THE PROTECTION OF INFORMATION BILL

1. BACKGROUND

1.1 The Ministry State Security recognizes there are still inconsistencies and discrepancies in the current Act which must be dealt with. A review of the Protection of Information Act, 1982 (Act No. 84 of 1982), presently regulating the protection from disclosure of certain information, showed that the Act is outdated, due to the fact that it contains some provisions that are contrary to the Constitution and other legislation in that it contains legal presumptions which are deemed to be unconstitutional. It also does not provide sufficient protection for the State against information peddlers and current trends concerning espionage.

1.2 On 5 March 2008 Cabinet approved the submission of the Protection of Information Bill, 2008 to Parliament. The Bill was tabled in Parliament but then removed due its detailed and technical nature. The Joint Standing Committee on Intelligence amongst others, raised concerns relating to the following clauses: the public interest defence clause, hostile activity offences, disclosure of classified information offence, knowing (unlawful) possession of classified information offence and attempt clause. The Bill was accordingly sent back to the Ministry of State Security for redrafting.

1.3 Taking into account the concerns previously raised, the Protection of Information Bill was redrafted. This draft took into account comments of interested parties as well as practical provisions that are mandatory for the protection of information.

1.4 On 26 November 2009, the Bill was presented before the Cabinet Committee for Justice, Crime Prevention and Security. The Committee recommended that Cabinet notes a request that the Ministers of State Security and of Justice and Constitutional Development further consult on the possible inclusion of minimum sentencing in Chapter 11 of the Bill.

2. THE CURRENT INFORMATION PROTECTION REGIME

2.1 In the exercise of its executive authority to develop and implement national policy, the Cabinet on 4 December 1998, approved the Minimum Information Security

Standards ("MISS") as the national information security policy. The MISS replaced the former Guidelines for the Protection of Classified Information (SP 2/8/1) of March 1988. The MISS applies to all departments of State subject to the Public Service Act 103 of 1994 or any other department that handles classified information in the national interest.

2.2 The MISS set out a range of measures to protect classified information, including the classification and reclassification of documents, handling of classified documents, access to classified information, storage of classified document and removal of classified documents from premises. The MISS also provides for the security vetting of personnel. According to chapter 5 of the MISS, all persons who should have access to classified information must be subjected to security vetting. A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle. The MISS provides for specific vetting criteria, security screening procedures and period for the validity of security clearances. The MISS sets out security measures to protect classified information, including physical security, access control, computer security and communication security.

2.3 National laws and regulations prohibit the disclosure of certain information. Such laws include the *Protection of Information Act* 84 of 1982, as amended, the *South African Police Services Act* 68 of 1995, the *Intelligence Services Act* 65 of 2002, the *Intelligence Services Oversight Act* 40 of 1994, the *Defence Act* 42 of 2002 and the *Public Service Regulations,* 2001. Examples of such provisions includes:

- Section 4 of the *Protection of Information Act* 84 of 1982 prohibits the disclosure of protected documents or information in relation to, inter alia, security matters. However, it is deficient in many aspects, more specifically, it contains unconstitutional provisions relating to presumptions, it does not cater for relevant offences and minimum sentences and does not provide for criteria relating to State information before the courts.

- Section 26(a), (f) and (g) of the *Intelligence Services Act* 65 of 2002 makes it an offence for any person and members and former members of any intelligence service to disclose classified information under certain circumstances.

- Regulation E of Part II of Chapter 1 of the *Public Service Regulations,* 2001 prohibits an employee from releasing official information to the public without the necessary authority.

3. THE NEED FOR A NEW INFORMATION PROTECTION MECHANISM

3.1 The current system requires the spending of a great deal of government resources to protect a mass of information that does not actually require protection. The absence of a comprehensive statutory framework has resulted in an unstable and inconsistent classification and declassification environment, excessive costs and inadequate implementation. Government departments are straining under the burden of massive amounts of classified documentation. A lack of clarity and direction on what actually requires protection has resulted in this state of affairs.

3.2 The current protection mechanism, some of which was inherited from the apartheid era, encourages the needless protection of huge amounts f information. There still exists to some degree a default position of secrecy. This approach is inconsistent with South Africa's new constitutional order. ***The Bill aims to balance the presumption of secrecy with a presumption of openness.*** The aim of the current reforms is to significantly reduce the volume of information classified but at the same time to strengthen the protection of state information that truly requires protection.

3.3 A comprehensive statutory foundation for the classification and declassification of information is likely to result in a more stable and cost-effective set of policies and a more consistent application of rules and procedures. A legislative basis for the classification and declassification system, establishing clear guiding principles while retaining broad authority within government to establish and administer the details of the system, offers a practical and more predictable way to achieve meaningful changes.

3.4 A statutory framework is required which can deal with fundamental issues such as:

- What information may be classified and what information may not be classified?
- Who may classify information?
- When should classified information be declassified and who can declassify information?
- How long should information remain classified?
- What procedures for classification and declassification should be put in place and who should make such procedures?
- What system for the review of classified information should be put in place and what criteria or factors should be considered when classified information is reviewed?
- Should procedures be made for requests for the review of the classified status of information and if so what type of procedure and who may make such requests?
- Can declassified information be released to the public?
- What kind of oversight is required for the system of information protection?
- Should there be a central database with all declassified information which is available to the public and if so, who should establish and maintain such a database?
- What should be the prescribed procedures relating to State information during court proceedings?
- What are the relevant offences and minimum sentences relating to the offences?

3.5 The aim then is to ***provide a statutory framework which provides direction to those in government who are charged with information protection; substantially reduce the amount of state information that is protected from disclosure; provide more effective protection to that information that truly***

requires safeguarding; and to align the information protection regime with the values, rights and freedoms enshrined in the Constitution.

3.6 This Protection of Information Bill, attached as Annexure "1A", will ensure a coherent approach to the protection of State information; the classification and declassification of State information and will create a legislative framework for the State to respond to espionage and other related hostile activities. The Bill sets out procedures on how classified documents are to be handled during court proceedings, and requires court to prevent public disclosure of classified documents that form part of court records. It also does provide for specific espionage and related offences, such as, interception of or interference with classified information, provision of false information to a National Intelligence Structure and prohibition of disclosure of a State security matter. A first draft Bill was published in the *Gazette* for comments during March 2008.

4. EXECUTIVE SUMMARY OF THE BILL APPROVED BY CABINET, DECEMBER 2009

4.1 The broad aims of the bill which is to protect what actually has to be protected while avoiding excessive secrecy and where possible promote the free flow of information.

4.2 The constitutional framework for the protection of information is in broad terms the obligation imposed on government by the Constitution to, amongst other things, preserve the peace, secure the well being of the people of the Republic, protect and advance the national security, defend and protect the Republic, prevent, combat and investigate crime, establish and maintain intelligence services, provide effective and coherent government and provide effective and efficient public administration.

4.3 These constitutional obligations are carried out through the making of laws by Parliament, the creation of structures and institutions and the exercise of executive authority by the President together with other members of the Cabinet. The executive is specifically empowered to develop and implement national policy

and implement national legislation to achieve the constitutional objectives referred to above. Realizing such objectives includes the protection of information.

4.4 The Protection of Information Bill (the Bill) will ensure a coherent approach to protection of State information; the classification and declassification of State information and will create a legislative framework for the State to respond to espionage, associated hostile activities and other offences that relate to the vital protection of State information.

4.5 The Bill sets out procedures on how classified documents are to be handled during court proceedings, and requires courts to prevent public disclosure of classified documents that form part of court records.

5. OBJECTS OF BILL

The Bill seeks to-

(a) create a statutory framework for the protection of State information. State information is information generated by organs of State or is in the possession or control of organs of State;

(b) set out criteria and processes in terms of which State information may be protected from destruction or from unlawful disclosure;

(c) set out criteria and processes in terms of which information which is protected from disclosure and which is classified, may be declassified;

(d) create offences and proposed minimum sentences for unlawful disclosure of information, including the crime of espionage;

(e) make it an offence for an individual to knowingly supply false information to the national intelligence structures;

(f) establish guidelines for the treatment by courts of classified documents;

(g) provide for the Minister for State Security to issue regulations on information security across government; and

(h) repeal the existing Protection of Information Act (Act No. 84 of 1982).

5. STRATEGIC FOCUS AND OVERVIEW

6.1 South Africa, as highlighted in our National Intelligence Estimates, faces a huge threat of espionage and unauthorised disclosure of sensitive and valuable information that is in the hands of the State. This Bill is a key instrument to counter such threats by streamlining the procedures for enforcing such protection.

6.2 Chapter 1 provides detailed definitions of all technical terms and concepts. The statute will apply to all organs of State and natural and juristic persons. The Minister for State Security may, on good cause shown, exempt organs of State from certain provisions of the Act.

6.3 Chapter 2 outlines the principles which underpin the Act and which inform its implementation and interpretation.

6.4 Chapter 3 sets out National information security standards and departmental policies and procedures. Within 12 months of the date which this Act comes to effect, the Minister for State Security must issue National Information Security Standards prescribing broad categories of information that may be protected (classified or protected against destruction, alteration or loss). This chapter sets out what matters such standards may cover.

6.5 Chapter 4 addresses Information that requires protection against alteration, destruction or loss. This chapter sets out what information may be protected against alteration, destruction or loss (known as “valuable information”); the process of determining information as valuable; and how such information is to be protected.

6.6 Chapter 5 addresses Information which requires protection against disclosure. This chapter sets out what information may be protected from unlawful disclosure, and divides such information into three categories: “sensitive”, “commercial” and “personal”.

6.7 Chapter 6 addresses the Classification of information. This chapter set out principles that inform when to classify information; and outlines the method of classifying information. It also describes the three levels of classification: confidential, secret and top secret; and specifies who has the authority to classify information. Sensitive, commercial or personal information which is in material form may be protected by way of classification. Information may not remain classified for more than 20 years unless the head of the organ of State that classified the information certifies to the satisfaction of his or her Minister that continued protection against disclosure is critical to the national security of South Africa; necessary to prevent identifiable damage to the national interest; or necessary to prevent demonstrable physical or life threatening harm to a person or persons.

6.8 Chapter 7 addresses Criteria for continued classification of information. This chapter outlines the criteria that a head of an organ of State must consider in reviewing the classified status of information. It further sets out the procedure in terms of which interested third parties may request the head of an organ of State to review the status of classified material. Heads of organs of State are required to review the status of classified information at least once every ten years.

6.9 Chapter 8 addresses Transfer of records to national archives. Organs of State are required to review the status of information before transferring such information to the National Archives. Information transferred to the National Archives may not hold a classified status and shall be deemed to be automatically declassified. Existing classified information within the National Archives shall be subject to the declassification stipulations set out in the Act.

6.10 Chapter 9 addresses the Release of declassified information to public. Information that is declassified may be made available to the public in accordance with applicable national and departmental policies. A request made in term of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) for a classified record proceeds as determined in that Act. The classification must be reviewed and if it is decided that access is to be granted, the record must be declassified before it is made available.

6.11 The National Archives shall, in conjunction with those organs of State that originate classified information, establish a government-wide database of declassified information that heads of organs of State have determined may be made available to the public. Information contained within the database shall, at a reasonable cost, be made available and accessible to members of the public.

6.12 Chapter 10 addresses the Implementation and Monitoring. The Department for State Security shall have the responsibility to develop, coordinate and facilitate the implementation of national policies in an efficient and consistent manner across all organs of State. The responsibilities of this Department do not extend to the national intelligence structures such as the Department of Police and the Department of Defence and Military Veterans given that these departments have the necessary capacity and competence to implement the provisions contained in the Act.

6.13 Chapter 11 addresses Offences and penalties. This chapter provides for the following offences: Espionage offences; hostile activity offences; harbouring or concealing persons involved in espionage or hostile activities; unauthorised access to, interception of or interference with classified information; registration of agents and related offences; attempt, conspiracy, and inducing another person to commit an offence; disclosure of classified and related information; knowing

possession of classified information; destruction of valuable information; improper classification; disclosure of a state security matter. The penalties assigned vary on the basis of the nature of the offence and the actual or potential harm caused. This chapter further provides for the minimum sentences of offences.

6.14 Chapter 12 addresses the Protection of information before courts. This chapter outlines the process to be adopted by courts in the handling of classified documents that form part of court records. All documents with a classification shall remain protected by courts unless the courts direct otherwise.

7. IMPLEMENTATION PLAN

The Bill will be implemented in a phased manner. The provisions of the Bill, except for certain prescribed sections are suspended from operation pending the establishment of standards, policies, procedures and regulations contemplated in the Bill, or for a period of 18 months from the date on which the Bill takes effect, whichever occurs first.

8. ISSUES REDRESSED IN THE CURRENT PROTECTION OF INFORMATION BILL

8.1 The previous Bill submitted during the 2008 legislative period had received proposed amendments to be effected, namely, the insertion of espionage offences, hostile activities offences and a Proposed Public Interest Defence Clause.

8.2 The espionage offences and hostile activity offences have been duly incorporated into Chapter 11(sections 32 and 33) of the current Bill.

8.3 With regard to the Proposed Public Interest Defence Clause, it was the opinion of the drafters that the said recommendation should not be effected and incorporated into the current Bill as this clause creates legal uncertainty in the interpretation and application of the Bill.

8.4 The current Bill has addressed fundamental issues *inter-alia:*

- *Reduction of 4 classification levels to 3(Restricted Classification is redundant and therefore removed, other classification levels are sufficient);*

- *Includes various offences, inclusive of espionage and hostile activity(see chapter 11 sections 32 to 45 in this regard);*

- *Includes minimum sentences for the listed offences;*

- *Protection of State information before courts and the procedure relating thereto;*

- *The declassification of State information prior to the information being transferred to the National archives;*

- *Incorporating the Minimum Information Security Standards(MISS)which is a Cabinet guideline into legislation, thereby elevating the legal status of its provisions and procedures; and*

- *The removal of automatic declassification, this would have severe repercussion if there is such a clause.*