(b) Final Report of South African Human Rights Commission on African Diaspora Forum and 30 others v King Goodwill Zwelithini.

Referred to the **Portfolio Committee on Cooperative Governance and Traditional Affairs** for consideration and to the **Portfolio Committee on Justice and Correctional Services.**

COMMITTEE REPORTS

National Assembly and National Council of Provinces

PO BOX 15 Cape Town 8000 Republic of South Africa

www.parliament.gov.za

ANNUAL REPORT OF THE JOINT STANDING COMMITTEE ON INTELLIGENCE FOR THE FINANCIAL YEAR ENDING 31 MARCH 2016

1. INTRODUCTION

The Joint Standing Committee on Intelligence "The Committee or JSCI" is established in terms of section 2 of the Intelligence Services Oversight Act 1994, (Act No. 40 of 1994) ("The Oversight Act"). The purpose of the Committee is to perform an oversight function over the intelligence and counter-intelligence functions of the Services which includes the State Security Agency (SSA), the intelligence division of the South African National Defence Force and the intelligence division of the South African Police Service. The Committee hereby presents its report to the Parliament of the Republic of South African in accordance with section 6 of the aforementioned act.

2. COMPOSITION OF THE COMMITTEE AS AT 31 MARCH 2016

Name	**Political party**
Ms C C September	NA (ANC) Chairperson
Ms D E Dlakude	NA (ANC)
Ms Z S Dlamini-Dubazana	NA (ANC)
Mr D D Gamede	NA (ANC)
Mr D M Gumede	NA (ANC)
Mr C Nqakula	NA (ANC)
Mr J P Parkies	NCOP (ANC)
Mr O J Sefako	NCOP (ANC)
Mr J J Skosana	NA (ANC)
Ms T Wana	NCOP (ANC)
Mr H B Groenewald	NA (DA)
Mr H C Schmidt	NA (DA)
Mr DJ Stubbe	NA (DA)
Mr R N Cebekhulu	NA (IFP)
Mr B H Holomisa	NA (UDM)
Mr S C Mncwabe	NA (NFP)

Mr D L Twala (Economic Freedom Fighters) resigned as a Member of Parliament and the position was vacant as at 31 March 2016.

3. LEGISLATIVE MANDATE

Section 3 of the Oversight Act provides that the Committee, in exercising its oversight responsibility, performs inter alia, the following functions:

- Obtain audit and other reports from the Auditor-General and to consider the financial statements of the services;
- Obtain reports from the Evaluation Committee;
- Obtain reports from the designated judge as defined in the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (Act No. 70 of 2002);
- Obtain reports from the Ministers responsible for the Services;
- Consider and make recommendations on the report and certificates issued by the Inspector-General;
- Consider and make recommendations on all proposed legislation and regulation relating to any Service or any other intelligence or intelligence related activity;
- Review and make recommendations about co-operation, rationalisation and demarcation of intelligence functions performed by the Services;
- Order investigation by and to receive a report from the Head of a Service or the Inspector-General regarding any complaint received by the Committee from any member of the public provided such complaint is not trivial, vexatious or made in bad faith;

- Refer any matter in relation to an intelligence activity which the Committee regards as relevant to the promotion and respect of the Bill of Rights to the South African Human Rights Commission;
- Consider and make recommendations on matters falling within the purview of the Act and referred to the Committee by the President or a Minister responsible for any Service or Parliament;
- To request relevant officials to explain any aspect of reports furnished to the Committee;
- To hold hearings and subpoena witnesses on any matter relating to intelligence and national security; and to
- To consult with any member of Cabinet in relation to any function performed by the Committee in terms of the Oversight Act.

4. ACTIVITIES OF THE COMMITTEE

The Committee hereby reports on the following matters for the period 1 April 2015- 31 March 2016.

4.1 Allegations of Rogue Intelligence Unit at the South African Revenue Service (SARS)

The Joint Standing Committee on Intelligence “the Committee” (JSCI) received briefings from the South African Revenue Service (SARS) and the Office of the Inspector General of Intelligence on 12 May 2015. The SARS delegation was led by the Deputy Minister, Hon M Jonas accompanied by the Commissioner, Mr T Moyane and other seniormanagement members. Adv J Govender represented the Office of the Inspector General. The Minister of State Security was also present but did not make any presentation.

4.1.1 Presentation by the Deputy Minister of Finance and the Commissioner of SARS

The Committee was briefed on the Sikhakhane Report and the Advisory Board process that was headed by the retired Justice F Kroon. The findings of the Sikhakhane Report were as follows:

- The establishment, existence and operations of the National Research Group and or the High Risk Investigation Unit (HRIU) were unlawful and without the requisite statutory authority;
- That the unit was operated ostensibly in a covert manner and created a climate of intrigue, fear and subterfuge within SARS;
- Prima facie evidence that the unit may have abused its power and resources by engaging in activities that reside in other agencies of government and which the SARS had no authority to form;
- Prima facie evidence that the unit's activities may have included rogue behavior that had the potential to damage the reputation of SARS as an organ of state.

The Advisory panel led by retired Justice Kroon was to advise on the outcome of the Sikhakhane Report and to inter alia review governance structures.

The Commissioner advised that going forward it was a priority to establish a stable and efficient SARS tasked with the collection of all revenue due to the State. A review is being undertaken that is looking at the SARS operating model, value for money on the investment made by SARS, the efficiency and efficacy of systems, ownership of intellectual property to build internal capability and to ensure long-term sustainability and good governance processes. Furthermore, there are discussions and negotiations with the State Security Agency that have commenced with a view to establish a unit that will combat illicit trade within the parameters of the law and it is proposed to be located in SSA.

4.1.2 Presentation by the Office of the Inspector General of Intelligence

The Minister of State Security informed the Committee that he requested the Office of the Inspector General of Intelligence to investigate the allegations made against the SSA in an article published in the City Press on 10 August 2014. In the absence of an Inspector General of Intelligence, officials in the Office of the Inspector General briefed the Committee on the findings of the investigation. SARS falls outside the Inspector General's mandate and as such the report focused on various media allegations made against SSA. The Committee was informed that the allegations in the City Press article were investigated and that SSA was exonerated.

4.1.3 Committee Findings

- There is a need for an intelligence unit at SARS to combat illicit trade, amongst other things, but such intelligence capacity must operate within the legal framework;
- Investigations relating to criminal charges, if any, must reach finality as quickly as possible.

4.2 Process for filling the vacancy of the position of Inspector General of Intelligence

The Committee was seized to the process to fill the position of the Inspector General of Intelligence. The term of the previous incumbent came to an end on 31 March 2015. The position was advertised from 10 May 2015 and closed on 21 May 2015. The Committee received 58 applications. A subcommittee was established to consider applications and short candidates who met requirements. Shortlisting and interviews were to be held in open meetings.

The subcommittee submitted to the full JSCI Committee the following 11 (eleven) candidates for interviews: Mr Cecil Valentine Burgess; Mr Clinton Paul Davids, Mr Mathe Matthews Diseko, Mr Imtiaz Fazel, Ms Desire Fouche, Ms Annalize Gerber, Advocate Jayashree Govender, Mr Smanga Phillip Jele, Mr Andile Barnabas Kilifele, Mr Mampogoane Petrus Nchabeleng and Mr Mahlubandile Itumeleng Radebe. Interviews took place on 09 and 10 June 2015. On 17 June 2015 the Committee deliberated on the outcome of the interviews and Mr Cecil Valentine Burgess was nominated as the successful candidate to fill the position of the Inspector General of Intelligence.

The Committee adopted the report and it appeared in the ATC on 18 June 2015. During March 2016 the National Assembly resolved to refer the report back to the Committee for further processing. On 30 March 2016 the Committee considered the matter and resolved to re-advertise the position.

4.3 Annual Reports and Auditing of the Secret Services Accounts of the Intelligence Services

4.3.1 Annual Report: State Security Agency

The Minister of State Security informed the JSCI that the department achieved most of its set targets but was concerned about cybercrime and terrorism but that the department was making good progress on those matters. The department received a qualified report due to limited access to sensitive information that could compromise national security. The Minister further noted that the issue of the Inspector General should be finalised and a future discussion on the proposal of a deputy Inspector General should happen in the near future.

The Director-General provided details of the projects undertaken during the year under review with specific emphasis on those partially achieved. The Director-General proposed striking a balance and building a greater understanding in respect of the auditing of the intelligence community. In this regard the Deputy Minister proposed a workshop to build trust and understanding with auditors and the intelligence services.

4.3.2 Annual Report: Crime Intelligence

The JSCI was unhappy with the style and orientation of the report of the police's Crime Intelligence. The Minister suggested an agreed format of reporting between the Portfolio Committee on Police and the JSCI, to align the reports submitted to the two committees.

Crime Intelligence indicated that during the year under review it achieved all the targets that were set in its Annual Performance Plan. Irregular expenditure was due to non-compliance with Treasury Regulations as documents were seized during a court case. Until the documents were returned, the irregular expenditure would remain an issue. A significant improvement was that outstanding policies had been finalised. The Committee noted that notwithstanding the presentation not being in line with the Committee requirements, there has been an improvement.

4.3.3 Annual Report: Defence Intelligence

The delegation was led by the Minister of Defence and Military Veterans. The Minister gave a brief overview of the Annual report. The Special Defence Account received a qualified audit for the first time as a result of limited access to sensitive information by the Office of the Auditor General of South Africa (AGSA).

The presentation by Defence Intelligence indicated that most of the targets that were set were achieved. Challenges that were reported included funding of the Defence Intelligence function, the military degree and the relocation of Defence Intelligence to a new headquarters. The Committee asked for plans on the headquarters in order to assist where possible. The Minister instructed the delegation to arrange for another meeting to provide detailed steps on the project of the headquarters to the JSCI including any blockages and challenges that may be hindering the relocation progress.

4.3.5 Audit-Reports

Each Service received a qualified report from the AGSA. The Audit Reports are attached hereto as Annexure B. Notwithstanding the qualified reports there has been positive progress, especially in respect of the SSA. There will however always be situations where the AGSA will not have access to certain information while conducting the Audit.

The AGSA advised that due to the intelligence environment they do not have unlimited access to information. As a result it would be misleading to give an unqualified audit opinion. Spending that cannot be verified by the supporting documentation will inevitably be classified as irregular expenditure. There will however be continuous engagements with the Services on this matter. All Ministers in the security cluster will be met by the AGSA together with their Directors-General to discuss the matter.

During the Committee oversight visit in January 2016 the Committee requested all the Services and the Office of the Inspector General to meet with the Auditor General and report thereafter to the Committee on the outcome thereof.

4.3.6 Committee Findings and Recommendations:

- A balance must be found between the need for accountability and good financial governance and access to information that has national security and intelligence implications.
- All the Services must report to the Committee on the outcome of engagements with the Auditor-General.
- The funding of the Intelligence Services is a concern to the Committee. The Minister of Finance will be invited to advise on the correct measures the Committee can explore regarding the Budgetary Review process that the JSCI is currently not participating in;
- Economic Intelligence and Cybercrime must be prioritised by the Services going forward. Each Service must indicate how they contribute to improving the security of the State against Economic and Cybercrime.
- The Committee expressed concern that presentations by the Services did not provide the Committee with information regarding crimes such as drug trafficking, copper theft and illegal mining.
- The Committee required that all details of Crime Intelligence work are presented, not only overt operations. The mere reporting of facts and figures does not place the Committee in a position to determine whether a difference is being made on the ground, and the value being received for the budget that is provided.

4.4 Annual Report: Office of the Inspector General of Intelligence

As a result of the vacancy in the position of Inspector General of Intelligence (IG) senior officials presented the activities of the Office of the Inspector General (OIGI) for the year under review. Flowing from the presentations the Committee observed the following:

- The vacancies at senior management level at National Communications (NC) has an impact on the execution of the mandate of NC;
- Information leakage from the Services is a cause for concern;
- The absence of a Risk Management Committee to monitor internal risk controls;
- That the Committee is unable to consider and make recommendations on the report and certificate transmitted to it in terms of section 7(7)(d) read with sections 7(11)(c) and 7(11)(d) of the Oversight Act.

4.5 Report by the Designated Judge on the Interception of Electronic Communications

The Committee, in accordance with Section 3(a)(iii) of the Intelligence Services Oversight Act, 1994 (Act 40 of 1994) may obtain from any designated judge as defined in section 1 of the Regulation of Interception of Communications and Communication related Information Act, 2002, (RICA), a report regarding the functions performed by him or her in terms of that Act including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate: Provided that such report shall not disclose any information contained in an application or direction contemplated in section 3 of RICA.

The Report by the Designated Judge is attached hereto as Annexure C.

During January 2016 the Committee held a workshop with stakeholders involved in the implementation of RICA and findings and recommendations are included.

4.6 Border Management: Oversight Visit to the Province of KwaZulu Natal

4.6.1 Introduction

A parliamentary delegation comprising the Joint Standing Committee on Intelligence as well as the Portfolio Committees on Police, Home Affairs, Defence and Military Veterans, and International Relations and Cooperation embarked on a five-day border management oversight visit to KwaZulu Natal, on 15-18 September 2015. The purpose of the oversight visit was to focus on the following areas:

- *Land borders*: Challenges related to land border safeguarding; all forms of cross-border crime; crime and corruption at the ports of entry; border safeguarding of the areas between ports of entry; community engagement to ascertain levels of inter-departmental cooperation; and, readiness to integrate the Border Management Agency (BMA).
- *Maritime borders:* Challenges related to crime and corruption at the harbours; plans for the integration of the BMA; means to ensure the success of Operation Phakisa (advancing the Blue Economy); maritime territorial control including piracy and maritime crime; and, the status of the African Integrated Maritime Strategy.
- *Air borders*: Challenges related to airspace control; crime and corruption at air ports of entry; the status of radar control relating to South Africa's airspace; and, the BMA's approach to air border safeguarding.

A full report on this Joint Oversight Visit will be tabled separately from this report. In preparation for the oversight visit the JSCI received briefings from Crime Intelligence, Defence Intelligence and the State Security Agency.

South Africa's borders encompass land, air and maritime. The expanse and nature of South Africa's borderline contributes to complex safeguarding. Due to the porous nature of the country's borders, border safeguarding faces a number of problems which enable, inter alia, illegal migration; the spread of cross country diseases, human trafficking and other cross-border crimes. These problems are compounded by the threat of corruption and a lack of funding for border safeguarding purposes. Given these ongoing concerns, securing the borders must be prioritised.

4.6.2 Briefing on Border Management by Intelligence Services

Cross Border Criminal activity include inter alia:

- vehicle smuggling;
- poaching;
- illegal crossings;
- foreigners gaining access to government grants from South Africa;
- cigarette smuggling;
- livestock theft;
- Weapon smuggling from Mozambique and Swaziland via KZN to Lesotho, and
- Breach of airspace by low flying aircraft

The fight against the abovementioned cross border criminal activity and securing our borders is hindered by below average security at points of entry and inadequate scanners and CCTV equipment. Staff securing borders are not all adequately trained and some entry points are understaffed. Lack of adequate management personnel contributes to lack of control and increased corruption and collusion by staff. Fences along the border are in poor condition and border

patrols are ineffective. Maritime border security is hampered by the inadequate number of appropriate patrol boats while insufficient radar coverage compromises the safeguarding of air space.

Border security can be improved by having a greater visibility of the South African National Defence Force at identified areas, intelligence operations to be conducted at criminal hot spots and an increase of planned patrols at designated areas.

4.6.3 Committee findings and recommendations

- Intelligence operations are not yielding the desired outcomes
- Officials are inadequately trained and equipped
- Installation of CCTV cameras and scanners at land border posts are not prioritized
  - o There is no central database of illegal entrants, stowaways and asylum seekers to identify repeat offenders and persons who abuse refugee status applications.
  - o Corrupt and criminal activities by locals, government officials and taxi drivers providing information to illegal crossers and smugglers regarding roadblocks or presence of security forces at different points of the border line are not properly managed.
- Inadequate radar coverage compromises air border security.
- The Committee resolved to invite the Ministers of the Security Cluster to discuss the concerns identified during the joint oversight visit to the borders of KZN and to prioritise border management going forward.

4.7 Regulation of Interception of Communications and Communication related Information Act, 2002, (RICA): Oversight Visit from 25 to 29 January 2016

4.7.1 Introduction

The Committee visited the Interception Centres Office (OIC), and National Communications (NC). It also participated in a workshop with stakeholders involved in the implementation of RICA.

The workshop was a joint initiative between the Office of the Judge for interception and the Committee to better understand the challenges in the implementation of RICA. Amongst the stakeholders that attended were the Department of Justice and Constitutional Development, State Security Agency, Post and Telecommunication, Communications, Crime and Defence Intelligence.

4.7.2 Visit to the Office of Interception Centres (OIC)

The OIC is established in terms of section 33 of RICA and is responsible for, inter alia, the implementation of the provisions of RICA in relation to interception activities. The Acting Head of the OIC informed the Committee that the main function of the OIC is to facilitate the interception of electronic communication for the Services. The process to intercept requires firstly a warrant from the designated Judge. Secondly the warrant must be sent to the Service Provider who will then route the electronic communication of the target listed in the directive to the OIC. The OIC therefore does not have capability, on its own, to intercept any electronic communication without the warrant and the routing of the communication to the OIC by the service provider.

The Acting Head summarised the challenges facing the OIC as follows:

- Rapid technological advancement has resulted in technical directives being outdated. Most of the equipment installed at the OIC was done at its establishment in 2002.
- Advancement of technology has also resulted in a gap in the ability to intercept certain communications
- An improved electronic application system will enhance the directive application process and the fight against crime.

In concluding the OIC recommended the following:

- Review of RICA legislation
- Electronic application for an interception directive to be implemented as quickly as possible
- Complete review of the structure
- Disaster recovery system should be established

4.7.3 National Communications (NC)

National Communications (NC) is a branch within SSA that is comprised of the OIC, the National Communications Centre and COMSEC which was previously Electronic Communications Security (Pty) Ltd.

The Acting Head of National Communications summarised part of the NC function as follows:

- To analsye the electromagnetic spectrum and programme the acquired signals to extract usable information;

- To install and maintain Signal Intelligence (SIGINT) collection platforms; and to
- Conduct feasibility studies to identify new geographic signal collection sites

Similarly to the challenge experienced by the OIC, rapid advances in technology are not compatible with the outdated technology NC is presently using. NC summarised its challenges as follows:

- Rapidly changing technology;
- Inability to collect SIGINT information for
- Intelligence purposes;
- Limited Access to relevant source of signals;
- Signal coverage due to the geographic position of South Africa; and
- Intellectual and professional capacity in respect of Communications Security.

4.7.4 Workshop with RICA stakeholders

The workshop laid a foundation for further work that the Committee will pick up during the next reporting cycle before specific recommendations are made. The committee found that RICA is in urgent need of review. The outdated legislation, together with the outdated technology provides a gap that is exploited by criminals. There are many Stakeholders involved in the implementation of RICA they should work much more closely together. The Committee noted the good working relationship, and a level of trust, between the Designated Judge and the LEA's which contributed in achieving the balance between protecting the constitutional right to privacy and fighting crime.

Recommendations

- The funding of the Intelligence Services is a concern to the Committee. The Minister of Finance will have to advise on the correct measures the Committee can explore regarding the Budgetary Review process.
- Economic Intelligence and Cybercrime must be prioritised by the Services, with each Service indicating how they contribute to improving the security of the State against Economic and Cybercrime factors.
- SARS should establish an intelligence unit to combat illicit trade, amongst other things, but such intelligence capacity must be created and deployed within the legal framework.
- Relevant Ministers dealing with communication related matters (RICA) must be able to address the responsibilities and accountabilities of the Service Providers and to discuss the reliability of the country on the service providers.
- A central database of illegal entrants, stowaways and asylum seekers to identify repeat offenders and persons who abuse refugee status applications, should be established.

Report to be considered.

GLOSSARY OF ACRONYMS

AGSA	Auditor General of South Africa
BMA	Border Management Agency
IG	Inspector General
JSCI	Joint Standing Committee on Intelligence
KZN	Kwazulu Natal Province
NC	National Communications
OIC	Office of Interception Centres
OIGI	Office of the Inspector General of Intelligence
RICA	Regulation of Interception of Communications and Communication – related Information Act, 2002 (Act No. 70 of 2002)
SARS	South African Revenue Service
SIGINT	Signal Intelligence
SSA	State Security Agency

ANNUAL REPORT ON INTERCEPTION

OF

PRIVATE COMMUNICATIONS

PERIOD 2014/2015

By JUSTICE YVONNE MOKGORO

Designated Judge

To : Joint Standing Committee on Intelligence: Parliament

Date: 15 October 2015

STRUCTURE

1. INTRODUCTION

The need for good quality and timely intelligence to counter crime and security threats cannot be exaggerated. For that reason, good quality must include reliability of the intelligence gathered. Although the interception of electronic communications has for a number of obvious reasons become a preferred method of gathering crime intelligence, it is critical to be cognisant of the constitutional limitations of an intelligence method of interception as a first-even in the face of highly organised criminal syndicates.

The idea is to continuously strike the fine balance between ensuring legal compliance without frustrating effective intelligence method. This test is that of justification, finding good cause, based on the facts of the particular case as required in Section 16(2)(a) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), Act 70 of 2002.

Further, the escalation of cyber-crime and its increasing sophistication continue to pose grave challenges to law enforcement agencies fulfilling their duties optimally and most efficiently. Crime syndicates in particular, utilize these technologies successfully and with ease, planning and perpetrating serious crimes like:

- Human trafficking;
- drug dealing and drug trafficking;
- money laundering;
- corruption and fraud;
- kidnappings;
- assassinations;
- terrorism;
- heists; etc

This state of affairs, together with the escalating rate of technological crime and highly sophisticated criminal methods has made interception a popular method of investigation not only in South Africa but in almost every country in the world. Thus, the world over, interception of communications relative to the right to privacy and human dignity, is generally considered a necessary evil to protect law abiding citizens from criminal conduct.

2. INTERCEPTION

Lawful interception plays a crucial role in advancing intelligence as part of gathering the investigative method. It represents an indispensable means of gathering criminal intelligence.[1] The Regulation of Interception of Communications and Communication-related Information Act, 2002 (Act 70 of 2002), ("RICA"), was designed to allow the State to intercept communications and provide communication-related information during the investigation of serious crimes. The process must, however be legal in that it must be authorised by the designated judge.

The RICA provides the necessary guidance and requires strict compliance with the procedure that should be undertaken when applying for an interception direction from the designated judge.[2] When doing so, the RICA demands thorough appreciation and application of section 14 of the Constitution, which relates to the right to Privacy.

For that reason, the application for an interception direction must be considered as a last resort, as the RICA seeks to guard against its abuse and the violation of constitutionally protected rights.

[1] Notes on OECS Interception of Communications' Bill, page 6 found at: http://unpan 1.un.org/inradoc/groups/public/documents/TASF/UNPAN024636.pdf

[2] Regulations of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 RICA is the successor to the Interception and Monitoring Act 127 of 1992.

3. INTERNATIONAL LAW

To detect and investigate crimes that are committed through the use of electronic technology has been a global challenge for years. This resulted in the approval of the use of interception devises by the Council of Europe Convention, to which South Africa is a signatory. Almost all countries in the world, for example, the United Kingdom (Regulation of Investigatory Powers Act, 2000), the United States of America (, inter alia,Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as amended), Australia (Telecommunications (Interception) Act 1979), New Zeeland (Crimes Act and Misuse of Drugs Act), various countries in Europe etc, have adopted legislation to regulate the lawfully intercepted communications in order to combat criminal activities. In general the interception and monitoring of communications in all these countries balance the subject's right to privacy with that of the need to investigate and detect crime. Interception of communications in these countries is only allowed if it is judicially sanctioned or approved by an independent higher authority.

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

To deal with the question of finding better mechanisms in addressing this challenge, the South African Law Reform Commission (SALRC) felt it was important to undertake a review of the effectiveness of the then Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992). The investigation had shown that the Interception and Monitoring Prohibition Act, was outdated in that it did not adequately deal with new developments in the field of electronic technology and the use thereof in the commission of crimes.

As a result of the recommendations of the SALRC the Interception and Monitoring Prohibition Act, was replaced by the RICA. The aims of the RICA are, inter alia, to:

(a) Protect subjects of the Republic against the unlawful interception of communications;
(b) oblige all electronic communications service providers (ECSPS) to provide a service which is interceptable and which is able to store communication related information;
(c) provide for a structure which is responsible for the lawful interception of communications;

(d) oblige ECSPS to record and store information which can be used to identify their customers;

(e) prohibit the possession and manufacturing of interception devises;

(f) provide for the lawful interception of communications in emergency situations;

(g) provide that the interception of communications must, unless the RICA provides otherwise, be approved by a designated judge.

Some of these aspects are dealt with in more detail below:

4.1 Prohibition of interception of communication

The Regulations on Interception of Communications prohibit any person to intentionally intercept or attempt to intercept, or otherwise procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission unless it is done in terms of the provisions of the RICA.[3]

[3] Section 2

4.2 Interception in cases of emergency

In a case of an emergency, where there are reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person is being endangered, the applicant can orally request the ECSP concerned to intercept any communication to or from the sender in any other manner which the telecommunication deems appropriate or provide such assistance as may be necessary to determine the location of such a person (sections 7 and 8 of the RICA).[4]

These processes are however subject to judicial scrutiny in that the information obtained as well as affidavits from the ECSPS and law enforcement officers who requested the information must be submitted to the designated judge for scrutiny.

4.3 Application for issuing of directions and entry warrants

Under the RICA, a designated judge may authorise –

(a) the interception of direct or indirect communications by way of an interception direction in terms of section 16 of the RICA;(b)the interception of real-time

[4] Section 8(1)(b) and (aa)

communication-related information on an ongoing basis by means of a direction in terms of section 17 of the RICA;

(b) the combined interception of of direct or indirect communications, real-time communication-related and provision of archived communication-related information by means of a direction in terms of section 18 of RICA;

(c) the decryption of intercepted information by means of a decryption direction in terms of section section 21 of RICA; and

(d) entry warrants for the purposes of entering a premises for the placing of interception devices in terms of section 22 of RICA.

The above-mentioned directions or entry warrant can only be granted after the law enforcement agencies make a formal application to the designated judge. In considering such an application, the RICA imposes various factors that must be considered by the designated judge before he or she may grant a direction or entry warrant.

With regard to an interception direction, the Act compels any person who is authorised to intercept communication, to complete an application and submit it to the designated

judge for consideration. The application should clearly indicate, *inter alia,* the identity of the applicant, the identity of the law enforcement officer, the person whose communication is required and the telecommunication service provider to whom the direction must be addressed.[5]

To invoke the application of section 36 of the Constitution, the Act further requires the applicant, in his or her application, to include the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception applied for.[6] Furthermore, the application must indicate, where applicable, whether other investigative procedures have been applied and failed to produce the required evidence and why other investigative means are unlikely to succeed or appear to be too dangerous.[7]

An interception direction may be granted if the designated judge is satisfied that:

- A serious offence has been or is being or will be committed or public health or safety is threatened etc;

[5] Section 16
[6] Section 16(2)(d)(ii)
[7] Section 16(2)(e)

- the interception will provide information regarding the offence or threat;
- the facilities from which the communications will be intercepted are usually used by the person; and
- other investigative methods had been unsuccessful or too dangerous.

5. KEEPING OF RECORDS BY HEADS OF INTERCEPTION

The head of an interception centre (i.e The OIC) must on a quarterly basis submit to the State Security Agency (SSA) a written report of the records kept, abuses in connection with execution of directions and any defect in any electronic communications system which has been discovered.[8]

This obligation is there to ensure that there is full compliance with the RICA at all times.

[8] Section 37(1)(2)(a)(i-iii)

6. SUPPLEMENTARY DIRECTIONS REGARDING APPLICATIONS

A designated judge or designated judges, jointly, after consultation with the respective Judges-President of the High Courts, may issue directives to supplement the procedure for making applications for the issuing of directions or entry warrants and the directive issued must be submitted to parliament.[9] During the period of this report, no supplementary directions have been found necessary. Therefore, none has been issued.

7. THE ACT *vs* THE RIGHT TO PRIVACY

Section 14 of the Constitution protects everyone's right to privacy, which includes the right not to have "the privacy of their communications infringed".[10] Furthermore, Privacy is a fundamental human right recognised internationally in instruments like the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and regionally in the African Charter on Peoples' Rights, etc. It underpins human dignity and other key values such as freedom of association and freedom of speech.[11]

[9] Section 58(1) and (3)
[10] The Constitution of the Republic of South Africa, 1996
[11] Privacy and Human Rights-An International Survey and Privacy Laws-http://gilc.org/privacy/survey/intro.html

Article 8 of the Convention on Human Rights explicitly states that, "there shall be no interference by a public authority with the exercise of this right except in accordance with the law and to the extent that it is necessary in a democratic society and in the interests of national security, public safety or the economic well-being of the country. The right to privacy in this regard may also be limited in preventing disorder or crime, for the protection of health, or the rights and freedom of others".

The Article makes it clear that the information collected by enforcement agencies, must only relate to that which is identified by the warrant issued, such that, only persons or people who are suspected of committing serious offences or participating in activities against the interests of national security, may forfeit their right to privacy.[12]

In our Constitution, no right is absolute. All rights, including the right to privacy are limited, but only in terms of a law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.[13]

[12] European Convention on Human Rights for the Protection of Human Rights and Fundamental Freedom-www.hrcr.org/docs/Eur convention/euroconv3.html

[13] The Constitution of the Republic of South, section 36(1) 1996-Limitation Clause

Indeed, "the shift in balance towards absolute individual privacy is in itself a threat to security and the consequence of this choice will [in the context of the state of crime rates in South Africa] affect our personal safety, our right to live in a society where lawlessness is not tolerated and the ability of law enforcement to prevent serious and other violent criminal activity".[14]

In the matter of *The Investigating Directorate and Others v Hyundai Motor Distributions,* Justice Langa DP held that

> *"It is a notorious fact that the rate of crime in South Africa is unacceptably high. There are frequent reports of violent crime and incessant disclosures of fraudulent activity. This has a serious effect not only on the security of citizens and morale of the community but also on the country's economy. This ultimately affects the government's ability to address the pressing social welfare problems in South Africa. The need to fight crime is thus an important objective in our society…"[15], then*

[14] Lawful interception-Andres Rojab-centre for advanced Internet Architectures Swinburne University of Technology-Feb 9 2006- http://caia.swin.edu.au

[15] The Investigating Directorate and Others v Hyundai Motor Distributions (PTY) (LTD) 2001 (1) SA 545 (CC)

In *Califonia v Ciraolo* the court held,

> *"The right to privacy is not meant to shield criminal activities or to conceal evidence of crime from the criminal justice process, however, state officials are not entitled without good cause to invade the premises of persons for purposes of searching and seizing property…"*[16]

8. CHALLENGES

There is a continued general public perception that some law enforcement and other institutions and/or officers use these intrusive interception methods to advance their own interests with no regard to the rights and values the RICA aims to protect in the context of the Constitution. The media, in particular the social networks, are inundated with reports, allegations and comments of manipulation and abuse of the interception system by officials and even individuals, ranging from-

- obtaining of information in less than 36 hours, without the Designated Judge's knowledge;
- acquisition of cell phone billing and ownership records through crime intelligence, without the Judge's knowledge or approval, in order to expedite the investigation;

[16] California v Ciraolo 476 US 207 (1985) at 213-4

- obtaining text messages and cell phone billing records needed for personal reasons, through a contact at crime intelligence and/or the service providers;
- the popularity of interception method which is preferred over conventional methods of investigation;
- the apparent lack of trust of the Designated Judge with regard to information gathered through crime intelligence;
- failure of applicants to provide fact-based justification for an application to the Judge;
- applicant's need to comprehend that suspicion of crime without any factual basis is not sufficient for application for interception;
- the tendency for vagueness of basis for an application, the cut and paste approach to an affidavit and the tendency to regard the authorisation for interception as a given and therefore the taking and

- wide allegations of bribery of contacts at banks and telecommunications service providers etc.[17]

Not all of these challenges may be resolved through legislative amendments. Some may only be resolved through the dedication, commitment, full understanding and appreciation of the important role of investigation officers gathering crime intelligence in a democratic society based on the values of human dignity, freedom and equality. The need to sharpen and constantly improve the investigative skills and prowess of our law enforcement officers comes to mind - no doubt an important aspect of contemporary policing.

9. RICA AND THE FUTURE

The RICA was assented to on 30 December 2002 and came into operation on 30 September 2005. From 2002 to date, there have been substantial developments that took place in the electronic communications field. The Electronic Communications Act, 2005 (Act 36 of 2005), introduced a new electronic communications dispensation in South Africa, moving away from the dispensation envisaged in the RICA, where there is a clear, distinction based on a

[17] How the government spies on you-Mail and Guardian Online-http://mg.co.za/articles/2011-10-14

fixed line, internet and mobile cellular communications based on the Telecommunications Act, 1996 (Act No. 103 of 1996). The RICA should therefore be revamped to bring the terminology in line with the current electronic communications dispensation as is envisaged in the Electronic Communications Act, 2005.

New services are seeing the light, inter alia, Black Berry Messenger Services, BlackBerry Enterprise Services, Skype and a host of other services, which is mostly Internet based, which is clearly not interceptable, and even if it were interceptable, the encryption that is applied to such services makes it nearly impossible for the law enforcement agencies to obtain any information on the content of a communication. This aspect must be further investigated in order to find a solution.

The RICA needs to be revised in light of the obligations which the Republic may incur if we accede to the African Union Convention on the establishment of a credible legal framework for cyber security in Africa in order to deal with cybercrime.

The RICA should in so far as if possible regularly be revised in order to ensure that it keeps pace with ongoing developments.

9.1 Amendments to the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002) (the RICA)

The Department of Justice and Constitutional Development has indicated that legislation which affects various amendments to the RICA is on the legislative program of the Department for the 2016/2017 financial year. Amendments which are considered are, among others, amendments which are aimed at –

(a) facilitating an electronic process for applications for directions and service of directions contemplated in Chapter 3 of the RICA;

(b) ensuring the integrity of the process of obtaining customer information;

(c) further regulating listed equipment provided for in sections 44, 45 and 46 of the RICA;

(d) complimenting information sharing between electronic communications service providers and Government agencies;

(e) further providing for interception capabilities of law enforcement agencies;

(f) imposing obligations on electronic communications service providers who provide an internet service to record and store call related information; and

(g) appoint a regulatory body to ensure compliance with the RICA by the electronic communications service providers.

The terminology used in the RICA will also be reviewed to address interpretation problems which are being experienced.

A specific problem was identified which relates to the RICA registration process, provided for in section 40, where the particulars of customers were incorrectly captured. According to available information, certain persons RICAed various SIM-cards in their name and thereafter sold the SIM-cards to other persons without complying with section 40(5) of RICA. In terms of section 40(5) of the RICA, any person who sells or in any manner provides an activated SIM-card to another person (other than a family member), as well as the person who receives the SIM-card, must, immediately upon the sale or provision of the SIM-card, provide the relevant electronic communication service

provider with their full names, surnames and identity numbers. Specific amendments are introduced to address this shortcoming in the RICA.

9.2 The Cybercrimes and Cybersecurity Bill, 2015 (the Bill)

The Department of Justice and Constitutional Development has recently published the Bill for public comment. The Bill–

(a) comprehensively criminalises offences which can be committed in cyberspace;

(b) provides for expanded jurisdiction;

(c) gives law enforcement agencies cyber specific investigative powers;

(d) deals with international co-operation in matters relating to cybercrime;

(e) provides for the establishment of various structures in Government to deal with cybercrime and cybersecurity;

(f) provides for the protection of critical information infrastructures;

(g) deals with certain aspects of evidence;

(h) imposes obligations on electronic communications service providers to report cybercrime and to provide assistance to their clients to curb cybercrime; and

(i) provides for international agreements between the Republic and foreign States or territories.

The Bill also affects amendments to other legislation, among others, the RICA.

The Bill contains provisions which ensure that there is synergy between the RICA and the Bill in so far as it relates to information which must be obtained to investigate or prove cybercrimes (clauses 39, 40 and 41).

In so far as international co-operation is concerned the Bill introduces new processes, which involve the office of the designated Judge, see clauses 41(3) to (11) (disclosure of data) and clauses 46 to 48 (requests for international co-operation). If Parliament follows the course proposed in the Bill it will mean that the workload of the office of the designated judge will increase substantially and it is hoped that the office of the designated judge will be expanded accordingly.

In terms of clause 66 of the Bill, the Schedule to the RICA is amended by the inclusion of the various offences contemplated in the Bill in the Schedule to the RICA. The Schedule to the RICA is further amended to include offences which are substantially similar to the offences provided for in the Bill, which are or was committed in a foreign State or territory. The effect of these amendments is that the RICA can be used to intercept indirect communications, real-time communication-related information and archived communication-related information in respect to the offences provided for in the Bill.

10. NEW LAW ENFORCEMENT AGENCY (NLEA)

Two additional agencies namely South African National Defence Force (SANDF) and Financial Intelligence Centre (FIC) has started to submit applications for interception during 2014. The Designated Judge has provided the necessary workshop to both these agencies, with a view to heighten the consciousness, understanding and appreciation of the need for the submission of RICA compliance application at all times.

11. SOME INFORMATION ON "GRABBER" AND OTHER LISTENING DEVICES.

Under the RICA Act, the devices utilised by various Law Enforcement Agencies do not require the designated Judge's authorisation. Once authorisation has been obtained to install a listening device, the nature of the device does not require approval of the designated judge. Whatever challenges are experienced in that regard can be explained by the particular agencies.

12. STATISTICAL INFORMATION OF APPLICATIONS FOR DIRECTIONS

12.1 State Security Agency (SSA)

Figures for the period are as follows:

	2014/2015	2013/2014
• New Applications	41	28
• Re-applications	52	34
• Amendments	57	38
• Extensions	54	35
• Combined Amendments and Extensions	23	13
• Entry Warrants (Installation of listening devices)	4	5
• Section 11 (Application for RICA information)	103	66

• Refusals	10	5
• Oral Applications for Interceptions (i.t.o Section 7 & 8)	4	2
• **Total**	**348**	**231**

12.2 THE SOUTH AFRICAN POLICE SERVICES (SAPS)

Figures for the period are as follow:

	2014/2015	**2013/2014**
• New Applications	233	158
• Re-applications	35	23
• Amendments	12	10
• Extensions	36	6
• Refusals	0	0
• Amendments and Extensions	70	22
• **Total**	**386**	**385**

12.3 THE SOUTH AFRICAN SECRET SERVICE(SASS)

Figures for the period are as follow:

	2014/2015	**2013/2014**
• New Applications	2	2
• Refusals	0	0
Total	**2**	**2**

12.4 FINANCIAL INTELLIGENCE CENTRE(FIC)

Figures for the period are as follow:

	2014/2015	2013/2014
• New Applications	6	3
• Amendments	1	
• Extensions	7	
• Amendments & extensions	3	
• Refusals	1	0
Total	**18**	**3**

12.5 SOUTH AFRICAN NATIONAL DEFENCE FORCE (SANDF)

Figures for the period are as follow:

	2014/2015	2013/2014
• New Applications	5	3
• Amendments	1	1
• Refusals	0	0
Total	**6**	**4**

Combined figures for SSA, SAPS, SASS, FIC and SANDF are as follow:

	2014/2015	**2013/2014**
• Applications (New)	286	194
• Re-applications	87	56
• Amendments	71	49
• Extensions	97	41
• Amendments and Extensions	96	35
• Entry Warrants	4	5
• Section(11)	103	66
• Oral intercepts	4	2
• Refusals	11	5
• **Total**	**760**	**453**

The total number of all applications for interception in the current financial year has increased by 296 from the total of application in the previous year. Four (4) Entry Warrants, the most invasive of all interceptions had been applied for and granted. All four (4) has been requested by SSA and were therefore obtained for States Security investigations. Similarly in the 2013/2014 financial year five (5) Entry Warrants had been applied for by SSA and were also granted. No other agency had applied for Entry Warrant in

the last financial year. Oral applications are submitted in cases of utmost urgency. Four (4) applications had been submitted and all 4 had been for purposes of the SSA investigations and were approved.

13. THE SUCCESS RATE OF INTERCEPTION.

The rate of success of the interception method in the fight against crime is not easily discernable. It may be argued that the number of successful interceptions is equal to the number of applications for extension of existing interception directions, in that every application for extension requires clear indication of the relevant court – admissible evidence obtained in the last direction and what further information is intended to be obtained to make a case against a target right for prosecution. Besides, the successful prosecution of a particular target does not rely only on information obtained through interception. Success depend on a holistic approach to the investigation of a particular case.

The success of interception as an investigative method is therefore highly subjective.

14. ADMINISTRATION

The Office for the Control of Interception and Monitoring of Communications, processes applications submitted to the designated Judge in terms of the provisions of the Regulation of Interception of Communications and Communication-related Information Act,2002(Act 70 of 2002) (the RICA).

14.1 Staffing

The staff component comprises of six officials namely Assistant. Director, Legal Administration Officer, Administration Officer, Chief Administration Clerk, Receptionist and Registry Clerk. Their responsibilities in brief are as follows.

14.2 Office Manager (Ass. Director)

Planning and organizing activities of the component. Provide leadership pertaining to financial and administrative Services. Manage processing of applications. Liaising with all stakeholders in Law enforcement. Co-ordinating activities of all law enforcement agencies. Duties also include staff management, asset management, compilation of statistics, ensure high level of confidentiality in the office and provides overall executive support to the office of the designated Judge.

14.3 Legal Administration Officer

Provides Legal support to the designated Judge. She is responsible for all the research required by the designated Judge to facilitate the role and functions of the designated Judge, including compilation of information for public presentations, seminars, workshops and conferences.

14.4 Administration Officer

Render secretarial and administrative duties to the Judge, provides administrative support for the office as a whole, processes all payments and assists with efficient management of stores and assists clients daily.

14.5 Chief Registry Clerk

Supervision of Registry personnel ensures proper handling of records, ensures proper execution of track and trace list and also ensures that documents are delivered to National Office and Office for Interception Centres.

14.6 Receptionist

Performs receptionist functions, performs clerical duties, supports the Judge and other staff members, filing and updating all records.

14.7 Registry clerk

Opening, closing and disposing of files according to National Archival Instructions, ensures correct placing of records, maintains proper track and trace lists daily, re-filing daily and related miscellaneous tasks.

14.8 Budget

Historically, the office of the Designated Judge does not have its own budget. It continues to function as a component of the Higher and Record Management Directorate in the Department of Justice and Correctional Services. All requisitions are therefore subject to approval by the Director (PAIA and Records Management) who manages the resources of the Unit in terms of need.

14.9 OFFICE INFRASTRUCTURE

Furniture

The Office is in dire need of new office furniture, filing system, new telephone system, official cell phones for Chief Registry Clerk and Administration Officer. A request was made for the purchase of office furniture on the 25/07/2013. The request was forwarded to the Director

(PAIA & Interception). In it was approved by the then Acting Deputy Director-General (Corporate Services) on the 01/08/2013.The office was later advised that there is no funding for furniture.

Official cell phones

A request was made for official cellular phones for Chief Registry Clerk and Administration Officer. It was forwarded to the designated official on the 30 July 2013. The office is still awaiting a response in this regard.

Why the need for cell phones?

The office deals with application on a 24hrs basis. The Chief registry Clerk transports the applications daily to the Judge. It is therefore necessary to be reachable and be able to make contacts by telephone at all times.

Mobile Filing System

Why Mobile Filling System?

The office handles top secret documents which must be stored for a minimum period of 5 years. In order to comply with the Archival Act, storage is a challenge. A mobile filling system will address this difficulty.

A request to purchase mobile filing system was forwarded to the Director on the 30 July 2013. We are still waiting for a response.

15. CONCLUSION

Indeed, that the system of lawful interception of private communications may be open to abuse is a likelihood that we should not be blinded to.it could be for expediency where the legal application process may be overly cumbersome. However, abuse in any form cannot be tolerated. However, together the relevant monitoring systems are well-functioning, ever conscious of the need for utmost vigilance.

As a matter of fact, that the approach of the designated judge has been one of capacity-building among others:

- Two annual workshops on the understanding of the interceptions application process and its challenges, in the context of the constitutional provisions and values are planned, and two (2) have been conducted by the designated judge-for the benefit of all sectors and role players in the interception process.

- Individual attention is provided where necessary, giving specific comments on the shortcomings of each application and continuously conscientising applicants of the importance of the realisation that interception directions are not there for the taking and shall be justified by facts which point to the commission of a crime or a crime in process and
- The need to be ever conscious that interception is not an investigative method of first resort. It is employed only once conventional methods have been shown in the application to have been ineffective and or impossible, due to the particular circumstances of the case.

This capacity-building method has been highly effective and generally welcomed. The response to the workshops and the above individual attention has borne positive results, e.g mere suspicion is not based on sex generally no longer viewed as basis for an interception application and there is clear appreciation that an application for an interception direction is not there for the taking.

Report of the auditor-general to parliament on the South African police service crime intelligence: secret service account

Report on the financial statements

Introduction

1. I have audited the financial statements of the South African Police Service Crime Intelligence: Secret Account set out on pages XXX to XXX, which comprise the *appropriation statement, the statement of financial position as at 31 March 2015, the* statement of financial performance, statement of changes in net assets and cash flow statement for the year then ended, as well as the notes, comprising a summary of significant accounting policies and other explanatory information.

Accounting officer's responsibility for the financial statements

2. The accounting officer is responsible for the preparation and fair presentation of these financial statements in accordance with the Modified Cash (MCS) Standard prescribed by the National Treasury and the requirements of the Public Finance Management Act of South Africa, 1999 (Act No. 1 of 1999) (PFMA), and for such internal control as the accounting officer determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor-general's responsibility

3. My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with International Standards on Auditing. Those standards require that I comply with ethical requirements, and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

4. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

5. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my qualified audit opinion.

Basis for qualified opinion

Level of audit assurance

6. Owing to the nature of certain operational transactions and the circumstances under which they are incurred and recorded as well as the circumstances under which the assets and services are procured and utilised, the level of assurance in respect of certain operational expenditure is, under these circumstances lower than with ordinary audits.

Qualified opinion

7. In my opinion, except for the possible effects of the matter described in the basis for qualified opinion paragraph, the financial statements present fairly, in all material respects, the financial position of the South African Police Service Crime Intelligence: Secret Service Account as at 31 March 2015, and its financial performance and cash flows for the year then ended, in accordance with the MCS and the requirements of the PFMA.

Report on other legal and regulatory requirements

8. In accordance with the Public Audit Act of South Africa, 2004 (Act No. 25 of 2004) and the general notice issued in terms thereof, I have a responsibility to report findings on the reported performance information against predetermined objectives for selected programmes presented in the annual performance report, non-compliance with legislation and internal control. The objective of my tests was to identify reportable findings as described under each subheading but not to gather evidence to express assurance on these matters. Accordingly, I do not express an opinion or conclusion on these matters.

Predetermined objectives

9. I performed procedures to obtain evidence about the usefulness and reliability of the reported performance information for the following selected programme presented in the annual performance report of the account for the year ended 31 March 2015:

   - Programme 1 – crime intelligence on pages XX to XX

10. I evaluated the reported performance information against the overall criteria of usefulness and reliability.

11. I evaluated the usefulness of the reported performance information to determine whether it was presented in accordance with the National Treasury's annual reporting principles and whether the reported performance was consistent with the planned programme. I further performed tests to determine whether indicators and targets were well defined, verifiable, specific, measurable, time bound and relevant, as required by the National Treasury's Framework for managing programme performance information (FMPPI).

12. I assessed the reliability of the reported performance information to determine whether it was valid, accurate and complete.

13. I did not identify any material findings on the usefulness and reliability of the reported performance information for programme 1: crime intelligence.

Additional matter

14. Although I identified no material findings on the usefulness and reliability of the reported performance information for the selected programme, I draw attention to the following matter:

Achievement of planned targets

15. Refer to the annual performance report on pages XX to XX for information on the achievement of planned targets for the year.

Compliance with legislation

16. I performed procedures to obtain evidence that the account had complied with applicable legislation regarding financial matters, financial management and other related matters. I did not identify any instances of material non-compliance with specific matters in key legislation, as set out in the general notice issued in terms of the PAA.

Internal control

17. I considered internal control relevant to my audit of the financial statements, annual performance report and compliance with legislation. I did not identify any significant deficiencies in internal control.

Other reports

Investigations

18. A criminal investigation is currently being conducted since 2011/12, by the Hawks (Department of Priority Crime Investigations (DPCI)) into allegations of misuse and abuse of the Department's funds by certain members.

Auditor - General

Pretoria

23 July 2015

AUDITOR-GENERAL
SOUTH AFRICA

Auditing to build public confidence

Report of the auditor-general to Parliament on the State Security Agency

Report on the financial statements

Introduction

1. I have audited the financial statements of the State Security Agency set out on pages xx to xx, which comprise the statement of financial position as at 31 March 2015, the statement of financial performance, statement of changes in net assets and cash flow statement for the year then ended, as well as the notes, comprising a summary of significant accounting policies and other explanatory information.

Accounting officer's responsibility for the financial statements

2. The accounting officer is responsible for the preparation and fair presentation of these financial statements in accordance with the South African Standards of Generally Recognised Accounting Practice (SA Standards of GRAP) and the requirements of the *Public Finance Management Act of South Africa*, 1999 (Act No. 1 of 1999) (PFMA), and for such internal control as the accounting officer determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor-general's responsibility

3. My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with International Standards on Auditing. Those standards require that I comply with ethical requirements, and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

4. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

5. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my qualified audit opinion.

Basis for qualified opinion

High inherent risk due to the nature of the environment

6. The State Security Agency accounts for non-sensitive and sensitive project expenditure incurred in connection with the performance of the function and the duty of the Intelligence Services as defined in section 1 of the Intelligence Services Act, 2002 (Act 65 of 2002). The level of assurance that can be given by my audit on sensitive projects expenditure and assets included in notes 7 and 18 to the financial statements respectively, is lower than in the case of other audits due to the significant inherent risk relating to the sensitivity of the environment in which they are incurred and the manner in which they are recorded. This expenditure amounts to 9,6% of the 2014/15 financial year's total budget.

Qualified opinion

7. In my opinion, except for the possible effect of the matter described in the basis for qualified opinion paragraph, the financial statements present fairly, in all material respects, the financial position of the State Security Agency as at 31 March 2015 and its financial performance and cash flows for the year then ended, in accordance with the SA Standards of GRAP and the requirements of the PFMA.

Emphasis of matters

8. I draw attention to the matters below. My opinion is not modified in respect of these matters.

Claims against the department

9. With reference to note 33 to the financial statements, the department is opposing several claims instituted against it. The ultimate outcome of these matters cannot presently be determined and as a result no provision for any liability has been raised.

Restatement of corresponding figures

10. As disclosed in note 30 to the financial statements, the corresponding figures for 31 March 2014 have been restated as a result of an error discovered during the year ended 31 March 2015 in the financial statements of the SSA at, and for the year ended, 31 March 2014.

Additional matters

11. I draw attention to the matters below. My opinion is not modified in respect of these matters.

Supplementary explanations of budget variances presented outside the financial statements

12. The supplementary explanations of budget variances contained in the appropriation statement do not form part of the financial statements. I have not audited these explanations and, accordingly, do not express an opinion thereon.

Report on other legal and regulatory requirements

13. In accordance with the Public Audit Act of South Africa, 2004 (Act No. 25 of 2004) (PAA) and the general notice issued in terms thereof, I have a responsibility to report findings on the reported performance information against predetermined objectives for selected programmes presented in the annual performance report, compliance with legislation and internal control. The objective of my tests was to identify reportable findings as described under each subheading but not to gather evidence to express assurance on these matters. Accordingly, I do not express an opinion or conclusion on these matters.

Predetermined objectives

14. I performed procedures to obtain evidence about the usefulness and reliability of the reported performance information for the following selected programmes presented in the annual performance report of the State Security Agency for the year ended 31 March 2015:

    - Programme 2: Domestic intelligence on pages xx to xx
    - Programme 3: Foreign intelligence on pages xx to xx.

15. I evaluated the reported performance information against the overall criteria of usefulness and reliability.

16. I evaluated the usefulness of the reported performance information to determine whether it was presented in accordance with the National Treasury's annual reporting principles and whether the reported performance was consistent with the planned programmes. I further performed tests to determine whether indicators and targets were well defined, verifiable, specific, measurable, time bound and relevant, as required by the National Treasury's *Framework for managing programme performance information* (FMPPI).

17. I assessed the reliability of the reported performance information to determine whether it was valid, accurate and complete.

18. The material findings in respect of the selected programmes are as follows:

Domestic intelligence

Usefulness of reported performance information

19. I did not raise any material findings on the usefulness of the reported performance information for the programme

Reliability of reported performance information

20. The FMPPI requires auditees to have appropriate systems to collect, collate, verify and store performance information to ensure valid, accurate and complete reporting of actual achievements against planned objectives, indicators and targets. Significantly important targets were not reliable when compared to the source information or evidence provided. This was due to a lack of documented system descriptions for the accurate recording of actual achievements, monitoring of the completeness of source documentation in support of actual achievements and frequent review of the validity of reported achievements against source.

Foreign Intelligence

Usefulness and reliability of reported performance information

21. All material findings raised on the usefulness and reliability of the reported performance information for the programme were subsequently resolved.

Additional matter

22. I draw attention to the following matter:

Achievement of planned targets

23. Refer to the annual performance report on pages xx to xx and xx to xx for information on the achievement of the planned targets for the year. This information should be considered in the context of the material findings on the reliability of the reported performance information for the selected programmes reported in paragraphs xx to xx of this report.

Adjustment of material misstatements

24. I identified material misstatements in the annual performance report submitted for auditing on the reported performance information for programme 2: Domestic intelligence and programme: 3 Foreign intelligence. As management subsequently corrected only some of the misstatements, I raised material findings on the reliability of the reported performance information

Compliance with legislation

25. I performed procedures to obtain evidence that the department had complied with applicable legislation regarding financial matters, financial management and other related matters. My findings relating to material non-compliance with specific matters in key legislation, as set out in the general notice issued in terms of the PAA, are as follows:

Strategic planning and performance management

26. Specific and appropriate information systems to enable the department to monitor the progress made towards achieving the goals, targets and core objectives as indicated in the strategic and annual performance plan did not exist, in contravention of public service regulation part IIIB.1(f)(i)(ii).

27. Procedures for the facilitation of effective performance monitoring, evaluation and corrective action were not established as required by treasury regulation 5.3.1.

Expenditure management

28. Effective steps were not taken to prevent irregular expenditure, as prescribed by section 38(1)(c)(ii) of the PFMA and treasury regulation 9.1.1.

Internal control

29. I considered internal control relevant to my audit of the financial statements, the annual performance report and compliance with legislation. The matters reported below are limited to the significant internal control deficiencies that resulted in the basis for qualified opinion, the findings on the annual performance report and the findings on compliance with legislation included in this report.

Leadership

30. Processes and controls relating to the oversight and review of performance information need to be enhanced and strengthened. This will ensure that the annual performance report submitted for audit is accurate and complete.

31. The policies and procedures for travel and accommodation, including covert travel and accommodation, should be updated to prevent irregular expenditure due to inadequate procurement procedures.

Other reports

Investigations

32. As reported in the 2011-12 regularity audit report, an investigation was conducted into alleged fraud at Opmed. The matter was reported to the South African Police Service. Two former NIA/Opmed members were charged and found guilty in the Pretoria Specialised Commercial Court. The cases against other members and service providers are continuing.

33. An investigation was instituted after reports that transfers were made from NIA's account, within Momentum, to the account of a broker. This matter was reported to the Financial Services Board (FSB) and Financial Advisory and Intermediary Services (FAIS) for investigation. The investigation was completed and the matter was referred to the NPA and Hawks for further consideration.

34. An investigation was instituted at the Covert Support Unit. The deputy director-general: Operations, together with three other members, was suspended pending the outcome of the investigation. In December 2010 the director-general accepted the deputy director-general's resignation. The investigation is still ongoing.

35. The Inspector General is conducting an investigation at the request of the director-general. The investigation relates to operational expenditure transactions and is currently still in progress.

Auditor - General

Pretoria

17 September 2015

AUDITOR-GENERAL
SOUTH AFRICA

Auditing to build public confidence