to address cybercrime requires a partnership between business, government and civil society. Unless these spheres of society work together, South Africa's efforts to achieve its cybersecurity policy objective will be severely compromised.

1.1.7 In ensuring a secure South African cyberspace the development, implementation and monitoring of cybersecurity protocols, standards including software and hardware is a critical component. South Africa lags behind other countries in this regard.

1.1.8 In conclusion, the main objective of the cybersecurity policy is to ensure that the South African cyberspace is secure. This policy seeks to provide guidance to the South African public, government and private sector on the matters relating to :

- Institutional mechanisms to support South Africa's cybersecurity policy and strategy.
- Measures to reduce cybersecurity threats and vulnerabilities.
- Fostering collaboration between government, business and civil society.
- Promoting and strengthen international cooperation in support of cybersecurity.
- Building capacity and promoting a culture of cybersecurity.
- Promoting compliance with appropriate technical and operational standards.

1.2. Legislative Framework

1.2.1 The South African cybersecurity policy takes into cognizance existing government policies, legislations, international obligations. The Policy will be informed by and not limited to the following legislations:

- Electronic Communications and Transaction Act, 2002 (Act No.25 of 2002) ("ECT Act");
- Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 ("RICA Act");
- Electronic Communications Security (Pty) Ltd Act, 2002 ("COMSEC Act");
- International Cooperation in Criminal Matters Act, 1996 ("ICCMA");
- The Council of European Convention on Cybercrime, 2001 ("convention"); and
- Criminal Law (Sexual Offences and Related Matters) Amendment Act, no 32 of 2007.
- Films and Publications Act No.65 of 1996
- Films and Publications Amendment Act 34 of 1999
- Films and Publications Amendment Act 18 of 2004

1.2.2 This policy recognizes that there are national procedural and international coordination issues that should be within the expertise of the Criminal Justice system (SAPS, Department of Justice, and NPA) and will be dealt with accordingly by the relevant jurisdiction.

2. POLICY OBJECTIVES

2.1 The aim of this Policy is to establish an environment that will ensure confidence and trust in the secure use of ICTs. This will be achieved through the following objectives:

- To facilitate the establishment of relevant structures in support of cybersecurity;
- To ensure the reduction of cybersecurity threats and vulnerabilities;
- Foster cooperation and coordination between government and private sector;
- Promote and strengthen international cooperation;
- To build capacity and promoting a culture of cybersecurity; and
- Promote compliance with appropriate technical and operational cybersecurity standards.

3. CREATING INSTUTITIONAL CAPACITY TO RESPOND CYBERCRIME AND THREATS

There is undoubtedly an ever increasing threat on South Africa's ICT infrastructure, which is unavoidable since South Africa is connected global economy. In order to combat cyber threats, a collaborative approach both nationally and internationally is required. Organisational structures that can play an important role in this collaborative approach are Computer Security Incident Response Teams ("CSIRT"), National Cybersecurity Advisory Council, Cyber Inspectorate and Law enforcement.

3.1. National Cybersecurity Advisory Council

Currently there is no structure that coordinates strategic policies and interventions. Various sectors have put in place mechanisms and initiatives to deal

with cyber threats and vulnerabilities. There is a need to provide for an integrated and coordinated national approach in cyber related issues in order to complement efforts and avoid duplication of resources. In response to such a need this policy provides for the establishment of the National Cybersecurity Advisory Council to coordinate all cybersecurity initiatives. The policy further provides for the appointment of Council members and their tenure, the Constitution of the Council, terms of reference to be determined by the Minister of Communications in line with this policy**.**

3.1.1 Role of the National Cybersecurity Advisory Council

- Advise the Minister of Communications on policy issues and other matters pertinent to cybersecurity;
- Promote intergovernmental cooperation on cybersecurity matters;
- Promote and encourage coordinated private – public partnerships on issues regarding cyber security in the country;
- Assess the state of national cybersecurity, determine needs and advise on appropriate responses and priorities; and
- Provide oversight regarding the implementation of national cybersecurity initiatives and structures;

3.1.2 Constitution and Tenure of the Council

There will be a total of at least 15 Council members and the council will consist of members appointed ex-officio based on their roles in cybersecurity and members appointed through a public nomination process;

Ex-officio members will consist of representatives of the following state entities:

- Department of Justice
- Department of Defence
- South African Police Services
- National Intelligence Agency
- Comsec
- Department of Communications
- National Prosecuting Authority
- National CSIRT

The Minister of Communications will invite nominations for the other members through the Gazette and media. These members will be appointed by the Minister, on recommendation from an independent selection panel consisting of at least 5 persons, who command public respect for their fair-mindedness, wisdom and understanding of issues pertinent to cybersecurity. The panel will be representative of the security, legal, scientific, academic and business domains;

The independent selection panel will consist of at least 5 persons appointed at the discretion of the Minister of Communications. The panel will be representative of the following fields of expertise ICT security, legal, scientific, academic and business domains.

The Minister of Communications will invite nominations for the panel through the Gazette and media. The Panel will then be appointed from among successful applicants.

- The Minister will appoint a Chairperson from among the members of the Panel.
- The members of the Panel will serve in a part-time capacity for a period of 3 years, such appointment is renewable once.
- The Minister will appoint a Chairperson from among the members of the Council;
- The Council when viewed collectively must be broadly representative of the country. The Council will be composed of academic and legal sectors, science, technology and engineering sector, private sector, public sector and the cybersecurity community; and
- Members of the National Cybersecurity Advisory Council will serve in a part-time capacity for a period of 5 years such appointment which is renewable once.

3.2. CSIRT

A CSIRT (Computer Security Incident Response Team) is a team of dedicated information security specialists that prepares for and responds to cyber security breaches (incidents). It acts as a central point of contact for all cyber security threats and breaches. The CSIRT response is typically in five phases; identify a threat, Analysis a threat, Contain a threat, Mitigate a threat and Report the out

come of the threat to interested parties. This policy provides for the establishment of two categories of CSIRTs; a National CSIRT an entity acting in the national interest serving the private sector, government and civil society and a Government, and a Government CSIRT an entity acting in the interest of Government serving organs of state.

It is crucial to note that CSIRT's do not substitute the existing local and national emergency preparedness, disaster recovery, business continuity or crisis teams, intelligence agencies or any other similar organization. This policy provides for the establishment of a National CSIRT and a Government CSIRT.

3.2.1 National CSIRT

It will be responsible for monitoring threats and coordinating the national response to cybersecurity incidents and coordinate the protection of critical infrastructure against cyber incidents. The National CSIRT will be the entity acting in the national interest serving the private sector, government and civil society. The National CSIRT shall be established by the Department of Communications. The role of the National CSIRT will include the following among others to:

- act as national point of contact for coordination of incident handling activities, including identifying stakeholders and developing public private relationships and collaboration with other CSIRTs to address cybersecurity;
- analyse incidents, vulnerabilities, threats, information about which is disseminated by other CSIRTs, vendors, technology experts etc.;
- create and maintain situational awareness concerning the risk environment of the South African cyber space;
- act appropriately on threat information;
- facilitate interaction both nationally and internationally, including through international memberships to organisations such as Forum for Incident Response and Security Team (FIRST);the Minister will develop policy guidelines to inform such interaction.
- encourage and facilitate the establishment CSIRTs in various sectors; and
- conduct cyber audits, assessments and readiness exercises;
- establish standards and best practices for South Africa for council's consideration.

3.2.2 Government CSIRT

This policy recognises the need for a Government CSIRT, which has been established under the auspices of COMSEC with its objective as monitoring government's cyberpace activities and to identify and protect critical information infrastructure for the organs of state. The role of the Government CSIRT is to:

- Act as a single point of contact for all Organs of State for all cybersecurity matters;
- Coordinate incident response activities between Government departments;
- Facilitate information sharing and technology exchange with Organs of State;
- Facilitate information sharing and technology exchange with the National CSIRT;
- Establish standards and best practices for Organs of State;
- Develop agreed measures to deal with cybersecurity matters impacting on Organs of State; and
- Conduct cyber audits, assessments and readiness exercises in Organs of State.

3.3. Cyber Inspectorate

3.3.1 The ECT Act provides for the establishment of the Cyber Inspectorate. Cyber Inspectorates will contribute towards the creation of a safe, secure cyberspace for the consumer, business and government. Existing law enforcement capacity is insufficient to handle the ever increasing cyber crime. The establishment of a dedicated Cyber Inspectorate team has become an urgent part of the cyber security framework. In addition to providing assistance to law enforcement agencies, the Inspectorate will provide services to the public and business directly as well as the institutions such as Films and Publications Board, Financial Services Board, Consumer Affairs Committee, South African Bank Risk Intelligence Centre etc.

3.3.2 As part of the South Africa's cybersecurity framework, this policy reiterates the provisions of the ECT Act regarding the establishment of the Cyber Inspectorate. The Cyber Inspectorate shall monitor and inspect any websites or activity on an information system in the public domain and report any unlawful activity to the appropriate authority.

3.3.3 The Cyber Inspectorate's role is complementary to the existing law enforcement's insufficient capacity to handle alarming increase in cyber crimes.

3.3.4 It is proposed that a multi discipline task team be appointed to develop an implementation strategy for the Cyber Inspectorate. The task team shall be composed of a dedicated team of volunteers headed by the Department of Communications. The task team will consist of the following departments:

- Department of Justice
- Department of Defence
- South African Police Services
- National Intelligence Agency
- Comsec
- Department of Communications
- National Prosecuting Authority

3.4. Law enforcement

3.4.1 Currently South Africa has insufficient capacity to deal with the ever increasing cyber threats and crime; hence the necessity to significantly increase cybercrime investigation and prevention capability. A number of initiatives to investigate and police cybercrimes are required in order to increase South Africa's overall-capacity to deal with cybercrimes. This policy provides for the development of interventions to strengthen capacity in law enforcement and other agencies that deal with cybercrime. South Africa needs to comply with international best practice and adhere to the European Convention on Cybercrime.

3.4.2 This Policy seeks to enhance law enforcement's capabilities for preventing and prosecuting cybercrime. To this end, the Policy facilitates the development and implementation of cybersecurity efforts to reduce cyber attacks and cyber threats through the following means:

- Capacity development in law enforcement and other agencies that deal with cybercrime should be strengthened;
- Information sharing on matters such a cyber incidents, investigations etc must be shared to improve policing efforts and to ensure risk management in business and society; and

- A programme to share lessons learned from cybercrime and attacks.

4. REDUCING CYBERSECURITY THREATS AND VULNERABILITIES

4.1 In recognition of the challenges that cybersecurity presents for ICT, the ITU has been mandated to develop guidelines and strategies to assist member states with putting in place measures to deal with these issues.

4.2 Threats to Critical Information Infrastructure (CII) can be either intentional or unintentional targeted or non-targeted, and can originate from sources such as dissatisfied employees, criminals, hackers, virus writers, competitors or even espionage operatives. The unavailability of Critical Information Infrastructure (CII) can impact South Africa in terms on its social, economic and national security needs, and this can vary from negligible to severe with potential for serious social, economic and even national security implications. South Africa therefore needs to develop regulations and strategies to identify and protect CII.

4.3 The need for a vigilant approach to information security through continuous mapping, assessing and forecasting of threats and vulnerabilities has been demonstrated by cyber attacks on some critical information infrastructure of some countries. It is imperative that requisite interventions are put in place to ensure South African cyberspace is always secure.

4.4 In order to ensure reduction of cybersecurity threats and vulnerabilities, this policy provides for the:

- Minister of Communications develop regulations to ensure the protection and identification of CII.
- Development strategies and plans to ensure the identification and protection of CII.
- Development of measures to prevent and combat cyber crime through reviewing of relevant legislation for improved security, intelligence gathering, detection of cyber crime, law enforcement, reporting of crime, investigation, digital forensics, prosecution, adjudication and conviction.

5. COORDINATED LOCAL AND INTERNATIONAL PARTNERSHIPS

The fight against cyber threats and crime requires a partnership between citizen, business and government. However given the borderless nature of cyberspace, national efforts are not always adequate. This policy seeks to:

5.1 Foster cooperation and coordination between government, private sector and citizens

5.1.1 The preparedness and robustness of our Cybersecurity defences continually evolves as the technology develops, and due to the borderless nature of the cyber world, governments are increasingly finding that cyber connectivity provides a common point of cooperation which can also be a common point of disaster. Therefore, there is a greater need for strategic partnership between the private sector, civil society and government in build confidence and security in the use of ICT's. Deliberate measures to foster such a partnership will ensure a coordinated approach in developing policies, legislation and other strategies that will ensure the protection of South African cyberspace.

5.1.2 In addition to its own critical information infrastructure, government depends significantly on critical information infrastructure provided by the private sector. The unavailability of such infrastructure due to cyber security incidents would have severe implications to both government and the private sector. It is therefore in the interest of both government and the private sector to ensure that such critical information infrastructure is well protected against cyber incidents and that risk mitigation capacity exists. It is imperative that collaboration between government and the private sector is institutionalized and ensure an environment of trust is created. Such a mechanism will present a platform for sharing information critical to combating cyber crime.

5.1.3 The advances in internet usage has brought with it challenges. These challenges are cyber crimes activities such as child pornography, fraud, identity theft etc. These crimes threaten National Security, the economic and the general well being of the citizens of the Republic. This is a world wide phenomenon and is not unique to South Africa. These challenges are not limited to the Internet but can be found in the mobile usage. The role of ICT in the social economic development of any country is widely acknowledged.

5.1.4 This Policy provides for the establishment of mechanisms to facilitate for cooperation and coordination between government and private sector. The objective of these platforms is to ensure that information sharing takes place in the interest of securing South Africa's cyberspace.

5.2 Promote and strengthen international cooperation

5.2.1 Global nature of cyberspace means that a risk or cyber attack has a potential of being a risk or cyber attack of the globally. Therefore, international collaboration is critical in securing cyberspace nationally and globally. Such efforts must ensure that effective cooperation at all levels of society public, government and business. There is a need to develop a framework of engagement at multilateral level that will ensure South Africa:

- Effectively participate, influence and implements the Global Cybersecurity Agenda.
- Supports collaborative efforts of institution such a Forum for Incident Response and Security Team FIRST) and International Multilateral Partnership Against Cyber-Terrorism (IMPACT).
- Supports and promotes the development of international understanding and consensus on cybersecurity matters.
- Facilitate that South Africa complies with international agreements and commitments.
- Ensure that South African cyberspace not only meets international standards and best practices but also guarantees a sense of security.
- In this regard, this Policy seeks to ensure cooperation in Cybersecurity regionally, continentally and globally in accordance with South Africa's foreign policy strategic objectives and global governance.

6 CONTINOUS INNOVATION, SKILLS DEVELOPMENT AND COMPLIANCE

The dynamic nature of Cybercrime has necessitated the continuos development of R & D capabilities and requisite skills to mitigate cybercrime. This policy seeks to:

6.1 To build capacity and promoting culture of Cybersecurity

6.1.1 Resolution 57/239 0f 2002 of the United Nations identifies the following elements for creating a global culture of cybersecurity: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment;

6.1.2 Cybercrime and threat affect all spheres of our society, there is a need to develop capacity to deal with these issues such as developing specialized

cybersecurity programmes and careers, developing a culture of security sensitiveness in cyberspace, developing R&D capabilities, development of mechanisms to coordinate and share information on cyber threats etc;

6.1.3 To this end, there is need to develop interventions that will ensure South Africa has requisite capacity to deal with cybercrime. The policy recognises a need for synergy between the various institutions such as tertiary institutions, Meraka E- Skills Institute, Information Security Centre of Competence (ISCOC) and any other players;

6.1.4 Furthermore, multi lingo public awareness progammes across all media platforms is essential; and

6.1.5 This policy provides for:

- the stimulation and sustained distinction in research while simultaneously generating highly qualified human resource capacity in order to impact meaningfully on key national and global areas of knowledge; and
- the development of strategies that will ensure South Africa has the capacity to continuously deal with cyber threats and crimes. The strategies must address capacitating law enforcement agencies, the judiciary, cyberspace technocrats and public in general.

6.2 Promote compliance with appropriate technical and operational cybersecurity standards

6.2.1 Cybersecurity has progressed from a novelty to a global concern. Compliance with appropriate technical and operational cybersecurity standards is a necessity, since sensitive information is increasingly stored on computers and networks. In South Africa, it is necessary to employ Cybersecurity standards to ensure conformity and consistency in practices between the relevant stakeholders and the cybersecurity community. In addition, cybersecurity standards guide government, private sector and the cybersecurity practitioners.

6.2.2 An ICT security standard roadmap was developed by the ITU. This roadmap assists in the development of security standards by bringing together information about existing standards and current standards work.

6.2.3 As a country, South Africa not only has to monitors and participates in the development of relevant standards but has to align its standards to international best practices. In South Africa, the SABS (StanSA1), is the leading standard-developing body.

6.2.4 This policy promotes;

- compliance with appropriate technical and operational cybersecurity standards. Where appropriate the Minister will regulate compliance with such standards.
- the development of legal and regulatory frameworks that support cybersecurity standards.
- the creation of standards that will ensure a safe and secure environment that will enable the growth of e-commerce and an inclusive information society.

6.3 Promote E-Commerce and the information society

6.3.1 The transition of global economies has significantly shifted from paper-based to an advanced electronic commerce. Electronic commerce does not recognize national borders or time zones, nor is it limited by physical distance.

6.3.2 Rather it depends on the existence of common software architecture, standard protocols and secure communication processes.

6.3.3 E-commerce has the potential to transform the global market and facilitate relationships between nations; it enables exchange of information, products, services and payments for commercial and communications purposes between people, this range from business to business, business to consumers, government to business and government to consumers.

6.3.4 The information society is described by WSIS Plan of action as people centred, inclusive and developmental oriented where every individual can icreate, utilise, and share information and knowledge using information communication technologies to achieve their full potential in promoting their sustainable development and improving the quality of their lives.

6.3.5 This cybersecurity policy is guided by the following principles:

[1] Standards South Africa

- It supports business procedures that are in harmony with generally accepted international commercial practices. These include fair, non-discriminatory and transparent taxation systems.
- It is committed to creating a favourable environment for open and fair participation in electronic commerce.
- It aims to comply with relevant law enforcement measures that may be developed and implemented to limit and prevent cyber crimes, including money laundering. This should extend to the protection of intellectual property rights, encryption, patents and the protection of privacy.

7 BENEFITS OF CYBERSECURITY

7.1 This policy presents the country with a unique opportunity of ensuring that South Africa builds confidence and security in the use of ICT's. The policy will achieve the following benefits:

- Ensure confidence and security in the use of ICT's by government, business, society and the individual; Achieving higher rates of investment;
- Create a safe and secure cyberspace;
- Contribute to economic growth and competitiveness of South Africa;
- Ensure the identification and protection of critical information infrastructure; and
- Ensure a business enabled e-commerce environment.

8 CONCLUSION

8.1 This Policy is guided by the unique challenges that the country faces. In addressing these challenges, the Policy seeks to make South Africa global leader in harnessing ICT's for socio-economic development. This Policy will assist the Government to meet its commitments to the people of South Africa as well as to the global community, especially the developing world.

8.2 It is Government's intention to continue on an open and inclusive partnership, taking along all stakeholders in an effort to build confidence and security in the use of ICT's.

9 ACRONYMS

Acronyms	
CSIRT	Computer Security Incident Response Team
CII	Critical Information Infrastructure
ECT	Electronic Communications and Transactions Act
COMSEC Act	Electronic Communications Security Act
FPB	Films and Publications Board
FIRSTS	Forum for Incident Response and Security Team
GCA	Global Cybersecurity Agenda
HLEG	High Level Expert Group on Cybersecurity
ISCOS	Information Security Centre of Competence
ICCMA	International Cooperation in Criminal Matters Act
IMPACT	International Multilateral Partnership Against Cyber Terrorism
PPP	Public Private Partnership
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act, No. 70 of 2002
SABS	South African Bureau of Standards
STANSA	
SABRIC	South African Banking Risk Intelligence Centre
TIA	Technology Innovation Agency
WSIS	World Summit on the Information Society
WTSA	World Telecommunications Standard Assembly

10 DEFINITIONS

"Council of European Convention on Cybercrime" means the European Council treaty on Cybercrimes which is open to other countries.

"Critical Information Infrastructure" means All ICT systems, data systems, data bases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the State;

"Critical Information Infrastructure" means All ICT systems, data systems, data bases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the State;

"Cybersecurity" means the protection of data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in networks that are connected to the Internet.

"Independent Selection Panel" means panel tasked to recommend to Minister of Communications members of the National Cybersecurity Advisory Council who are not Ex-officio members;

"UN General Assembly Resolution 56 /183, 2001" means a UN General Assembly Resolution that endorsed the organization of the World Summit on the Information Society (WSIS), a Summit which focused on bridging the digital divide by promoting development through access to information, knowledge and communication technologies;
"UN General Assembly Resolution 57 / 239 of 2002" means a UN General Assembly Resolution that endorsed the creation of a global culture of cybersecurity;