Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID-AFRIKA

Vol. 536 Pretoria, 19 February / Februarie 2010 No. 32963

CONTENTS • INHOUD

No.		Page No.	Gazette No.
	GOVERNMENT NOTICE		
Communications, Department of			
Government Notice			
118	Electronic Communications Act (36/2005): Notice of intention to make South African National Cybersecurity Policy.	3	32963

GOVERNMENT NOTICE

DEPARTMENT OF COMMUNICATIONS

No. 118 **19 February 2010**

NOTICE OF INTENTION TO MAKE SOUTH AFRICAN NATIONAL CYBERSECURITY POLICY

I, Gen (Ret) Siphiwe Nyanda, Minister of Communications, hereby give notice of the intention to make South African National Cybersecurity Policy in the schedule in terms of section 3(1) of the Electronic Communications Act, 2005 (Act No. 36 of 2005).

Interested persons are hereby invited to furnish written submissions on the proposed Cybersecurity Policy, within 30 calendar days of the date of publication of this notice at any of following addresses:

For attention:	Mr. Jabu Radebe Chief Director, Cybersecurity Department of Communications;
post to:	Private Bag X860 Pretoria 0001;
or deliver to:	First Floor, Block E iParioli Office Park 399 Duncan Street Hatfield, Pretoria;
or fax to:	(012) 427 7057;
or e-mail to:	cybersecurity@doc.gov.za

Please note that submissions received after the closing date may be disregarded.

Mr. Jabu Radebe can be reached at tel. (012) 427 8038 for any enquiries.

Gen (Ret) Siphiwe Nyanda
Minister of Communications

the doc

Department:
Communications
REPUBLIC OF SOUTH AFRICA

DRAFT

CYBERSECURITY POLICY

OF

SOUTH AFRICA

19 February 2010

TABLE OF CONTENT

1 INTRODUCTION 3

1.1 Context 3

1.2 Legislative Framework 4

2 POLICY OBJECTIVES 4

3 CREATING INSTUTITIONAL CAPACITY TO RESPOND TO CYBERCRIME AND THREATS 5

3.1 National Cybersecurity Advisory Council 5

3.2 COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT) 6

4 REDUCING CYBERSECURITY THREATS AND VULNERABILITIES 8

5 COORDINATED LOCAL AND INTERNATIONAL PARTNERSHIPS 8

5.1 Foster cooperation and coordination between government, private sector and citizens. 8

5.2 Promote and strengthen international cooperation 8

6 CONTINOUS INNOVATION, SKILLS DEVELOPMENT AND COMPLIANCE 9

6.1 Promote compliance with appropriate technical and operational Cybersecurity standards 9

7 BENEFITS OF CYBERSECURITY 9

8 CONCLUSION 10

9 ACRONYMS 11

10 DEFINITIONS 12

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 the Geneva 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 International Telecommunication Union (ITU) to assist in further developing the Global Cybersecurity Agenda (GCA), a High-Level Experts Group (HLEG) on Cybersecurity 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 Africa does not have a coordinated approach in dealing with Cybersecurity. Whilst various structures have been established to deal with Cybersecurity issues, the structures are inadequate to deal with Cybersecurity 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. Bridging the technology/law divide remains a fundamental challenge.

1.1.5 Securing our cyberspace also requires international collaboration given the global nature of ICT's. South Africa does not have extensive international collaboration with other countries to support its Cybersecurity initiatives to secure its 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 ensure a secured cyberspace 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 are a critical component. South Africa lags behind other countries in this regard.

1.1.8 It is apparent given the issues identified that the implementation of this policy goes beyond the mandate of the Department of Communications. In recognition of the different mandates played by the various Departments, it is inconceivable for any one Department to implement all the issues identified in this policy. The success thereof this policy depends on the collective efforts of all the relevant Government Departments, the implementation of the policy will be coordinated by the Department of Communications.

1.2 Legislative Framework

1.2.1 In South Africa, there are various pieces of legislation administered by different Government Departments that impact on Cybersecurity. This policy acknowledges various legislations, the policy also acknowledges that the South African Cybersecurity legal framework will not be a homogeneous document but a collection of legislations, which when viewed collectively will ensure that South African cyberspace is secure.

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:

- Facilitate the establishment of relevant structures in support of Cybersecurity;
- Ensure the reduction of Cybersecurity threats and vulnerabilities;
- Foster cooperation and coordination between government and the private sector;
- Promote and strengthen international cooperation on Cybersecurity;
- Build capacity and promoting a culture of Cybersecurity; and

- Promote compliance with appropriate technical and operational Cybersecurity standards.

3 CREATING INSTUTITIONAL CAPACITY TO RESPOND TO CYBERCRIME AND THREATS

The increase in uptake and usage of the internet will contribute significantly to economic growth. This however is likely to lead to an increase in cybercrime. In order to ensure that South African cyberspace is secured, South Africa should establish appropriate organisational structures to support our national Cybersecurity initiatives:

3.1 National Cybersecurity Advisory Council

Currently there is no structure that coordinates Cybersecurity policies and interventions at operational and strategic levels. There is a need to provide for an integrated and coordinated national approach in Cybersecurity related issues. In response to such a need, this policy provides for the establishment of a National Cybersecurity Advisory Council (NCAC) to coordinate all Cybersecurity initiatives at a strategic level.

3.1.1 Role of the National Cybersecurity Advisory Council (NCAC)

The role of the NCAC is to:

- Advise the Minister of Communications on policy issues and other matters pertinent to Cybersecurity;
- Promote intergovernmental cooperation on Cybersecurity matters;
- Promote and encourage coordinated public-private 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.

3.2 COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT)

This policy provides for the establishment of a National CSIRT, and various sector CSIRTs including a Government CSIRT. The National CSIRT will identify, analyse, contain, mitigate and report the outcome of the threats to relevant parties. Sector CSIRTs will coordinate activities in their respective sectors and communicate with the National CSIRT.

3.2.1 National CSIRT

The National CSIRT shall be established by the Department of Communications in conjunction with relevant Government Departments, the private sector and civil society. The role of the National CSIRT will include the following:

- Act as national point of contact for the coordination of incident handling activities, including identifying stakeholders and developing public private relationships and collaborating with sector CSIRTs;
- Analyse incidents, vulnerabilities, threats, and other information;
- Disseminate the information to other by sector CSIRTs, vendors, technology experts etc.;
- Create and maintain situational awareness concerning the risk environment of South African cyberspace;
- Act appropriately on threats;
- Facilitate interaction, both nationally and internationally, including through international memberships to organisations such as the Forum for Incident Response and Security Teams (FIRST); and, in consultation with the Minister, develop policy guidelines to inform such interaction;
- Encourage and facilitate the establishment of sector CSIRTs;
- Conduct cybersecurity audits, assessments and readiness exercises; and
- Establish standards and best practices for South Africa for NCAC's consideration.

3.2.2 Government CSIRT

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 cybersecurity audits, assessments and readiness exercises in Organs of State.

3.2.3 Sector CSIRT

The role of the sector CSIRTS is to:

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

4 REDUCING CYBERSECURITY THREATS AND VULNERABILITIES

4.1 There is a need for a vigilant and proactive approach to information security through continuous mapping, assessment and prediction of potential threats and vulnerabilities. South African cyberspace will be secured through the:

- Development of proactive measures for the prevention and combating of cybercrime;
- Development of technical, regulatory and legal measures for the reduction of Cybersecurity threats and vulnerabilities; and
- Identification and protection of critical information infrastructure (CII).

5 COORDINATED LOCAL AND INTERNATIONAL PARTNERSHIPS

The fight against cybercrime and threats requires a partnership between public sector, private sector and civil society. However, given the borderless nature of cyberspace, national efforts are not always adequate.

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

Cooperation and coordination between public sector, private sector and civil society will be fostered at strategic and operational level by the National Advisory Council and the National CSIRT.

5.2 Promote and strengthen international cooperation

5.2.1 Recognising the need for global collaboration on technical and legal matters in order to curb cybercrime, South Africa will become member and participate in the following international organisations subject to existing international agreements and the Constitution.

- Forum for Incident Response and Security Teams (FIRST);
- International Multilateral Partnership Against Cyber-Terrorism (IMPACT); and
- Any other relevant international fora on matters of Cybersecurity.

6 CONTINOUS INNOVATION, SKILLS DEVELOPMENT AND COMPLIANCE

The dynamic nature of cybercrime requires the continuous development of Research and Development (R&D) capabilities and requisite skills to mitigate cybercrime. This policy provides for the:

- Building capacity to address specific requirements of law enforcement, judiciary, security practitioners and civil society; and
- Promoting a culture of Cybersecurity through the development of programmes that address the specific needs of business, government and users in general.

6.1 Promote compliance with appropriate technical and operational Cybersecurity standards

This policy provides for:

- Compliance with appropriate technical and operational Cybersecurity standards. Where appropriate and in consultation with the National Cybersecurity Advisory Council, the Minister shall enforce compliance with such standards;
- The development of legal and regulatory frameworks that support Cybersecurity ; and
- 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.

7 BENEFITS OF CYBERSECURITY

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 implementation of the policy leading to a secure cyberspace, will achieve the following benefits:

- Confidence and security in the use of ICT's by Government, business, society and the individual;
- higher rates of investment;
- A safe and secure cyberspace;
- Economic growth and competitiveness of South Africa; and

- Identification and protection of critical information infrastructure; and
- Secure 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 a 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 trust in the secure use of ICT's.

9 ACRONYMS

Acronyms	
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Teams
FIRST	Forum for Incident Response and Security Team
GCA	Global Cybersecurity Agenda
HLEG	High Level Expert Group on Cybersecurity
ICT	Information and Communications Technology
IMPACT	International Multilateral Partnership Against Cyber Terrorism
ITU	International Telecommunication Union
NCAC	National Cybersecurity Advisory Council
UN	United Nations

10 DEFINITIONS

"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;

"Computer Security Incident Response Team (CSIRT)" is a team of dedicated information security specialists that prepares for and responds to cyber security breaches (incidents)

Cybercrime" means cyber crimes as defined in chapter XIII of the ECT Act (No.25 of 2002

"Cybersecurity" is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user assets.

Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and a totality of transmitted and/or stored information in the cyber environment.

"Cyberspace" means a physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.

"Department" means Department of Communications;

"Organ of State" means an Organ of the State as defined in section 239 of the Constitution; and

"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.