DRAFT POSITION PAPER

ON

INFORMATION SECURITY

AS PRESENTED BY THE DEPARTMENT OF PUBLIC SERVICE AND ADMINISTRATION

VERSION 0.3

TABLE OF CONTENT

1. OVERVIEW

The position paper on information security is intended to briefly contextualise issues around information security with a purpose of developing and contextualising information security related policies, strategies, standards and regulations in government. It is an attempt towards the organisation of a framework of proper plans and designs of secure information environments for the public servants and citizens. It is a stepping stone towards the establishment of core rules for safeguarding information from accidents, deliberate misuse illegal and harmful access. It is an integrated initiative which, seeks to offer all organs of state with the tools necessary to integrate Information Security best practice into day-to-day operations in the process of public service design and delivery. This document also seeks to guide and inform organisational and personnel behaviour on issues of information security. Of necessity, computer systems, which contain or process such information are also catered for in this framework.

In considering the information security framework and equation, roles and functions of various stakeholders and role-players have to be identified and clarified. What is at this stage important to mention is the fact that nowadays information in government exists in soft, electronic or computerised form. The future scenario (with the advent of the information society and knowledge economy) is that the amount of soft/electronic information will eventually exceed physical information. Modes of accessing and transferring information will continue to escalate in complexity and diversity with the advent of wireless/mobile technologies, Universal Mobile Telecommunications Systems, and what is often referred to as third generation technologies. This is even aggravated by the advent of convergence in multimedia technologies and end user information access devices

The department of Public Service and Administration is chiefly responsible for the management of information and processes leading to public service delivery in a secure and efficient manner. It is from this premise that this document is put together i.e. to create a platform and a stepping stone for debate and discussions around the issue of information security.

2. PURPOSE

Information Security is the cornerstone of success, this particularly so in the realm of post industrialisation characterised by information and knowledge as critical success factors for socio-economic productivity. Without a framework upon which to base standards and procedures, decisions are likely to be inconsistent and security holes will be present - ready to be exploited by both internally by other government officials and external persons alike.

Information can exist in many forms. It can be spoken, written, printed, stored physically and electronically, transmitted by post or electronically. It can be shown on films and broadcasted in all sorts of multimedia that are increasingly becoming easily available and accessible. The bottom line remains That in whatever way, manner or form the information might exist, it has to be protected against illegal, disruptive and harmful access in the interest of national security, crime prevention, effective and reliable business continuity.

The basic intention and purpose of this document is therefore to set the scene and build a framework for consultation. This involves: -

- (in line with international best practice), the endorsement of ISO 17799 as a de facto information security standard for government.
- The adoption of the Information Security Requirements as set in the proposed amended public service regulations
- the adoption of information security policies as a blue print to inform respective departmental and state organs' internal security policies.

3. OPPORTUNITIES CHALLENGES AND BENEFITS

In this day and age, it is highly improper for any individual or organisation not to safeguard his/her belongings. This applies to information particularly since it is increasingly growing to become a critical asset and component of the value chain of any organisation. The absence of security is the absence of a sense of ownership. It is the subjection to vulnerability, theft, prejudice, malice and destruction. In the context of governance and the state, national security, sovereignty and administration becomes at stake. A secure information environment allows the necessary functionality while protecting systems from intentional and unintentional manipulation or destruction.

The advent of cyberspace brings along with it promises of cost and time efficiency, and an omnipresence of public services. This correlates with the principles enshrouded in the "Batho Pele concept and goes a long way in deriving value out of the use of physical revenue for service delivery with the

aid of innovative technology. Protection, authenticity, non-reputability, confidence and integrity come upfront as the major benefits for the implementation of an information security framework. As government sets itself up as a role model user of technology, e-Government and information security will serve as a catalyst for e-commerce, e-business, the proliferation of the Internet, cyberspace and the leapfrog into the information society. e-Government security will assist profoundly in the bridging of the chasm of the digital and knowledge divide that exist within our country, as well as encourage the average citizen to participate more in the public domain thereby bringing the benefits of democracy to the people.

In order for one to appreciate the impact of information security, one has to look at the flip side of the coin i.e. the absence of such security. Adequate Information security policies underpin the security and well being of information resources. The government cannot afford to wait until there is a major loss through a security incident before anything in done to prevent this.

4. CURRENT SCENARIO & RELATED INITIATIVES

Many security audits and studies conducted across the globe concur that the greatest threat to information security comes from within the organisation. Employees pose the greatest threat to information security.

There is a lot of cross cutting issues in the information security environment. a lot of roles and functions as a result there of are overlapping. The DPSA is of the opinion that information security needs to be effectively executed in government irrespective of whom does this. To this effect we are in a process of putting together guidelines, policies and regulations around this issue as a platform for further debate and to provide clarity, eliminate duplications and fill in the gaps. In doing this, our point of departure is the ISO 17799, which is the universal standard for information security.

PROPOSED INFORMATION SECURITY FRAMEWORK & ISO 17799

The DPSA proposes adoption of the ISO 17799 Information Security framework, for Public Service. ISO 17799 deals with the following aspects, as contained in the e-Government Policy Framework Consultation Paper, and the ISO 17799:

- Securing Hardware, Peripherals and equipment
- Controlling access to Information
- Processing Information and Documents
- Purchasing and Maintaining Commercial Software

- Developing and Maintaining in-house software
- Combating Cyber Crime
- Complying with Legal and Policy Requirements
- Planning for Business Continuity
- Addressing Personnel Issues relating to security
- Controlling e-Transaction Information Security
- Delivering Training and Staff Awareness
- Dealing with Premises Related Considerations
- Detecting and Responding to Information Security Incidents
- Classifying Information and Data

In general (though not all exhaustive information security roles and responsibilities can be informed by the security grid as presented below: -

5. LEGAL FRAMEWORK

1. Public Service Act and Regulations

In terms of the Public Service Act, 1994, the **Minister for the Public Service and Administration** ("MPSA")is responsible for—

a. any policy which relates to **information management** and **information technology in the public service**; and

b. the provision of a framework of norms and standards with a view to giving effect to any such policy *(section 3(2)(a)(v) and (b))*.

c. The MPSA may make regulations in terms of the Public Service Act—

> regarding the **general security in departments**, as defined in the Act, and the **security requirements** with which employees must comply (section 41(1)(d)(iii)); and

The Public Service Regulations, 2001, contain the following provisions that relates to information technology security ("IT security"):

a. An employee may not release official information to the public unless she or he has the necessary authority (regulation II E of Chapter 1);

b. A **head of a department** must establish (I) an **information plan** that supports the planning process and objectives in respect of the strategic plan, (ii) an **information technology plan** that supports the information plan, and (iii) an **operational plan** that enables the implementation of the information technology plan and information management (regulation III E of Chapter 1); and

c. An **employee** must honour the **confidentially** of matters, documents and discussions, classified or implied as being confidential or secret (regulation C.4 of Chapter; see also clause 6 in Part 1 of Annexure 2 and clause 4 in Parts 2 and 3 of Annexure 2 for the confidentially clauses in the contracts of heads of departments and other members of the Senior Management Service).

d. in order to promote efficient, economic and effective use of resources and to improve the management and functioning of departments, subdepartments, branches, offices and institutions, regarding the management of information and the **utilisation of information technology** (section 41(1)(e)(iv)).

All the above is limited by the exclusion of the SANDF, SAPS, Department of Correctional Services, NIA, SASS and state educational institutions

2. State Information Technology Agency Act

According to the State Information Technology Agency Act 88 of 1998 ("SITA Act"), the **objective of the State Information Technology Agency** ("SITA") is to provide **information technology, information systems and related services** in a **maintained information systems security environment** to, or on behalf of, ***participating departments and organs of state*** and in regard to these services, act as an agent of the South African Government (section 6). The following terms are defined in that Act as follows:

> *"information systems"* means applications and systems to support the business whilst utilising information technology as an enabler or tool;

"information systems security" means to preserve the availability, integrity and confidentiality of information systems and information according to affordable security practices;

"information technology" means all aspects of technology which are used to manage and support the efficient gathering, processing, storing and dissemination of information as a strategic resource; and

"participating department" means any department making use of services provided by the Agency, i.e. SITA (section 1).

SITA must in the execution of its functions —

(a) maintain a comprehensive information systems security environment according to approved policy and standards; and

(b) adhere to the policies on information management and information technology and a framework of norms and standards to give effect to such policies, as well as regulations made in this regard by the MPSA in terms of the Public Service Act and the State Information Technology Agency Act (section 7(2) and (3)).

3. National Strategic Intelligence Act

In terms of the National Strategic Intelligence Act 39 of 1994, **the National Intelligence Agency must fulfil the national counterintelligence responsibilities**, and for this purpose must conduct and co-ordinate counterintelligence. According to that Act the term **"counterintelligence"** means **measures and activities** conducted, instituted or taken—

a. to impede and to neutralise the effectiveness of foreign or hostile intelligence operations;

b. to protect classified intelligence; and

c. to counter subversion, sabotage and terrorism aimed at, or against personnel, strategic installations or resources of the Republic (section 2(1)(b)).

The **South African Secret Service** ("SASS") must institute—

a. **counterintelligence measures within the SASS**; and

b. in consultation with the NIA, **counterintelligence measures outside the Republic** (section 2(2)(b)).

The functions of the **National Intelligence Co-ordinating Committee** ("Nicoc") includes—

a. the **co-ordination and prioritisation of intelligence** activities within the National Intelligence Structures, namely Nicoc, the

intelligence divisions of the SANDF and of the SAPS, NIA and SASS; and

making **recommendations to the Cabinet** on **intelligence priorities** (section 4(2)(b) and (f)).

The **NIA** must provide logistical, technical and administrative **support to Nicoc** (section 4(3)). The **Coordinator for Intelligence** must **manage and administer the functions of Nicoc** and **establish the structures** (including committees) necessary for the **efficient functioning of Nicoc** (section 5(1)).

4. Minimum Information Security Standards

4.1 On 6 December Cabinet approved the Minimum Information Security Standards ("MISS") document as national information security policy. **However, the necessary legal framework for the implementation of the MISS, has not taken place yet. Therefor it is approved policy, but these standards have not been laid down as legal prescripts by means of original legislation or subordinate legislation. Apparently, the MISS is currently under revision.**

4.2 Chapter 6 deals with communication security while Chapter 7 deals with computer security. According to paragraph 2 of Chapters 6 and 7, the authority to promulgate computer and communications policy is delegated to the Chairperson of the Functional Security Committee of the National Intelligence Co-ordinating Committee ("Nicoc") after the Chairperson has ensured that it is integrated and in line with policy regarding other security principles and legal principles were taken into account. Such policy is to be issued separately from the MISS, but is to be regarded as part of the MISS (par 1 of Chapters 6 and 7). The head of an institution is made responsible for the necessary security training and awareness of personnel using computers. The head of security of an institution must report breaches in the computer environment to NIA (par 8 of Chapter 7 and Chapter 9).

4.3 According to the MISS all computer storage media, when containing classified information, must be handled according to the document security standards contained in Chapter 4. Paragraph 5 of Chapter 4 deals with the transmission of documents by computer. Encryption as prescribed must be applied and a record must be kept of classified documents transmitted and received (par 5.1 and 5.2 of Chapter 4).

5. National Archives of South Africa Act

1. The National Archives of South Africa Act 43 of 1996 aims to provide for a National Archives, the proper management and care of the records of governmental bodies and the preservation and use of a national archival heritage. The word **"record"** is defined as "recorded information regardless of form or medium" (section 1). The term **"governmental body"** means any **legislative, executive, judicial or administrative organ of state** (including a statutory body) **at the national level of government** (section 1).

5.2 The objects and functions of the **National Archives** are *inter alia* to—

a. **preserve public** and non-public **records** with enduring value for use by the public and the State;

b. ensure the **proper management and care of all public records**;

c. maintain a national automated archival information retrieval system, in which all provincial archives services shall participate;

d. promote an awareness of archives and records management, and encourage archival and records management activities;

e. generally promote the preservation and use of a national archival heritage (section 3).

5.3 The **National Archivist** must inter alia take such **measures** as are necessary —

a. to arrange, describe and retrieve records (section 5(1)(a)); and

b. to preserve and restore records (section 11(4)).

5.4 Generally, the **National Archivist** is responsible for the **proper management and care of public records** in the custody (ie control of records based upon their physical possession) of governmental bodies (sections 13(1) and 1). The **National Archivist** must also determine—

a. records classification systems to be applied by governmental bodies;

b. the **conditions subject to which records may be** microfilmed or **electronically reproduced**; and

c. **the conditions subject to which electronic records systems should be managed** (section 13(2)(b)).

The term **"electronic records system"** means **"any records system in which information is generated electronically and stored by means of computer technology"** (section 1).

The **Minister for Arts, Culture, Science and Technology** may make **regulations** as to the **management and care of public records** in the custody of governmental bodies and, generally, with reference to any matter which is necessary or expedient to be prescribed in order to achieve or promote the objects of the National Archives of South Africa Act (sections 13(3) and 18). The **National Archivist** may from time to time issue **directives and instructions**, which shall not be inconsistent with the regulations, as to the **management and care of public records** in the custody of governmental bodies (section 13(4)).

The **head of a governmental body** must **designate** an official of the body to be the **records manager** of the body. The records manager is responsible to ensure that the governmental body complies with the requirements of the National Archives of South Africa Act. Additional powers and functions may be prescribed by regulation for a records manager. (See section 13(5).)

6. Protection of Information Act and Promotion of Access to Information Act

6.1 The Protection of Information Act 84 of 1982 creates offences and regulates incidental matters. It inter alia contains the following prohibitions:

- Prohibition of certain acts in relation to prohibited places
- Prohibition of obtaining and disclosure of certain information
- Prohibition of disclosure of certain information
- Prohibition of certain acts prejudicial to security or interests of Republic
- Obstructing persons on guard at prohibited places
- Harbouring or concealing certain persons and failing to report information relating to agents

Two of these relates to the functions of NIA and SASS and the compilation and disclosure of certain information (sections 3(b)(ii) and 4(1)(b)(i) of the Protection of Information Act).

6.2 The Promotion of Access to Information Act 2 of 2000 does not contain any general provisions relevant to information technology security in respect of public bodies. Concerning public bodies (as defined therein), the main object of that Act is to give effect to the constitutional right of access to information held by the State by providing procedures and mechanisms for exercising and enforcing that right. The Act also contains limitations on that right, namely grounds on which access to records of public bodies must or may be refused. It should be noted that one of the discretionary grounds of refusal is that a record of a public body may be refused if the record is a computer program (as defined in the Copyright Act 98 of 1978), owned by the State or any public body, unless that program is required to give access to a record to which access is granted under the Promotion of Access to Information Act (section 42(3)(d)).

6. Draft Electronic Transactions Bill

7.1 Part VIII (clauses 59 – 62) of the draft Electronic Transactions Bill *of 4 June 2001* ("draft Bill"), deals with the protection of critical databases. In clause 1—

a. **"critical data"** is defined as "data that are of critical importance to the national security of the Republic, and/or the economic and social well-being of its citizens"; and

b. **"critical database"** is defined as "organised collections of critical data in an electronic or digital form from where it may be accessed, reproduced or retracted data".

7.2 The **Minister of Communications** may, by notice in the *Gazette*—

a. declare certain classes of information to be critical date for the purposes of Part VIII; and

b. establish procedures to be followed in the identification of critical databases for the purposes of Part VIII (clause 60).

7.3 The **Minister of Communications** may, also by notice in the *Gazette*, prescribe—

a. requirements for the registration of critical databases with the Department of Communications or such other body as the Minister may specify;

b. procedures to be followed for registration;

c. any other matter relating to registration (clause 61).

7.4 The **Minister of Communications** may, by notice in the *Gazette*, prescribe matters relating to—

a. the **general management of critical databases**;

b. access to, and transfer and control of critical databases;

c. infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;

d. **procedures and technological methods to be used in the storage or archiving of critical databases**;

e. **disaster recovery plans** in the event of loss of critical databases or parts thereof; and

f. **any other matter required for the adequate *protection*, management and control of critical databases** (clause 62).

6. The Interception and Monitoring Bill

This Bill provides for the interception and monitoring of certain communications, postal articles. It provides for the prohibition of certain illegal telecommunications services that are cannot be monitored, intercepted or interpreted. It does so within the realm of other legislation i.e. criminal procedure, the constitutional rights to freedom and privacy, the democratic right to be informed etc.

4. ROLE PLAYERS AND STAKEHOLDERS

In determining the role players and stakeholders in the government information security environment, the roles and functions have to be comprehensively mapped in an all encompassing framework. This section must be read in context to the legal framework as provided in the previous section. Because information security is such a contagious and burning issue, there are quite clearly a lot of cross cutting roles. The premise for the DPSA is an outcome based approach that will provide a framework for the implementation of information security with minimum or no contestations for roles and functions amongst role players. The following should assist: -

1. The provision of Physical security

   This refers to security provided for on behalf of infrastructure that houses information. In the traditional environment, this refers to buildings, offices, drawers and cabinets etc. Whereas in the electronic/cyber environment this refers to computer hardware, servers, mainframes, systems and other end user access gadgets and devices. In most instances, it is the responsibility of the respective organisations to provide such type of security, however this must be provided for with reference to specific guidelines.

2. Content Security

   This refers to the safeguarding of all forms of actual audio, visual, and text content . Traditionally physical security goes to an extend in providing content security, however in the electronic environment, tangibility, physical location, time and distance become irrelevant. Content security in this instance is provided for by way of for example firewalls, passwords, access codes and biometrics, cryptography and encryption, Security measures provided for content can be varied with increasing levels of sophistication pending the sensitivity and secrecy of the information.

3. Network Security

   This refers to security provided for information in transit including transfer protocols, applications, switches and routers. The global trend in this scenario is to complement what is suggested in two above with a Public key infrastructure and certification to ensure authenticity, integrity, confidenciality and non-repudiation of communications, messages, transactions or information in transit.

4. Personnel security

   This refers to the security of individuals who deal with sensitive and top secret information.

The government wants to offer services for citizens that would the life cycle of public service needs for all citizens and corporations as illustrated below: -[2]

Stakeholders in this environment include, the National Intelligence Agency, South African Communications Security Agency, The Department of Communications, Department of Public Service and Administration, Department of Defence, The State Information Technology Agency, South African Police Services, Department of Arts culture Science and technology, NICOC, and the Justice Department[1]. The expectation is that the outcome of discussions around this document should inform the functions of each and every role player for policy and strategic purposes.

The Minister of Intelligence must do everything necessary for the efficient functioning, control and supervision of the coordination of intelligence supplied by the National Intelligence Structures. That Minister must perform any such function which affects a function of the SANDF or SAPS in consultation with the Minister responsible for the SANDF or SAPS, as the case may be. The Minister of Intelligence may make such regulations as to any matter which is necessary or expedient to be prescribed in order that the purpose of the National Strategic Intelligence Act may be achieved. Regulations that may affect a function of the SANDF or SAPS must be made in consultation with the relevant Minister. The regulations made under that Act may not be published in the Gazette, but must be notified to persons to whom it applies in such manner as the Minister of Intelligence may determine. (See section 6 as amended by section 26 of General Intelligence Law Amendment by Act 66 of 2001.) That Amendment Act is envisaged to commence on 1 July 2001.

The DPSA in this instance has an important facilitation role to play in ensuring that information security is comprehensively and effectively present for and on

behalf on all state information. Because most of the information (what is classified as critical information is synchronous and prevalent of the information and communications technologies, the Department of Communications has a role to play in ensuring the safety and authenticity of information in electronic or digital transit. this is the position as held in section 7 of the by the Interception and monitoring Bill.

In a nutshell (though not all inclusive)

- **NIA** sets information security standards, advises departments on action plans, formulate strategies to ensure business continuity
- **SACSA in conjunction with SITA** devices encryption algorithms to render data transmitted useless to anyone except the intended recipient
- **DoC** sets policies and standards on public communication media with a view of ensuring maximum availability.
- **DPSA** ingratiates Information Security to guide behaviour of Public Servants
- **Auditor General** appraises Departments for compliance with information security standards and whether business continuity was ensured
- **DACST** deals with aspects of archiving state information

in implementing an information security plan, the following considerations have to be taken into account: -

a. Risk Assessment

   This will assist to identify the vulnerability of the organisation in terms of information security attacks. It will assist in Identifying any potential

threat that may adversely affect state assets or network operations, especially the most critical elements within government; The risk assessment will then estimate the level that a given threat or vulnerability may actually happen based on established criteria for evaluating these factors; Identify and provide a system of priority ranking of valuable assets within the organisation for protection against identified and relevant risks. In this instance, the likelihood of attacks should be forecasted with the organisational potential impact. Risk assessment is therefore the determination of business harm that might arise as a result of absence or failure in security measures.

b. Weigh Options

The process here involves the Collection of data for measuring the impact of any potential loss or damage, including costs involved with the recovery or replacement. It involves a diagnosis of existing security solutions together with the associated policy framework, guidelines and regulations. The implementation of a security solution might for example infringe the constitution or the Promotion of Access to Information Act or any other associated legal clause. Where applicable, policies have to be re-viewed and re-aligned with realities as reflected in the risk assessment. The outcome of the weighing process ought to assist management in their selection of available cost-effective actions or mechanisms to mitigate or reduce potential risks

c. Implementing a solution

Care must be taken in this instance (particularly when dealing with government information) that the solution being implemented is a variation of other solutions available off the shelf in the global market of security provision. Where applicable an organ of state should be assigned the task of developing security solutions.

7. RECOMMENDATIONS

- All government information has to be protected against unlawful access.
- An established a central management focal point for information security management should be implemented with immediate effect;
- Information security should be approached in a holistic and balanced manner according to a specific framework.
- An outcome based approach is recommended. it is irrelevant who fulfils what aspect of the entire information security equation. suffice it to say that those roles have to be fulfilled.
- The DPSA should be tasked with continuing to manage the information security framework for government

- DPSA proposes regulations on Information Security, as contained in the draft Information Security Regulation, and accompanying Information Security Policies Handbook
- Awareness about security issues should be promoted
- Information security policies, procedures and regulations should be based upon the foundation of the SABS ISO/IEC 17799
- Different role players in this field have to interact and guide the GITO Council in order to produce a synergistic output. Critical role-players are identified to be NIA, DOC and DPSA
- Government should spend money on systems that comply with the general information security framework, and standards set by appropriate role players.
- No government department or any organ of state shall develop or produce an information security product or system if it is not done via the appropriate organisation or Agency
- In order to add to accountability all government data communications need to be facilitated by a system of authentication and non-repudiation.
- The role of SITA must be strengthened in the provision of information security solutions and monitoring for government

7. CONCLUSION

We want to continuously improve quality of life for South African citizens. This document begins to put issues into perspective in terms of information security in government. It serves as a platform for discussion, singling out some of the fundamental and salient issues around the topic of information security Questions of whom, how, where and how should and will be answered as follow-up to this document. Information security is critical and needs to be very tightly managed and provided in governance

Critical Success Factors

- co-ordination, collaboration, consolidation and consultation
- Senior management support and involvement
- Designated focal points and assigned responsibility
- Comprehensively defined policies and procedures
- Involvement of both business and technical experts
- Documentation, monitoring and maintenance