
GOVERNMENT NOTICE

DEPARTMENT OF COMMUNICATIONS

No. 118

19 February 2010

NOTICE OF INTENTION TO MAKE SOUTH AFRICAN NATIONAL CYBERSECURITY POLICY

I, Gen (Ret) Sphiwe 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;

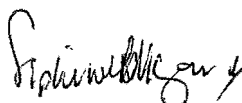
or deliver to: First Floor, Block E
iParioli Office Park
399 Duncan Street
Hatfield, Pretoria;

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) Sphiwe 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 INSTITUTIONAL 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	CONTINUOUS 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