CONFIDENTIAL

DRAFT

NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA

May 2011

A NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA

CONTENTS

EXECUTIVE SUMMARY **3**

A. ACRONYMS **5**

B. DEFINITIONS **6**

1. INTRODUCTION 9
2. THE SOUTH AFRICAN CONTEXT 12
3. PURPOSE OF THE NCPF 15
4. NATIONAL CYBERSECURITY POLICY OBJECTIVES 16
5. CREATING INSTUTITIONAL CAPACITY TO RESPOND TO CYBERSECURITY IMPERATIVES 17
6. COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT) 17
   - *6.1 NATIONAL CSIRT* ..... ***Error! Bookmark not defined.***
   - *6.2 GOVERNMENT CSIRT* ..... ***Error! Bookmark not defined.***
   - *6.3 SECTOR CSIRTs* ..... ***Error! Bookmark not defined.***
7. NATIONAL CRITICAL INFORMATION INFRASTRUCTURE (CII) PROTECTION 21
8. CRYPTOGRAPHY 22
9. IDENTITY MANAGEMENT 22
10. PROMOTE AND STRENGTHEN LOCAL AND INTERNATIONAL COOPERATION 24
11. CAPACITY DEVELOPMENT, RESEARCH AND DEVELOPMENT 25
12. TECHNICAL AND OPERATIONAL STANDARDS COMPLIANCE 27
13. ROLES AND RESPONSIBILITIES OF RELEVANT ORGANS OF STATE 27
14. CONCLUSION 29

ANNEXURE: **30**

A. SYNOPSIS OF NATIONAL CYBERSECURITY IMPLEMENTATION SCHEDULE: 30

B. REFERENCE MATERIAL 32

A NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA

EXECUTIVE SUMMARY

Information and Communications Technologies (ICT's) are indispensible in modern society. The interconnectivity of computer networks contributes significantly to economic growth, education, citizens' participation in social media and many others.

This new electronic environment is commonly known as **cyberspace**. However, this dependence of the daily functioning of society on information communication technology solutions has led to a concomitant need for the development of adequate security measures. **It is generally accepted by the international community and the United Nations that the threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a real and very serious security risk confronting all nations.**

The numerous cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of international and also local security threats. For this reason, the cyber threats need to be addressed at both the global and national levels.

Given the seriousness of cyberthreats and of the interests at stake, it is therefore imperative that the comprehensive use of information communication technology solutions be supported by a high level of security measures and be embedded in a broad and sophisticated cybersecurity culture.

National cybersecurity is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's security, economy and wellbeing. Ensuring the security of a country's cyberspace comprises a range of activities at different levels.

The danger that cybersecurity threats pose, is very real.

The JCPS Cluster has consequently developed as part of its mandate and obligations under Outcome 3: All people are and feel safe in South Africa, a National Cybersecurity Policy Framework (NCPF) to comply with Output 8 of Outcome 3: which requires the development and implementation of a cybersecurity policy and the development of capacity to combat and investigate cybercrime that seeks to promote in particular the following:

- Measures to address national security threats in terms of cyberspace;
- Measures to promote the combating of cybercrime;
- Measures to build confidence and trust in the secure use of ICT;
- The development, review and updating existing substantive and procedural laws to ensure alignment.

The NCPF is intended to provide a holistic approach pertaining to 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. This framework will be supported by a National Cybersecurity Implementation Plan which will be developed in consultation with relevant stakeholders, identifying roles and responsibilities, timeframes, specific performance indicators, and monitoring and evaluation mechanisms. The development and large-scale implementation of a system of security measures as implemented elsewhere in the world will form part of the National Cybersecurity Implementation Plan.

Through the NCPF, the JCPS Cluster seeks to address the following:

- The development and implementation of a Government led, coherent and integrated cybersecurity approach to address cybersecurity threats;
- The promotion of a cybersecurity culture and compliance with minimum security standards;
- Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;
- Ensure the protection of national critical information infrastructure;
- The establishment of public-private partnerships for national and action plans in line with the NCPF; and
- Ensure a comprehensive legal framework governing cyberspace.

A: ACRONYMS

CSIRT	Computer Security Incident Response Teams
DoC	Department of Communications
DoJ&CD	Department of Justice and Constitutional Development
DoD&MV	Department of Defence and Military Veterans
DST	Department of Science and Technology
FIRST	Forum for Incident Response and Security Teams
GRC	Governance, Risk Management and Compliance
ICT	Information and Communications Technology
ICASA	Independent Communications Authority of SA
ISPs	Internet Service Providers
JCPS	Justice, Crime Prevention and Security Cluster
NCPF	National Cybersecurity Policy Framework
NPA	National Prosecuting Authority
PKI	Public Key Infrastructure
SSA	State Security Agency
SAPS	South African Police Service

NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA

B: DEFINITIONS

In the context of this policy,

"National 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 Republic[1];

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

"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;

"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;

"Cyber warfare" means actions by a nation/state to penetrate another nation's computers and networks for purposes of causing damage or disruption[2];

"Cyber espionage" means the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of

---

[1] This relates to critical services such as the economy, social services and law enforcement (inclusive of the justice system and state security).

[2] This definition do not purport to be a universally accepted definition in a UN reference framework.

classified nature), from individuals, competitors, rivals, groups, Governments and enemies for personal, economic, political or military advantage[3];

"Cyber terrorism" means use of internet based attacks in terrorist activities by individuals and groups, including acts of deliberate large scale disruptions of computer networks, especially computers attached to the internet, by the means of tools such as computer viruses[4];

"Cybercrime" means illegal acts, the commission of which involves the use of information and communication technologies;

"ICT" (Information and Communication Technologies) mean any communications device or application including radio, television, cellular phones, satellite systems, computers, network hardware and software and other services such as videoconferencing ;

"Information society" means people-centred, inclusive and development-oriented information, where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and people to achieve their full potential in promoting their sustainable development and improving the quality of their life.

"Malware" means malicious software, and is programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behaviour. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or dangerous software or program code. Malware's most common pathway from criminals to users is through the Internet: primarily by e-mail and the World Wide Web. (Symantec published a report in 2008 indicating that "the release rate of malicious code and other unwanted programs may be exceeding

---

[3] **Ibid.**

[4] **Ibid.**

that of legitimate software applications." According to F-Secure, "As much malware [was] produced in 2007 as in the previous 20 years altogether." [5]).

"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.

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

"**Phishing**" indicates the fraudulent way of attempting to acquire sensitive information such as usernames, passwords and credit card details by someone masquerading as a trustworthy entity in an electronic communication, to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

[5] **http://en.wikipedia.org/wiki/Malware**

A NATIONAL CYBERSECURITY POLICY FRAMEWORK FOR SOUTH AFRICA

1. INTRODUCTION

1.1 A number of strategic interventions and tactical interventions have been successfully implemented over the past few years and other interventions are in the process of being implemented within the Justice, Crime Prevention and Security (JCPS) Cluster in the fight against crime with the objective of making South Africa Safe. As part of Government's Outcome based priorities, the JCPS Cluster signed on 24 October 2010, the JCPS Delivery Agreement, relating to Outcome 3: **"All People in South Africa Are and Feel Safe".** This Outcome focuses on certain areas and activities, clustered around specific Outputs, where interventions will make a substantial and a positive impact on the safety of the people of South Africa. One such area relates to Output 8: which requires the development and implementation of a Cybersecurity Policy and the development of capacity to combat and investigate cybercrime. In line herewith, this document therefore sets out a National Cybersecurity Policy Framework (NCPF) for South Africa.

1.2 It is generally accepted that Information and Communications Technologies (ICT's) have become indispensible in modern society. The increased interconnectivity of computer networks and the expansion of broadband including mobility are contributing significantly to economic growth, digital integration, education, electronic governance, citizens' participation in governance and many others. This new electronic environment is commonly known as cyberspace. It has created a "global village" with instantaneous communication possible between persons on the opposite sides of the world. The Cybersecurity Policy Framework therefore recognises that cybersecurity threats and the combating thereof have both a national as well as an international context.

1.3 Cyberspace comes with new types of challenges to the governments of the world. It introduces a further dimension to National Security. It is a borderless platform that enables more sophisticated threats such as, cybercrime, cyber terrorism, cyber war and cyber espionage. The numerous cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of international and also local security threats. The acknowledgment that such attacks pose a threat to international security reached new heights in 2007 owing to the first-ever co-ordinated cyber attack against an entire country (Estonia) and also because of large-scale cyber attacks against information systems in many other countries as well. The co-ordinated cyber attacks against government agencies, banks, and media and telecommunications companies in a single country (Estonia) demonstrated that the vulnerability of a society's information Infrastructure is an aspect of national security that needs attention in all countries. There are views that internet is becoming more and more militarized. The problem is very specific to malware being distributed through terror groups.[6]

1.4 The recurrence and growing incidence of cyber attacks indicate the start of a new era in which the security of cyberspace acquires a global dimension and the protection of National critical information Infrastructure must be elevated, in terms of national security, on a par with traditional defence interests.

1.5 National cybersecurity is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's security, economy and wellbeing. Ensuring the security of a country's cyberspace thus comprises a range of activities at different levels. Toward this end, the most important policy domains include reducing the vulnerability of cyberspace, preventing cyber threats and attacks in the first instance and, in the event of an attack, ensuring a swift recovery of the functioning of information systems. Thus, a cyber strategy must appraise the vulnerability of a country's critical infrastructure, devise a system of preventive measures against cyber attacks, and decide upon the allocation of tasks relating to cyber security management at the national level.

[6] Beeld: 12 May 2011, article entitled Web raak al hoe meer militaristies, sê joernalis.

Moreover, it is also important to improve the legal framework against cyber attacks, to enhance international and institutional co-operation, and to raise public awareness and develop training and research programmes on cyber security.

1.7 The above threats necessitate a comprehensive and all-encompassing approach in dealing with cyber threats. In short, a cybersecurity culture, driven in main by the State, is critical to ensure that citizens take advantage of the information age, whilst remaining conscious of the threats and vulnerabilities of cyberspace. The NCPF recognises the need to balance, on the one hand, the risks associated with the use of information systems and, on the other hand, the indispensability of extensive and free use of information technology to the functioning of open and modern societies. The growing threats to cyber security should not hinder the crucial role of information and communications technology in stimulating the growth of economies and societies.

1.8 In response to the above challenges, Governments worldwide have established policies and structures that govern interaction and collaboration between Government, private sector, academia and civil society in an effort to prevent, react to, combat and mitigate cybersecurity vulnerabilities and attacks.

1.9 The NCPF recognises that the State is charged with implementing a Government led, coherent and integrated cybersecurity approach which, amongst others, will:

a) Promote a cybersecurity culture and demand compliance with minimum security standards;
b) Strengthen intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;
c) Establish public-private partnerships for national and international action plans;
d) Ensure the protection of national critical information infrastructure; and

e) Promote and ensure a comprehensive legal framework governing cyberspace.

1.10 This framework is intended to implement an all encompassing approach pertaining to all the role players (State, public, private sector, civil society and special interest groups) in relation to Cybersecurity. This framework will be supported by a National Cybersecurity Implementation Plan which will be developed in consultation with relevant stakeholders, identifying roles and responsibilities, timeframes, specific performance indicators, and monitoring and evaluation mechanisms. The development and large-scale implementation of a system of security measures as implemented elsewhere in the world will form part of the National Cybersecurity Implementation Plan.

2. THE SOUTH AFRICAN CONTEXT

2.1 South Africa has become dependent on the Internet to govern, to conduct business and for social purposes. The Internet has become indispensable to many South Africans and will continue to be, as more people join the information highway. Taking into consideration the increase in national and international bandwidth in South Africa, cybercrimes and threats are and will continue to increase. These Cybercrimes and threats have the potential to impact on our national security and economy.

2.2 Currently there are various pieces of legislation, some with overlapping mandates administered by different Government Departments and whose implementation is not coordinated. Furthermore, the legislation when viewed collective to don't adequately address South Africa's Cybersecurity challenges.

2.3 The absence of an aligned legal and regulatory framework, and the challenge of uncoordinated Cybersecurity efforts is not unique to South Africa, other jurisdiction are faced with the same challenges.

2.4 Statistics in 2011 indicate that South Africa remains in the top three of countries that are targeted for phishing purposes, the other two countries are the USA and the UK. It was noted that the number of unique phishing attacks

identified by the RSA authorities (aimed at RSA instances and individuals from outside the RSA worldwide) in February 2011 was 18,079 – an 11 percent increase from January. This represents, for the first time in nearly a year, that the total number of phishing attacks in a single month reached over 18,000. The U.S. remained the top hosting country for these attacks in February – hosting two out of every three phishing attacks identified by the RSA. The countries that have consistently been among the top five hosts over the last six months include the U.S., UK, Canada and Germany. For over a year now (13 consecutive months), the U.S.,UK and South Africa have remained the top three targets of mass phishing campaigns. The U.S., while still remaining the top targeted country in February, witnessed a nine percent decrease in attack volume. The UK saw a seven percent increase while South Africa remained unchanged since January, suffering a 7.5 percent of the attack volume. [7] [redacted] addition to phishing, other e-Crime incidents in the RSA has increased to the [redacted] illions of rands. These cybercrimes inciden[redacted] increa[redacted] monetary value [redacted] Road Accident Fund (through the use of key loggers) to the value of about [redacted] a Gauteng/ ABSA electronic fraud incident(s) to the value of R30m, Landbank/ ABSA electronic incident [redacted] SARS electronic fraud incidents [redacted] about R100m. The ban[redacted]ector is especially vulnerable to cybercrime. In light of the above and many more unreported incidents there is a ne[redacted]ombat cybercrime.

2.5 The borderless nature of cybercrimes introduces a further dimension to National Security. Numerous cyber attacks have been launched against a number of countries , such as the attack on Estonia in 2007, which crippled the country's electronic systems . South Africa is not immune to such attacks. The protection of South Africa's critical information infrastructure and the coordination thereof is therefore essential. South Africa needs to develop mechanisms that will ensure proactive and coordinated national response to cyber threats and incidents including combating cybercrime. The Government's leadership role in this regard is important, whilst acknowledging that

[7] **Source: RSA Anti-Fraud Command Center, March 2011.**

Cybersecurity is everyone's responsibility, public sector, private sector and civil society.

2.6 The role of the ICT's in social and economic development on a country has been widely acknowledged; however the full potential of ICT's cannot be realized unless there is confidence and trust in the secure use of ICT's. Government should take responsibility to ensure that the private sector and civil society are not only aware of the dangers of operating in cyberspace but also take necessary measures not to become victims of cybercrime. It is thus prudent to develop a culture of Cybersecurity that will address the needs pf the public sector, private sector and civil society.

2.7 Opportunities of ICT and the challenges of cybersecurity are fuelled by advances in technology. There is consequently a need to develop the requisite skills to exploit the opportunities of an information economy and meet the dynamic challenges of Cybersecurity. South Africa will always be lag behind or be vulnerable unless we develop requisite skills. There is a need to create an enabling environment for Cybersecurity training, education, research and development' and skills development programmes in South Africa.

2.8 South Africa is a consumer of ICT's and depends on overseas manufactured technologies to secure its Cyberspace. The downside of this, is that our critical information infrastructure will continue to have some degree vulnerability. Thus it is important to develop indigenous cybersecurity technologies. Unless we develop R&D capabilities to address this, we will continue to rely of foreign technologies for this purpose. The absence of stringent compliance monitoring to ensure that technologies used comply to international and national Cybersecurity standards.

2.9 South Africa will in the promotion and development of cybersecurity measures in relation to this NCPF bear in mind the international instruments and measures that may be relevant such as the work of the various agencies of the United Nations8

3. PURPOSE OF THE NCPF

3.1 The purpose of the NCPF is to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure whilst strengthening shared human values and understanding of cybersecurity in support of national security imperatives and the economy. This will enable the development of an information society which takes into account the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression.

3.2 The NCPF seeks to ensure that Government, business and civil society are able to enjoy the full benefits of a safe and secure cyberspace. To this end, the public sector, private sector and civil society will work together to understand and address the risks, reduce the benefits to criminals and seize opportunities in cyberspace to enhance South Africa's overall security and safety including its economic well being.

3.3 This NCPF provides for:

a) Measures to address national security in terms of cyberspace;

b) Measures to combat cybercrime;

---

8 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 ICTs. 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. The UN is of the view that the implementation of instruments, such as the Budapest Convention, is a way to help countries worldwide to address cybercrime as indicated at the 12th United Nations Congress on Crime Prevention and Criminal Justice. Adopted on 19 April 2010, the "Salvador Declaration" confirms the need for a global capacity building effort to strenghten the full implementation of existing treaties and standards – while continuing to study new remedies.

c) The development, review and updating existing substantive and procedural laws to ensure alignment; and

d) Measures to build confidence and trust in the secure use of ICT.

4. NATIONAL CYBERSECURITY POLICY OBJECTIVES

4.1 The NCPF articulates the overall aim and objectives of the South African Government and sets out strategic priorities that will be pursued to achieve these objectives. In order to achieve the strategic vision set out in this policy, it is expected that this National Cybersecurity Policy Framework will:

a) Centralise coordination of cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge based economy;

b) Anticipate and confront emerging cyber threats and coordinate responses thereto, by reducing cyber threats and vulnerabilities through technical measures; cybercrime policy and strategies; regulatory measures; general awareness; and legal measures, inter alia, enhancing all substantive and procedural laws;

c) Foster cooperation and coordination between Government, the private sector and civil society by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology.

d) Promote international cooperation;

e) Develop requisite skills, research and development capacity,

f) Promote a culture of cybersecurity,

g) Promote compliance with appropriate technical and operational Cybersecurity standards.

5. CREATING INSTUTITIONAL CAPACITY TO RESPOND TO CYBERSECURITY IMPERATIVES

5.1 The Justice Crime Prevention and Security Cluster (JCPS), working in consultation with other Government Clusters such as the Economic Cluster, will oversee the implementation of this policy framework, with the aim to ensure centralized coordination of cybersecurity issues.

5.2 A dedicated Cybersecurity Response Committee chaired by State Security Agency will be established within the JCPS Cluster to coordinate cybersecurity activities.

6. NATIONAL CYBER SECURITY COORDINATING CENTRE AND COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT)

6.1 Not withstanding various National Security structures established within the Intelligence community and the broader security cluster Departments and other government and private sector entities, South Africa does not have a centralised structure to anticipate cyber threats and respond to those threats. This situation, can lead to being reactive to responding to cybersecurity threats and attacks, and resulting in an uncoordinated approach.

6.2 In addressing to these challenges of government not having a centralised structure (such as the computer security incident team (CSIRT)) to aniticipate cyber threats and coordinate South Africa's responses thereto, the NCPF promotes the establishment of the following:

6.3 NATIONAL CYBER SECURITY COORDINATING CENTRE (NCSC)

6.3.1 The NCSC shall be established by the JCPS cluster and will play an oversight and coordinating role in the operations of all Computer Security Incident Response Teams (CSIRTs) in SA.

6.3.2 The NCSC will provide guidelines and national standards on the establishment of CSIRTs with special focus on National Security matters.

6.3.3 The Department of State security, in consultation with other State Organs dealing with National security issues, shall be responsible for the establishment of the NCSC. This will include the development of relevant policies, standards processes and procedures for information sharing and coordinated National security response on all national cyber security incidents.

6.3.4 The key focus areas for the NCSC will be all matters related to cyber warfare, cyber intelligence and Cybercrime and will:

a. Act as single point of contact on cybersecurity matters pertinent to national security (national defence, national intelligence and cybercrime);

b. Coordinate cybersecurity incident response activities regarding national intelligence, national defence and cybercrime.

c. Facilitate information sharing and technology exchange relevant to national security in cyberspace;

d. Establish and guide standards and best practices for South Africa;

e. Develop agreed measures to deal with cybersecurity matters impacting on national security;

f. Facilitate interaction, both nationally and internationally, including through international memberships to organisations such as the Forum for Incident Response and Security Teams (FIRST); and develop policy guidelines to inform such interaction;

i. Facilitate the identification, protection and develop national standards on the protection and security of the National Critical Information Infrastructure (NCII);

g. Assist with Corporate Security and Policy Development, Governance, Risk Management, and Compliance (GRC), Identity and Security Management, Security Information and Event Management (SIEM), Digital Forensics;

h. Develop response protocols to guide coordinated responses to cybersecurity incidents and interaction with the various stakeholders such as the National CSIRTs and the cybersecurity fraternity in general;

i. Do regular assessment and testing of National critical information infrastructures including vulnerability assessments, threat and risk assessment and penetration testing;

j. Conduct cybersecurity audits, assessments and readiness exercises and advise on the development of a national response plan; and

k. Perform any other function consistent with the policy objectives set out herein.

6.3.5 The Department of Communications, in consultation with relevant ICT industry bodies and the general public, shall initiate, establish and develop operational processes and procedures for Sector CSIRTs in the Republic in accordance with the national guidelines and standards set out by the NCSC.

6.3.6 In establishing these CSIRTs, the DoC shall set out the role and functions of each Sector CSIRTs including ensuring that the CSIRTs in SA:

(a) Disseminate relevant information to NCSC or other sector CSIRTs where necessary,

(b) Act as a single point of contact for that specific sector on Cybersecurity matters;

(c) Create and maintain situational awareness concerning the risk environment of South African cyberspace;

(d) Initiate national cybersecurity awareness campaigns;

(e) Establish information sharing processes and procedures with the NCSC as part of the broader SA National Cyber security coordination.

(f) Facilitate information sharing and technology sharing within that sector;

(g) Conduct Cybersecurity audits, assessments and readiness exercises for the sector;

(h) Develop agreed measures to deal with Cybersecurity matters impacting on the sector;

6.3.7 The SSA shall, in consultation with DoC, encourage and facilitate the establishment of regional and continental CSIRT's and provide advice on best practice guidance on ICT security for Government, business and civil society;

7 NATIONAL CRITICAL INFORMATION INFRASTRUCTURE (CII) PROTECTION

7.1 This policy framework recognises the need to provide mechanism to ensure that South Africa's critical information infrastructure is protected and secured against cyber related crimes. It is also noted that a more secured critical information infrastructure will also help to achieve the continued provision of essential services and support national security, economic prosperity and social wellbeing of the Republic. The policy framework recognises that a significant proportion of SA's critical information infrastructure (CII) is privately owned or operated on a commercial basis.

7.2 The NCPF therefore seeks to ensure that appropriate steps are taken to ascertain that all National Critical Information Infrastructure (NCII) are identified and properly protected from a variety of threats. For continued availability of the critical information infrastructure, the NCPF provides for the development of a National Critical Information Infrastructure (NCII) Strategy that will address the identification and protection of NCII by :–

a) Developing National Critical Information Infrastructure regulations,inter alia:
   i. Information Security Policy and Procedures
   ii. Third Party Access to NCII
   iii. Access to & authentication on NCII
   iv. Storage and archiving of critical databases
   v. Incident management and business continuity
   vi. Physical and technical protection of all NCII

b) Facilitate an effective business - government partnership relating to the implementation of the CII Protection Plan. To this end, the private sector, state owned enterprises (SOE's), and other government agencies and institutions such as the State Information Technology Agency (SITA) will play a critical role in ensuring the implementation of NCII protection plan.

8 CRYPTOGRAPHY

8.1 There are an ever-increasing numbers of cryptographic devices, cryptographic software and users requiring secure communications and the geographic spread of locations of these devices. This policy framework provides for the regulation of cryptography given the critical role it plays in ensuring improved secure communications.

8.2 The NCPF notes that various attempts at regulating cryptography were initiated as a way of developing a coherent and integrated approach to this matter. These strategies are found in various laws such as:

- *National Convention Arms Control Act (Act 41 of 2002)*
- *Electronic Communications and Transactions Act (Act 25 of 2002)*
- *Electronic Communications Security (Pty) Ltd Act (Act 68 of 2002)*
- *Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002)*
- *State Information Technology Agency Act (Act 88 of 1998)*
- *Conventional Arms Control Regulations (R7969 of 2004)*
- *Cryptographic regulations (R 8418, of 2006)*

8.3 Taking into consideration the above-mentioned legislation, there is a need to:

a) Review the existing legislation and regulations thereof; and

b) Develop an integrated regulatory framework for Cryptography in the Republic.

9. E- IDENTITY MANAGEMENT IN CYBERSPACE

9.1 The ECT Act provides for the establishment of the South African Accreditation Authority to facilitate the accreditation and regulation of authentication services

and products. It further provides for the advanced electronic signature facilitating the recognition of electronic documents as legal and binding.

9.2 To this end, the South African Post Office (which in terms of the ECT Act was identified as a preferred service provider for advanced electronic signatures has developed Public key Infrastructure (PKI) to support advanced electronic signature (e-identity), the Department of Public Service and Administration pursuant to its mandate in E –Government has developed a PKI Strategy. The Department of Communication is pursuant to its mandate established the South African Accreditation Authority to accredit and regulate authentication services and products.

9.3 The NCPF seek to address the fragmented approach by developing an integrated National E-identity and PKI strategy. Such a strategy and implementation thereof will be critical in providing inter alia e-government services as well as to ensure security, confidentiality and integrity. Uptake and usage of e-identity in e-government services will stimulate other sectors as well. The issue of identity management in cyberspace is central to the building confidence and trust in the secure use of ICTs.

9.4 The NCPF acknowledges that transmission of information over the Internet for trading and communication purposes present new and sophisticated threats for both the senders and recipients of information. Therefore to ensure online transaction security, the NCPF provides for the development of a holistic national E-Identity and PKI strategy. The strategy will amongst others address:

a) Authentication and securing of the identities of the parties to an e-transaction.
b) Confidentiality, ensuring information is kept private.
c) Integrity ensuring the information or process has not been modified or corrupted.
d) Non-repudiation ensuring neither party can refute that thetransaction occurred (i.e. the transaction is binding).
e) The structure and regulatory framework for E-Identity and PKI.

10. PROMOTE AND STRENGTHEN LOCAL AND INTERNATIONAL COOPERATION

10.1 In terms of this policy framework, the National CSIRT will foster cooperation and coordination between the public sector, private sector and civil society.

10.2 Local cooperation

10.2.1 The goal for the Government-Industry Collaboration is among others, to develop government-industry collaboration and to use industry perspectives, equities and knowledge to enhance Cybersecurity. The Government-Industry Collaboration is based on the understanding that Cybersecurity is everyone's responsibilities and there is a need to leverage on the Industry knowledge, as they are the business of developing ways and means to combat cybercrime. The NCPF provides to the establishment of Collaboration with local stakeholder, and this collobaration will focus on the following aspects:

a) Inclusion of the industry and creating an enabling environment for a successful partnership;
b) Encouraging private sector groups to address common security interests and collaborate with government including encouraging cooperation among groups from interdependent industries;
c) Bringing private sector and government together in a trusted forums;
d) Creating a common understanding of the threats and vulnerabilities that the country faces.

10.3 International Cooperation

10.3.1 Internet as a form of media can in essence not be regulated in total by an authority or government. Given the borderless nature of the Internet and the

challenges it poses in terms of jurisdiction, it is important that countries learn and collaborate with each other in order to combat cyber crimes.

10.3.2 Therefore, international collaboration is critical in securing cyberspaces nationally and globally. Recognising the need for global collaboration on matters regarding cybersecurity, South Africa shall collaborate with relevant and appropriate international organisations and governments, subject the Constitution, national security imperatives, foreign policy and existing international agreements. To this end, South Africa will:

a) Participate in regional, African Union and international fora on matters pertinent to cybersecurity in order to ensure advance South Africa's views in the definition and elaboration of the global cybersecurity agenda in combating cybercrime and building confidence and trust in the secure use of ICT's.

b) Forge bilateral and multilateral partnerships in our national interest through various instruments inter alia Memorandum of Understanding, Convention, Treaty.

c) Affiliate to relevant international organisations in order to promote a coordinated global response to threats and vulnerabilities and to keep abreast of developments in the Cybersecurity front.

11. CAPACITY DEVELOPMENT, RESEARCH AND DEVELOPMENT

11.1 The dynamic nature of cybersecurity challenges necessitates the continuous development of capabilities and requisite skills.

11.2 The NCSPF therefore promotes the:

a) Development of capacity building strategies to address South Africa's, specific skills requirements to meet the ever increasing challenges of addressing cybersecurity threats.

b) Development of recruitment and retention strategies aimed at ensuring a sufficient level of technical expertise is developed and maintained within the Republic; and

c) Development of Cybersecurity research and development agenda and enhance Cybersecurity research within South African Universities, industry and the Department of Science and Technology.

12. PROMOTION OF A CULTURE OF CYBERSECURITY

12.1 To effectively deal with Cybersecurity, it is prudent that civil society, government and the private sector play their part in ensuring South Africa has a culture of Cybersecurity. Critical to this is the development of a culture of Cybersecurity, in which role players understand the risks of surfing in cyberspace. To facilitate the building the culture of Cybersecurity, the NCPF provides for inter alia:

a) Implementing cybersecurity awareness programs for private sector, public sector and civil society users;
b) Encouraging business to develop a Culture for Cybersecurity;
c) Supporting outreach to civil society, children and individual users;
d) Promoting an comprehensive national awareness program and guidelines
e) Reviewing and updating existing privacy regime;
f) Develop awareness of cyber risks and available solutions; and
g) Continously review cyber applications and the impact from a Cybersecurity perspective.
h) Compliment the culture of Cybersecurity with online support mechanisms.

13 TECHNICAL AND OPERATIONAL STANDARDS COMPLIANCE

13.1 The NCSPF also promotes:

a) The recognition of and compliance with appropriate international and local technical and operational cybersecurity standards. The Minister of Communications shall enforce compliance with such standards where appropriate and in consultation with the National Cybersecurity Advisory Council;

b) The continuous monitoring, review and assessment of regulatory frameworks that support cybersecurity ; and

c) The development and/or adoption of standards by the South African Bureau of Standards in consultation with relevant Government Departments, ICASA and industry. This will ensure a safe and secure cyberspace environment that will enable the growth of e-commerce and an inclusive information society.

14. ROLES AND RESPONSIBILITIES OF RELEVANT ORGANS OF STATE

14.1 This policy recognizes that there are a number of Organs of State that play a critical role in the implementation of cybersecurity measures and for effective implementation of this policy framework, the role of some of the main relevant Organs of State are set out below. Inclusive of the various roles and responsibilities set out, all other governmental priorities such as the protection of vulnerable groups, promotion of job creation and general protection of Constitutional values and principles are endorsed and should be promoted in the development of implementation plans and activities. Liaison with other clusters such as the economic cluster will be essential in the development of the various implementation plans guided by the NSPF.

a) The **Department of Justice and Constitutional Development** (DOJ&CD and the **National Prosecuting Authority** (NPA) have an overall responsibility for facilitating cybercrime prosecution and court processes in accordance with the applicable laws, including ensuring all relevant laws are aligned to this policy in order to create a coherent and integrated cybercrime prosecution approach in the Republic. This would require initiation of processes to effect necessary amendments to relevant legislation in order to make cybercrime or related crimes punishable in law.

b) The **State Security Agency (SSA)** has overall responsibility for coordination, accountability and implementation of cybersecurity measures in the Republic as an integral part of its National Security mandate. This will include aspects of developing and implementing regulations, collecting intelligence both locally and internationally, conducting necessary Cybersecurity investigations and reporting on South Africa's Cybersecurity situation.

c) The **South African Police Service (SAPS)** in terms of this NCPF is responsible for prevention, investigation and combating cybercrime in the Republic, which includes development of cybercrime policies and strategies, provides for specialized investigative capacity and interaction with national and international stakeholders. Development of the anti-cybercrime policy and implementation plans should include operational priorities such as those identified by the European Commission pertaining to the (i) fight against child sexual/physical abuse material on the Internet; (ii) actions to counter massive attacks against information systems such as "denial-of-service attacks (such as those affecting the banking sector); and (iii) actions combating identity fraud. It should also promote the development of cross-border law enforcement cooperation; public-private cooperation to fight cybercrime (in particular between law enforcement authorities and private companies); and promote enhanced international cooperation to fight cybercrime by taking part in various international initiatives such the UN High Level Expert Group on Cybersecurity and The International Telecommunication Union.

d) The **Department of Communications (DoC)** has the responsibility for:

i) Developing and implementing policies, regulations and industry standards. Provide strategic direction and coordination on local and international Cybersecurity matters pursuant to building an information economy and building confidence and trust in the secure use of ICT's.

ii) Establishing the National Cybersecurity Advisory Council (NCAC) whose role will be to advise the Minister of Communications on policy and technical issues and other matters pertinent to Cybersecurity;

iii) Establishing the National CSIRT.

e) **The Department of Defence and Military Veterans (DoD&MV)** has overall responsibility for coordination, accountability and implementation of cyber defense measures in the Republic as an integral part of its National defence mandate. To this end, the Department will develop policies and strategies pursuant to its core mandate.

f) **The Department of Science and Technology (DST)** has the responsibility for the development, coordination and implementation of national capacity development program. Furthermore, the Department shall be responsible for developing and facilitating the implementation of a national cybersecurity research and development agenda for South Africa.

g) All other Organs of State are required to align their ICT policies and practices with this NCPF.

15. CONCLUSION

15.1 It is envisaged that the NCPF when implemented will achieve the following benefits:

a) A safer and more secure cyberspace that underpins national security priorities;

b) The establishment of institutional structures to support a coordinated approach to addressing cybersecurity;

c) The identification and protection of critical information infrastructure;

d) A secure e-environment that stimulates economic growth and competitiveness of South Africa;

e) Promotion of a national research and development agenda relating to cybersecurity;

f) The effective prevention, combating and prosecution of cybercrime; and

g) The enhanced management of cybersecurity.

17.2 ANNEXURE:

A. SYNOPSIS OF NATIONAL CYBERSECURITY IMPLEMENTATION SCHEDULE:

ACTIVITY	LEAD DEPT	PROPOSED TIME FRAME
COORDINATION OF IMPLEMENTATION PLAN	JCPS CLUSTER: OUTPUT 8 IMPLEMENTATION DELIVERY FORUM	Approval of NCPF and thereafter Implementation P lan within 6 months
CYBERCRIME STRATEGY AND IMPLEMENTATION	SAPS	By end March 2012
LEGISLATIVE REVIEW	DOJCD	By end March 2012
CRYPTOGRAPHY STRATEGY AND REGULATIONS	SSA	By end March 2012
NCII STRATEGY AND REGULATIONS	SSA	By end March 2012
IDENTITY MANAGEMENT STRATEGY	HA	By end March 2012
NATIONAL CSIRT ESTABLISHMENT	DOC	By end March 2012
GOVERNMENT CSIRT ESTABLISHMENT	SSA	By end March 2012

SECTOR CSERT ESTABLISHMENT	**DOC**	**By end March 2012**
SKILLS DEVELOPMENT	**Science and Tecnology/ Education/ DPSA**	**By end March 2012**
TECHNICAL STANDARDS	**DOC/ SABS/ ICASA**	**By end March 2012**
RESEARCH AND DEVELOPMENT AGENDA	**DST**	**By end March 2012**
AWARENESS-RAISING	**DOC**	**By end March 2012**

B. REFERENCE MATERIAL

In developing the National Cybersecurity Policy Framework for South Africa, the following cybersecurity policies, strategies, guidelines and research material was taken into account and was central in the development of this submission.

1. *SA's draft Cybersecurity Policy- February 2010- Government Gazette no 32963 of 2010*

2. *International Telecommunications Union (ITU) Cybersecurity Guidelines for Developing Nations.- 2008*

3. *Australian Government Cybersecurity Policy- June 2010*

4. *Cybersecurity Strategy- Australia-*

5. *Japan's Cybersecurity Strategy- February 2011*

6. *National Security Vision- Malaysia- 2009*

7. *Malaysia's National Cybersecurity Policy- 2009*

8. *Comprehensive National Cybersecurity Initiative: Legal and Policy Considerations- John Rollins and Anna C Henning- March 2010*

9. *Cybersecurity Strategy of the United Kingdom- June 2009*

10. *Rockfeller-Snowe Cybersecurity Act- March 2010*

11. *Cybersecurity Policy of Germany*

References to the various sources was necessitated by the need to determine the approaches adopted by other jurisdictions in dealing with this ever changing security challenge. It is clear from the reference material referred to above that the technological developments have, however, exposed communication systems and networks globally to a growing number and wider variety of threats and vulnerabilities.