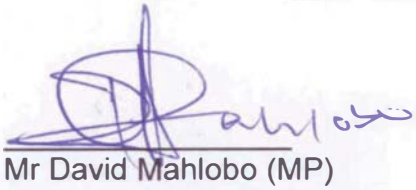
STATE SECURITY AGENCY

NO. 609 **04 DECEMBER 2015**

THE NATIONAL CYBERSECURITY POLICY FRAMEWORK (NCPF)

I, Mbangiseni David Mahlobo, Minister of State Security, hereby publish the National Cybersecurity Policy Framework (NCPF) as approved by Cabinet on the 7th March 2012 for public information.

Any queries relating to this document can be directed to Head of Communications Mr Brian Dube via e-mail at bdube@ssa.gov.za.



Mr David Mahlobo (MP)
Minister of State Security
September 2015

STATE SECURITY AGENCY

NATIONAL CYBERSECURITY POLICY FRAMEWORK

FOR SOUTH AFRICA

Table of Contents

ABBREVIATIONS

CII	Critical Information Infrastructure
CRC	Cybersecurity Response Committee
CSIR	Council for the Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
DOJ&CD	Department of Justice and Constitutional Development
DOD&MV	Department of Defence and Military Veterans
DST	Department of Science and Technology
DTPS	Department of Telecommunications and Postal Services
ECS	Electronic Communications Security
ECT	Electronic Communications and Transactions
FIRST	Forum for Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GRC	Governance, Risk Management and Compliance
HLEG	High-Level Experts Group
ICT	Information and Communications Technology
ICASA	Independent Communications Authority of South Africa
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ITU	International Telecommunication Union
JCPS	Justice, Crime Prevention and Security (Cluster)
MOU	Memorandum of Understanding
NCAC	National Cybersecurity Advisory Council
NCII	National Critical Information Infrastructure
NCPF	National Cybersecurity Policy Framework
NPA	National Prosecuting Agency
PKI	Public Key Infrastructure
SAPS	South African Police Service
SIEM	Security Information and Event Management
SITA	State Information Technology Agency
SOE	State Owned Entity
SSA	State Security Agency
UNODC	United Nations Office on Drugs and Crime
WSIS	World Summit on the Information Society

EXECUTIVE SUMMARY

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

2. This new electronic environment is commonly known as cyberspace. The 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. This is because the danger that Cybersecurity threats pose, is real.

3. 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. Given the seriousness of cyber threats 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. For this reason, the cyber threats need to be addressed at both the global and national levels.

4. National Cybersecurity is a broad term encompassing the 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 therefore comprises a range of activities at different levels.

5. World-wide Cybersecurity strategies are being developed and are aimed at setting policy goals, measures and institutional responsibilities in a succinct manner. Generally, the primary concern is to ensure the confidentiality, integrity and availability (C-I-A) of computer data and systems and to protect against or prevent intentional and non-intentional incidents and attacks. Priority is also given to critical information infrastructure protection (CIIP).

6. These strategies normally also contain measures against or reference to cybercrime. Measures against cybercrime provide a criminal justice response to C-I-A attacks against computers and thus complement technical and procedural Cybersecurity responses. However, cybercrime comprises also offences committed by means of computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights (IPR) infringements and many other offences. Furthermore, any crime may involve electronic evidence in one way or the other. While this may not be labelled "cybercrime", a cybercrime strategy would nevertheless need to ensure that the forensic capabilities be created that are necessary to analyse electronic

evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect.[1]

7. This South African National Cybersecurity Policy Framework is aligned to these goals and is necessitated to ensure a focussed and an all-embracing safety and security response in respect of the Cybersecurity environment and establishes and addresses the following:

a) The development and implementation of a Government led, coherent and integrated Cybersecurity approach to address Cybersecurity threats;

b) Establishing a dedicated policy, strategy and decision making body to be known as the JCPS Cybersecurity Response Committee, to identify and prioritise areas of intervention and focussed attention regarding Cybersecurity related threats. The Cybersecurity Response Committee will be chaired by the State Security Agency (SSA) and will be supported operationally by a Cybersecurity Centre, situated at the SSA

c) The capability to effectively coordinate departmental resources in the achievement of common Cybersecurity safety and security objectives (including the planning, response coordination and monitoring and evaluation);

d) Fighting cybercrime effectively through the promotion of coordinated approaches and planning and the creation of required staffing and infrastructure;

e) Coordination of the promotion of Cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to Cybersecurity threats, through interaction with and in conjunction with the Cybersecurity Hub (to be established within the Department of Telecommunications and Postal Services);

f) Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;

g) Ensuring of the protection of national critical information infrastructure;

[1] Council of Europe, Global Project on Cybercrime. Discussion paper Cybercrime Strategies, www.coe.int/cybercrime

h) The promotion of a Cybersecurity culture and compliance with minimum security standards;

i) The establishment of public-private partnerships for national and action plans in line with the NCPF; and

j) Ensuring a comprehensive legal framework governing cyberspace.

8. The National Cybersecurity Policy Framework (NCPF) is aligned with and dealt within the JCPS Cluster's mandate and obligations under Outcome 3: All people are and feel safe in South Africa. In this regard, Output 8 of Outcome 3 requires the development and implementation of a Cybersecurity policy and the development of capacity to combat and investigate cybercrime that seeks to promote the following:

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

9. The NCPF is intended to provide a holistic approach pertaining to the promotion of Cybersecurity measures by all role players and will be supported by a National Cybersecurity Implementation Plan which will be developed by the JCPS Cluster 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.

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 Cybersecurity breaches (Cybersecurity incidents);

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

"Cybersecurity Hub" means a CSIRT established to pool public and private sector threat information for the purposes of processing and disseminating such information to relevant stakeholders including the Cybersecurity centre.

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

---

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

2This definition does not purport to be a universally accepted definition in a UN reference framework.

3 Ibid.

"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.

"JCPS CRC" means Justice, Crime Prevention and Security Cluster's Cybersecurity Response Committee.

"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 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, as an example, 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. These modus

---

4 Ibid.

5 http://en.wikipedia.org/wiki/Malware

operandi are constantly evolving and is included here as typical examples of Cybersecurity / cybercrime threats that many people will encounter when using computers and information communication technology. 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.

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 (ICTs) have become indispensable 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 NCPF Policy Framework therefore recognises that Cybersecurity threats and the combating thereof have a personal, national and international context.

1.3 Cyberspace comes with new types of challenges to the governments of the world and it therefore 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 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 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,

media and telecommunications companies in Estonia demonstrated the vulnerability of a society's information infrastructure as 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.

1.4 The recurrence and growing incidence of cyber-attacks indicate the start of a new era in which the security of cyberspace requires a global dimension and the protection of National Critical Information Infrastructure must be elevated, in terms of national security, on 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 of a range of activities at different levels. Towards 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 critical information systems.

1.6 Thus, a Cybersecurity strategy must appraise the vulnerability of a country's critical information infrastructure, devise a system of preventative measures against cyber-attacks, and decide upon the allocation of tasks relating to Cybersecurity management at the national level. 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 Cybersecurity.

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 Cybersecurity 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 and other cyber ills;

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 by the SSA in consultation with relevant stakeholders, identifying roles and responsibilities, timeframes, specific performance indicators, and monitoring and evaluation mechanisms.

2. The South African Context

2.1 South Africa like many other countries has become dependent on the Internet to govern, to conduct business and for other social purposes. The Internet has become indispensable to many South Africans and will continue to be, as more people access 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 collectively does not 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 jurisdictions are faced with the same challenges.

2.4 Statistics in 2011 indicate that South Africa was in the top three countries that are targeted for phishing purposes, the other countries are the USA and the UK. In addition to phishing, other

e-Crime incidents in the RSA have increased to the value of millions of rands. The banking sector is especially vulnerable to cybercrime. In light of the above and many more unreported incidents, there is a need to combat 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 Cybersecurity is everyone's responsibility, public sector, private sector and civil society.

2.6 The role of the ICTs in social and economic development of a country has been widely acknowledged; however the full potential of ICTs cannot be realized unless there is confidence and trust in the secure use of ICTs. 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 within South Africa a culture of Cybersecurity that will address the needs of the public sector, private sector and civil society.

2.7 Opportunities of ICT and the challenges of Cybersecurity are fuelled by advances in technology. Consequently, there is 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 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 ICTs 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 of vulnerability. Thus it is important to develop indigenous Cybersecurity technologies. Unless we develop Research and Development 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 Nations.[6] In 2011, the International Telecommunications Union (ITU) and the UN Office on Drugs and Crime (UNODC) signed a memorandum of understanding (MOU) to help secure cyberspace for consumers, businesses, and children and to mitigate the risks posed by cybercrime. The MOU will enable the parties to avail the necessary expertise and resources to establish legal measures and legislative frameworks at national level, for the benefit of all interested countries. This initiative is a major milestone in implementing a co-ordinated global approach to an increasingly serious global problem.[7]

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 need to 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 therefore provides for:

a) Measures to address national security in terms of cyberspace;
b) Measures to combat cyber warfare, cybercrime and other cyber ills;
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.

---

6 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, as 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" contains the need for a global capacity building effort to strengthen the full implementation of existing treaties and standards – while continuing to study new remedies.

7 Itweb/ITU

4. Key Objectives of the NCPF

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:

4.1.1 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;

4.1.2 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;

4.1.3 Promote international cooperation;

4.1.4 Develop requisite skills, research and development capacity;

4.1.5 Promote a culture of Cybersecurity; and

4.1.6 Promote compliance with appropriate technical and operational Cybersecurity standards.

5. Capacity to Respond to Cybersecurity Imperatives

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

5.2 A dedicated JCPS Cybersecurity Response Committee will be established within the JCPS Cluster to coordinate Cybersecurity activities, drive the implementation of the NCPF and manage the implementation of Output 8. The Cybersecurity Response Committee will be chaired by the State Security Agency (SSA) and it will be supported operationally by a Cybersecurity Centre, situated at the SSA. All relevant JCPS departments will be represented on the Cybersecurity Response Committee.

5.3 The role of the JCPS Cybersecurity Response Committee will, amongst others, be to:

5.3.1 Ensure the achievement of NCPF policy objectives as outlined in section 4.1 above;

5.3.2 Coordinate Cybersecurity activities and be a central point of contact on all Cybersecurity matters pertinent to national security (national defence, national intelligence and cybercrime);

5.3.3 Identify and prioritise areas of intervention and promote focussed attention and guidance where required regarding Cybersecurity related threats and incidents;

5.3.4 Promote, guide and coordinate activities aimed at improving Cybersecurity measures by all role players, which would include amongst others, the strengthening of intelligence collection and improved State capacity to investigate, prosecute and combat:

a) Cybercrime,
b) Cyber terrorism,
c) Cyber espionange,
d) Cyber warfare and
e) Any other cyber related threats;

5.3.5 Oversee and guide the functioning of the Cybersecurity Centre, Cybersecurity Hub, RSA Government Electronic Communications Security Computer Security Incident Response Team (ECS –CSIRT) and any other CSIRT established in SA.

5.3.6 Promote and provide guidance to the process of the development and implementation of:

a) The protection of national critical information infrastructure Plan;

b) Situational analysis and awareness campaign concerning the risk environment of South African cyberspace;

c) Cybersecurity culture and compliance with minimum security standards;

d) Public-private partnerships for national and action plans in line with the NCPF;

e) Compliance with appropriate technical and operational Cybersecurity standards;

f) Cybersecurity training, education, research and development and skills development programmes;

g) International cooperation;

h) Facilitation of 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) Establishment of sector, regional and continental CSIRTs; and

j) Comprehensive legal framework governing cyberspace.

5.4 The role of the Cybersecurity Centre will be to:

5.4.1 Facilitate the operational coordination of Cybersecurity incident response activities regarding national intelligence, national defence and cybercrime;

5.4.2 Develop measures to deal with Cybersecurity matters impacting on national security;

5.4.3 Facilitate the analysis of Cybersecurity incidents, trends, vulnerabilities, information sharing, technology exchange on national security and threats to improve technical response coordination;

5.4.4 Provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructure (NCII);

5.4.5 Ensure regular assessment and testing of National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessment and penetration testing;

5.4.6 Provide coordination and guidance regarding Corporate Security and Policy Development; Governance, Risk Management, and Compliance (GRC); Identity and Security Management; Security Information and Event Management (SIEM), and Digital Forensics as it pertains to Cybersecurity matters within Organs of State;

5.4.7 Develop response protocols to guide coordinated responses to Cybersecurity incidents and interaction with the various stakeholders;

5.4.8 Ensure the conducting of Cybersecurity audits, assessments and readiness exercises and provide advice on the development of national response plans;

5.4.9 Provide the Secretariat services required in relation to the JCPS Cybersecurity Committee, and

5.4.10 Perform any other function consistent with the strategic and policy objectives set out herein.

6. Cybersecurity Hub and Additional CSIRTs

6.1 Notwithstanding the envisaged JCPS Cybersecurity Response Committee, the Cybersecurity Centre and the existing ECS-CSIRT, there is also a need to ensure appropriate consultation between the JCPS cluster departments, the private sector and civil society regarding Cybersecurity matters.

6.2 To deal with the above stated, this policy recognises that the crucial need for the facilitation of interaction between the key role players in the public sector, private sector and the broader civil society. The NCPF therefore promotes the coordination and consultation between the JCPS cluster departments, the private sector and civil society regarding Cybersecurity matters through the establishment of a Cybersecurity Hub within the Department of Telecommunications and Postal Services (DOC). The Cybersecurity Hub will be operated within the DOC in accordance with national security guidelines and standards issued by the JCPS Cybersecurity Response Committee.

6.3 To enhance interaction, consultations and to promote a coordinated aproach regarding engagements with the private sector and civil society, Cybersecurity Hub will, amongst others, have the responsibility to:

6.3.1 Coordinate general Cybersecurity activities, in consultation with JCPS CRC as well as including identifying stakeholders and developing public-private relationships and collaborating with any sector CSIRTs that may be established;

6.3.2 Disseminate relevant information to other sector CSIRTs, vendors, technology experts on Cybersecurity developments;

6.3.3 Provide best practice guidance on ICT security for Government, business and civil society;

6.3.4 Initiate Cybersecurity awareness campaigns;

6.3.5 Promote compliance with standards, procedures and policy developed by the JCPS Cybersecurity Response Committee regarding Cybersecurity matters with a bearing on national security.

6.3.6 Encourage and facilitate the development of appropriate additional sector CSIRTs. The sector CSIRTs will:

6.3.6.1 Be a point of contact for that specific sector on Cybersecurity matters;

6.3.6.2 Coordinate Cybersecurity incident response activities within that sector;

6.3.6.3 Facilitate information and technology sharing within the sector;

6.3.6.4 Facilitate information sharing and technology exchange with other sector CSIRTs;

6.3.6.5 Establish national security standards and best practices for the sector in consultation with the Cybersecurity Centre and the JCPS Cybersecurity Response Committee which are consistent with guidelines, standards and best practices developed in line with this policy framework;

6.3.6.6 Develop agreed upon measures;

6.3.6.7 Conduct Cybersecurity audits, assessments and readiness exercises for the sector; and

6.3.6.8 Provide sector entities with best practice guidance on ICT security.

7. Verification of Information Security Products and Systems

7.1 South Africa needs to independently assess and certify products and systems that are used to process or store information that can have an impact on national security. The NCPF therefore promotes the facilitation by the JCPS Cybersecurity Response Committee and the National Cybersecurity Hub of the development of a National Information Security Verification Framework that will enable the achievement of this objective by executing the following:

a) Facilitating effective partnerships between the Republic of South Africa and countries with established capacity to perform information security assessments and certifications.

b) Facilitating effective partnerships between the Government of South Africa, the private sector, academic and research institutions to ensure that there is always capacity to perform information security assessments and certifications within the borders of the Republic.

c) Developing National regulations for verification of products and systems with applications in Information Security.

d) Facilitating effective partnerships among government institutions, e.g. those tasked with technical assessments, and those whose responsibility is licensing, and those

who monitor, (e.g. the Auditor General), to ensure that solutions are implemented in accordance with certification conditions and legislation.

e) Establishing a body that will centrally coordinate the required national verification functions.

8. NCII Protection

8.1 The NCPF recognises the need to provide a 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 help to achieve the continued provision of essential services and support national security, economic prosperity and social well-being of the Republic. The policy framework recognises that a significant proportion of SA's national critical information infrastructure (NCII) is privately owned or operated on a commercial basis.

8.2 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 thus promotes 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, relating, inter alia, to:

i. Information Classification and Information Security Policy and Procedures;
ii. Third Party Access to NCII;
iii. Access to and authentication on NCII;
iv. Storage and archiving of critical databases;
v. Incident management and business continuity; and
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.

9. Cryptography

9.1 There are an ever-increasing numbers of cryptographic devices, crypto graphic software and users requiring secure communications and the geographic spread of locations of these devices. The NCPF therefore provides for the regulation of cryptography given the critical role it plays in ensuring improved secure communications.

9.2 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:

a) National Convention Arms Control Act (Act 41 of 2002)
b) Electronic Communications and Transactions Act (Act 25 of 2002)
c) Electronic Communications Security (Pty) Ltd Act (Act 68 of 2002)
d) Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002)
e) State Information Technology Agency Act (Act 88 of 1998)
f) Conventional Arms Control Regulations (R7969 of 2004)
g) Cryptographic regulations (R8418 of 2006)

9.3 Taking into consideration the above-mentioned legislation, the NCPF recognises that there is a need to:

a) Review the existing legislation and regulations thereof; and

b) Develop an integrated regulatory framework for Cryptography for the country.

10. Online E-Identity Management in Cyberspace

10.1 It is noted that the Electronic Communications and Transactions Act, 2002 (Act 25 of 2002) (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 advanced electronic signatures and facilitates the recognition of electronic documents as legal and binding.

10.2 The NCPF notes that the South African Post Office (which in terms of the ECT Act, 2002 is a preferred service provider for advanced electronic signatures) has developed a Public Key Infrastructure (PKI) to support advanced electronic signatures (e-identity) and the Department of Public Service and Administration pursuant to its mandate in E-Government will develop a

PKI Strategy. The Department of Telecommunications and Postal Services (DOC), pursuant to its mandate established the South African Accreditation Authority to accredit and regulate authentication services and products.

10.3 The issue of identity management in cyberspace is central to building confidence and trust in the secure use of ICTs. The NCPF seeks to address the fragmented approach by promoting the development of 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.

10.4 The NCPF acknowledges that transmission of information over the Internet for trading and communication purposes presents 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, assist to address:

a) Authentication and securing of the identities of the parties to an e-transaction;

b) Confidentiality, ensuring information is kept private;

c) Integrity issues, by ensuring the information or process has not been modified or corrupted;

d) Non-repudiation issues, by ensuring that neither party can refute that the transaction occurred (i.e. the transaction is binding); and

e) The structure and regulatory framework for E-Identity and a Public Key Infrastructure.

10.5 The NCPF also requires that the development of a holistic National E-Identity and PKI Strategy should be aligned to the broader objectives set out herein and in particular the roles and the responsibilities of the critical stakeholders in the implementation of the NCPF.

11. Promote and Strengthen Local and International Cooperation

11.1 In terms of this policy framework, the Cybersecurity Hub will foster cooperation and coordination between the public sector, private sector and civil society.

11.2 Local cooperation

11.2.1 The NCPF promotes the Public-Private-Civil sector collaboration and the use of industry perspectives, equities and knowledge to enhance Cybersecurity. The Public-Private-Civil sector partnership is based on the understanding that Cybersecurity is everyone's responsibility and there is a need to leverage on joint knowledge and perspectives, to combat cybercrime.

11.2.2 The NCPF thus promotes the establishment of collaboration with local stakeholders, with a 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 trusted forums; and

(d) Creating a common understanding of the threats and vulnerabilities that the country faces and the responses required.

11.3 International Cooperation

11.3.1 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 cybercrimes.

11.3.2 Therefore, international collaboration is critical in securing cyberspaces nationally and globally. Recognising the need for global collaboration on matters regarding Cybersecurity, South Africa is required to collaborate with relevant and appropriate international organisations and governments, in line with 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 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 ICTs.

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

(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.

12. Capacity Development, Research and Development

12.1 The dynamic nature of Cybersecurity challenges necessitates the continuous development of capabilities and requisite skills.

12.2 **The NCPF therefore promotes:**

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 a Cybersecurity research and development agenda and enhancement of Cybersecurity research within South African Universities, industry and the Department of Science and Technology.

d) Enterprise development so as to grow the information security sector in terms of skills and growing enterprises that produce technology that protect cyberspace.

13. Cyber-warfare

13.1 In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. The NCPF thus promotes that a Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa, be developed, guided by the JCPS Cybersecurity Response Committee.

14. Promotion of a Cybersecurity Culture

14.1 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 of a Cybersecurity culture, the NCPF provides for inter alia:

14.1.1 Implementing Cybersecurity awareness programs for private sector, public sector and civil society users;

14.1.2 Encouraging business to develop a positive culture for Cybersecurity;

14.1.3 Supporting outreach to civil society, children and individual users;

14.1.4 Promoting a comprehensive national awareness program and guidelines;

14.1.5 Reviewing and updating existing privacy regime;

14.1.6 Develop awareness of cyber risks and available solutions;

14.1.7 Continuously review cyber applications and the impact from a Cybersecurity perspective.

14.1.8 Compliment the culture of Cybersecurity with online support mechanisms.

15. Technical and Operational Standards Compliance

15.1 The NCPF 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.

16. The Role and Responsibility of the State

This policy recognizes that there are a number of Organs of State that play a critical role in the implementation of Cybersecurity measures. 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 NCPF.

16.1 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.

a) The NCPF also requires the DOJ&CD to develop an implementation plan for the review and alignment of all Cybersecurity laws with the policy objectives and mandates of the State institutions as set out herein. In this regard, the DOJ&CD will be required to lead a process, in consultation with other JCPS Cluster Departments, for the review and alignment of Cybersecurity laws and will be required to submit progress reports to the JCPS Cluster Cybersecurity implementation team on a continuous basis in accordance with the approved JCPS implementation plan.

b) The process for the review of the Cybersecurity laws seeks to ensure that all relevant laws are aligned to this policy framework, and create a coherent and integrated cybercrime legal framework and 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.

16.2 The **Ministry of State Security** and **the State Security Agency (SSA)** has overall responsibility and accountability for coordination, development and implementation of Cybersecurity measures in the Republic as an integral part of its National Security mandate.

16.2.1 The Ministry of State Security and SSA shall, amongst others, be required to perform the following key roles and responsibilities in relation to cybersecutity in the Republic:

(a) Ensure that the JCPS cluster is properly capacitated and is able to perform its function as set out in this Policy framework including ensuring that the JCPS cluster has the the necessary capacity to monitor, promote and guide the implementation of the NCPF.

(b) Ensure, in consultation with the relevant stakeholders, the establishment of the Cybersecurity Response Committee, Cybersecurity Centre and proper function of the existing RSA Government CSIRT in line with the approved JCPS implementation plan.

(c) Initiate and lead a process within the JCPS cluster for the development and approval of guidelines and National security norms for the establsihment of various sector CSIRTs as provided for in the policy framework.

(d) Have an overall responsibility for the development and formulation of National Cybersecurity in Republic and in consultation with stakeholders. This includes reviewing and amending existing Cybersecurity policies as well as prescribing regulations on information and communications technology security for the Republic in order to advance the National Security interests of the Republic

(e) Provide information assurance and secure information and communications technology infrastructure of National importance in support of national security; This should include the development of State capacity to provide threat monitoring, alerting, co-ordination and response for information communications technology related incidents pertaining to National Critical Information Infrastructure of the State;

(f) Prescribe a regulatory framework for the control by the State of the provision and application of cryptographic solutions, development of National strategy and regulations for the protection of National Critical Information Infrastructure, and prescribe information communications technology security technical standards to which the electronic communications security products and services of organs of State must comply;

16.2.2 The implementation of these responsibilities by SSA shall 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.

16.3 The **Department of Police** and the SAPS shall, in terms of the NCPF, be responsible for the prevention, investigation and combating of cybercrime in the Republic, which includes development of cybercrime policies and strategies, and providing for specialized investigative capacity and interaction with national and international stakeholders. Development of the anti-cybercrime policy and implementation plans should include operational priorities pertaining to:

(a) The fight against child sexual/physical abuse material on the Internet;

(b) Actions to counter massive attacks against information systems such as "denial-of-service attacks (such as those affecting the banking sector);

(c) Actions combating identity fraud;

(d) The development of cross-border law enforcement cooperation;

(e) Public-private cooperation to fight cybercrime (in particular between law enforcement authorities and private companies); and

(f) 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.

16.4 The **Department of Telecommunications and Postal Services** (DTPS) has the responsibility for:

(a) Developing and implementing policies, regulations and industry standards regarding ICT aspects in general and to assist in the provision of 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 ICTs. This includes building trust and confidence in the secure use of ICTs and to advise the Minister of Telecommunications and Postal Services on policy and technical issues and other matters pertinent to Cybersecurity;

(b) Establishing the National Cybersecurity Advisory Council (NCAC) to advise the Minister of Telecommunications and Postal Services on policy and technical issues, and other matters pertinent to Cybersecurity pursuant to building confidence and trust in the secure use of ICTs;

(c) Establishing the Cybersecurity Hub and to facilitate the establishment of any other sector CSIRTs.

16.5 The **Department of Defence and Military Veterans (DOD&MV)** has overall responsibility for coordination, accountability and implementation of cyber defence 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.

16.6 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.

16.7 All other Organs of State are required to align their ICT policies and practices with this NCPF in so far as it relates to Cybersecurity.

17. The role and Responsibility of the Private Sector

17.1 The private sector is responsible for implementing information security measures at least equivalent to those that are implemented by Government. The NCPF therefore promotes cooperation between the information security bodies that predominantly represent the private sector with equivalent bodies in Government. The Department of Telecommunications and Postal Services (DTPS) and the National Cybersecurity Hub will help facilitate such cooperation.

18. The Role and Responsibility of Civil Society

18.1 Each person has a responsibility to ensure that his or her computer, mobile phone or any ICT infrastructure at his or her disposal that links to the cyberspace has updated malware protection. Each person also has a responsibility to report information security incidents to the police or the most accessible CSIRT. DTPS will help facilitate campaigns to raise awareness in this regard.

19. Conclusion

19.1 It is envisaged that the NCPF 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 national 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.