An exploration of the chasm in the protection of classified information in South African government departments

by

LEHLOHONOLO WONDERBOY MAHLATSI

Submitted in the partial fulfilment of the degree of

MAGISTER TECHNOLOGIAE

In the subject

Forensic Investigation

at the

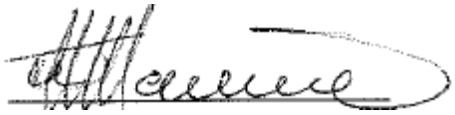
UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF R SNYMAN

JANUARY 2019

DECLARATION

I, Lehlohonolo Wonderboy Mahlatsi, hereby declare that this dissertation (An exploration of the chasm in the protection of classified information in South African government departments) submitted for the Magister in Forensic Investigation at the University of South Africa is my own original work and has not been previously submitted in any institution of higher education. I further declare that all sources cited or quoted are indicated and acknowledged by means of a comprehensive list of references.



Lehlohonolo Wonderboy Mahlatsi

Student number : 43312829

2018/10/20

CONFIRMATION OF LANGUAGE EDITING

I, Jack Chokwe, hereby declare that I have edited the master's dissertation entitled: "An exploration of the chasm in the protection of classified information in South African government departments" by Lehlohonolo Wonderboy Mahlatsi. An editing certificate has been provided to confirm the professional and proofreading of this dissertation. See Addendum B.

2018/10/27
Date

DEDICATION AND ACKNOWLEDGEMENTS

This study is dedicated to my late sister, Puleng Cynthia Mahlatsi, may her soul rest in peace "Mase". The struggle of a black girl in South Africa continues. #Azania

I would like thank God with Jesus Christ, Jesus Christ with our Comforter, the lion king of Juda, God Messiah to our parents, God Messiah to us, God Messiah to our children and their children in the future.

I would like to acknowledge the following people:

1. My mother, Pinky Susan Mahlatsi, I see her sacrifices in my children's eyes. I would like to thank my mom for the love and support. Enkosi Makhulu.

2. My father, Priest Joseph Mahlatsi, he was right, it is better to die for an idea that will live, than to live for an idea that will die. vitória é certa.

3. To my brothers, Lebo and Sabata Mahlatsi, my sister Mazzet, my cousins, nephews and niece, for your infinite love and content encouragement. Aluta continua.

4. My in-laws, Mr & Mrs Mokheseng, for remembering me in their prayers, and for their loyal support. Kea leboha.

5. My supervisor, Professor Rika Snyman, for her continuous guidance and support throughout my study. Baie dankie.

6. My life coach, Pitso Hlapane, for introducing me to the seven habits of highly effective people. Kgotso Mongaka.

7. My mentor, Dr Rachel Morake, for the incalculable value she has added to my life with her patient guidance, support and motivation. Modimo ke oo.

8. My Editor, Mr Jack Chokwe, I would like to express my sincere appreciation to him for editing my work.

9. Last but most important, to my wife Maki Jerminah Mahlatsi nee' Mokheseng and the girls, Lerato and Leano Mahlatsi, for their patient love, support and understanding during demanding times. May God remember you like Noah, protect you like David, resurrect you like Jesus, and let his will be your wheel always. Kea leboha Mabanyana.

   Tau e Sutlhile…

SUMMARY

The chasm in the protection of classified information in South African government indicates that all the departments have at their disposal information that is to some extent sensitive in nature and obviously requires security measures. This study shows that government officials who in their official duties come to contact with classified information are either vulnerable or are implementing the security controls incorrectly. It is also clear that in the absence of a comprehensive statutory framework, the government departments' classified information has resulted in an unstable and inconsistent classification and declassification environment. The statutory framework would, in addition to other things, address the rising threat of espionage and antagonistic activities, the selling of information and the protection of critical records in government, without hindering the constitutional rights of citizens to access information. This would create a system of valuable informantion and clarify which information requires security measures with respect to the protection of classified information.

KAKARETSO

Kgaohanao e tshireletsong ya tlhahisoleseding e sirelеditsweng ke mmuso wa Afrika Borwa e supa hore mafapha ohle a ona a na le tlhahisoleseding eo, ka ho hong, e leng ya sephiri mme e hloka maemo a tshireletso. Boithuto bona bo bontsha hore bahlanka ba mmuso bao, tshebetsong ya bona ya semmuso, ba teanang le tlhahisoleseding ya sephiri, ba kotsing hobane ba sebedisa ditaelo tsa polokeho ka mokgwa o fosahetseng. Ho boetse ho hlakile hore, bosikong ba moralo o phethahetseng wa semolao, disistimi tse sa sebetseng hantle tsa mafapa a mmuso tsa tlhahisoleseding ya sephiri di bakile tikoloho e sa tsitsang hape e sa hlophiswang ya tlhophiso le tloso ya tlhophiso ya tlhahisoleseding. Moralo wa semolao, hara tse ding, o ka sebetsana le phephetso e eketsehang ya bohlwela le diketsahalo tse ding tse belaetsang tse jwalo ka thekiso ya tlhahisoleseding, mme o sireletse direkote tsa mmuso tsa bohlokwa ntle le ho hatakela tokelo ya Molaotheo ya baahi ya phihlello ho tlhahisoleseding. Hona ho ka theha sistimi ya tlhahisoleseding ya bohlokwa le ho hlakisa hore na ke tlhahisoleseding efe e hlokang maemo a tshireletso ha ho tluwa ntlheng polokeho ya tlhahisoleseding ya sephiri.

ISISHWANKATHELO

Umsantsa okhoyo ekukhuseleni ulwazi olukhethekileyo kurhulumente woMzantsi Afrika ubonisa ukuba onke amaSebe anolwazi analo olunokuba nkenenkene, kwaye oludinga ukhuseleko. Esi sifundo sibonisa ukuba asesichengeni amagosa karhulumente aye athi apha ekusebenzeni kwawo, adibane nolwazi olukhethekileyo, ngoba azisebenzisa gwenxa iindlela zokulawula ukhuseleko. Kukwacaca ukuba, ekubeni kungekho sikhokelo namigaqo isemthethweni, iinkqubo ezingasebenzi kakuhle zamaSebe karhulumente, ulwazi olukhethekileyo aluhlelwa ngendlela eyiyo kwaye lufumaneka kwiimeko ezingaluphathi ngokukhetheka. Ubukho besikhokelo nemigaqo yokhuseleko lolwazi inganceda ekunqandeni isoyikiso esikhulu sobhukuqo mbuso nezinye iziganeko ezikrokrisayo, ezifana nokuthengiswa kolwazi, Esi sikhokelo singanceda nasekukhuseleni iingxelo zikarhulumente ezinkenenkene ngaphandle kokucinezela amalungelo abemi okufumana ulwazi njengoko uvuma uMgaqo Siseko. Oku kuya kuvelisa inkqubo yolwazi olunexabiso kwaye kuya kucacisa ukuba loluphi ulwazi oludinga imimiselo yokhuseleko malunga nokukhuselwa kolwazi olukhethekileyo.

LIST OF KEY TERMS

Classified Information

Confidential

Protection of Security

Restricted

Screcy

Scurity Threats

South African Government Departments

Threats

Top-Secret

Vulnerabilities

LIST OF ABBREVIATIONS

CAL POLY	-	California Polytechnic
DCAF	-	Geneva Centre for the Democratic of Armed Forces
DSD	-	Department of Social Development
DIRCO	-	Department of International Relations and Cooperation
E-mail	-	Electronic Mail
HESA	-	Higher Education South Africa
ICT	-	Information Computer Technology
IM	-	Instant Messaging
IT	-	Information Technology
MISS	-	Minimum Information Security Standard
NICOC	-	National Intelligence Coordinating Committee
NPA	-	National Procecuting Authority
PAIA	-	Promotion of Access to Information Act
POPI	-	Protection of Personal Information
RSA	-	Republic of South Africa
SAPA	-	South African Press Association
SAPS	-	South African Police Service
SJSU	-	San Jose State University
SRCM	-	Security Risk Control Measures
SSA	-	State Security Agency
UNISA	-	University of South Africa

TABLE OF CONTENTS

CHAPTER 1
GENERAL ORIENTATION AND METHODOLOGY

1.1 INTRODUCTION

The South African government departments work very closely with all the South African Security Clusters and other government institutions to stabilise the Republic of South Africa (RSA). The departments depend on the information that is collected, generated, processed, and finalised, in other to achieve the government's mandate. The government departments attract business opportunities from all over the world, including developed countries. Therefore, the protection of classified information is essential to the departments and the country at large. The government departments have invested tremendously in information security and yet it appears as though their system is infiltrated on a daily basis.

The aim of the research study was to explore the protection of classified information in the South African government departments. The researcher embarked on the background to the research problem and the nature, scope, and extent of the problem. The researcher presented the research aim, research purpose, and research questions. The key concepts of the research were articulated, the value of the research, the preliminary literature study, research approach design, and data collection. The researcher further included the method to ensure the trustworthiness of the study, ethical considerations and concluded in this chapter.

1.2 BACKGROUND TO THE RESEARCH PROBLEM

The South African government departments produce highly sensitive information that requires protection, however, the country does not have a statutory framework that provides protection to the government's classified information. The statutory framework can provide government departments that are entrusted with sensitive information, with the guidelines on how to manage the classification of information. It can also give direction on how the reclassification and declassification of information process are conducted. The proposed South African Protection of Information Bill,

which repeals the Protection of Information Act 84 of 1982 (South Africa, 1982), regulate the process in which the government classified information must be protected. The Bill ensures that the government's valuable information is not stolen or disclosed to unauthorised people. The submission of the Protection of Information Bill was approved by the South African Cabinet on the 5th of March 2008. It was later referred back by the Parliament, as a result of its technicalities and some of the details. Some of the concerns clauses that were raised by the Joint Standing Committee on Intelligence, includes the disclosure of classified information offense, hostile activity offenses, and public interest defence clause. The Bill was appropriately returned to the State Security for revision.

State Security Agency (SSA) (South Africa, 2010) indicates that the Protection of Information Bill was revised. The views of the interested parties were taken into consideration, as well as empirical provisions that are mandatory for the protection of government classified information. The Bill was presented before the Cabinet Committee for Justice, Crime Prevention and Security on the 26 November 2009. 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.

The South African Cabinet approved the Minimum Information Security Standard (MISS) on 4 December 1998 as the national information security policy. The MISS replaced the former Guidelines for the Protection of Classified Information of March 1988. The MISS applies to all the South African government departments, and the South African Police Service (SAPS).

The apartheid government used intelligence system to mislead the public and interest parties on State Information. Their method of record keeping was working parallel to State information that was meant to be accessible to the public. The State had a system that allows people to access State Information and they kept classified information restricted. The methods symbolize the apartheid government, which allowed the State to operate in secrecy, lack accountability, promote inequalities and abuse its powers. Prior to democratic South Africa in 1994, the apartheid government destroyed a lot of classified information without following procedures. To redress the

apartheid the mistakes of the past regimes, access to information was included as a constitutional right in South Africa (Currie, 2003:60).

The apartheid system valued the power of information secrecy and enforced it to promote an anti-democratic society that was uninformed, precisely because they knew the impact it can make on the South African public. All other rights were basically compromised without the rights of access to information and declaration (McKinley, 2003). Consequently, the democratic South African rejects to use similar methods that was used by anti-democratic State. The 2008 version of the Bill was very clear on redressing the apartheid methods of record keeping and it further provided the decisive automatic declassification of records that were produced during the apartheid regime. The Bill considered how the apartheid State system used information secrecy to oppress the people, which stay outside of the archival custody beyond a period of 20 years (Harris, 2013).

Section 32 of the Constitution of the RSA, 1996, provides that everyone has a right of access to any information held by the State. Like any other right in the Constitution, this right may be limited by law to the extent necessary to protect other important rights and interest. South Africa has a comprehensive law setting out the procedures for relying on the right of access to information and the reason why the request may be refused. This is the Promotion of Access to Information Act 2 of 2000 (PAIA), an Act specifically provided for in the Constitution. Though it limits the right to access to information, PAIA is widely regarded as doing so in a constitutionally permissible manner. It strikes, in other words, the proper balance between the right to governmental transparency and the need to protect important countervailing interests. These include national security, defence, economic interests, and the criminal justice system. A law like PAIA, that is intended to restrict access to information that has been classified in order to protect national security will necessarily be the one that limits section 32 of the Constitution (Harris, 2013).

The South African media has over the years played an influential role in the all facets of the country, either positively or negatively. The media has always been viewed as a tool that has the potential to unite the people. The role manner in which the media platform has been utilized has a direct impact on the country's democracy because if

it is negatively exploited, it is likely to develop an uncertainty to the investors. In recent years, the media has made it its business to criticize the political principals and their political parties. The media has always been seen as an essential democratic institution that can add value to sustainable development goals of the country. It can also promote equalities, social justice, peace an inclusive societies. The National Council of Provinces has defended The Protection of State Information Bill (2010) on the issue of silencing the South African media. Nevertheless, the concerns on the Bill will have an alarming effect on the media and would prevent and discourage the culture of information leaking. Its main objective is to ensure that intelligence structures are managing the government classified information according to the constitution of the country (Southall, 2012).

Nathan (2009) indicates that the intelligence institutions need to be clear on which information meets the requirements of secrecy and which information must be transparent. In the democratic States, the constitution of the country must be observed when making these determinations. These principles incorporate government that is honest, open and that values the public's rights to access data held by the government. They are fundamental since they are essential for responsibility and oversight, political and individual opportunity, popularity based contestation of intensity, hearty discussion and trade of thoughts, the full exercise of citizenship and the avoidance of maltreatment of power. The similar rationale is clear in South Africa's Protection of State Information Bill; which tries to empower the general public, encourages everyone to full practices and ensure that their rights are protected. Conversely, as indicated by PAIA, the arrangement of government under apartheid did not respond to the public demands on transparency, and neither did they promote the culture of openness. The system encouraged the public and private sectors to abuse its powers and violate the rights of the citizens.

The MISS (South Africa, 1998) opine that government departments require security measures that would protect the sensitive information that they produce and process. The protection of government information is determined by the degree of sensitivity, which gives guidance on how information must be classified or graded. After the determination of sensitivity, the information would be labelled classified information, and it would require specific security measures. (South Africa, 1998). Democratic

South Africa still applies the protection mechanism that was used by the apartheid State, which encourages the unnecessary protection of massive amounts of information. This method contradicts the order of the new Constitution of South Africa, because to some degree, there is a default of secrecy. The Bill aims to reduce the volume of classified information in the government departments and balance the presumption of secrecy with the presumption of transparency. Furthermore, it also provides direction on which government information needs to be protected.

1.3 THE NATURE, SCOPE AND EXTEND OF THE PROBLEM

In this research, the problem is the quality of protection of classified information in the government departments. Grama (2011:10) asserts that the number of vulnerabilities appears to be growing and there are flaws in how internal information security is applied. The security breach allows aggressors to identify employees and hack their personal and work accounts, posing a threat to State Security. Nkwana (2015:4) alludes that the equipment that store classified information in the government departments is stolen regularly. Nkwana (2015:4) further states that the level of security breaches and unauthorized information disclosure is very high, despite the departments' efforts to manage confidentiality and integrity.

Price (2009) alludes that the departments that manage a high volume of sensitive information must contend with the internal officials who are breaching the security. In the environment, that process financial, privacy, personal and classified government information, should be aware of insider threat. The Protection of Information Bill indicates who has an authority to classify State information. Chapter 3 of the Bill state that Head of the departments has the authority to classify and reclassify State information. This can be achieved by using the classification level outlined in Section 12 of the Act. The Bill alludes that the Head of the department as an Accounting Officer may delegate the duties to classify the information to the official at a senior level in writing. The provision to appoint adequately senior official is to ensure that the State information that is classified, meets all the requirement for protection and the official is highly informed. All individual items of information that falls under classified information would be categorised as classified.

SSA (South Africa, 2010) alludes that the Bill also indicates that when a member of the Security Service as contemplated in Chapter 11 of the Constitution who by the nature of their work deals with State information that may fall within the ambit of this Act, that person must classify such information in accordance with the classification level set out in section 5. The Bill further gives authority for the classification of information to the organs of State and the responsibility to declassify and downgrade. However, it also alludes to the fact that the heads of departments may authorize senior officials to take the responsibilities of downgrading and declassifying. The head of the department as an accounting officer may delegate such powers in writing. The SSA must identify the departments that have an unsuccessful rate of managing highly sensitive information and take their responsibility of handling of classified information and the functions of recording such information. They must also take the functions of classification and declassification of such records of a defunct department that have failed to protect the government's information. This can be done through consultation with government executives and agencies before making final declassification determinations.

The South African Press Association (SAPA:2015) posits that the operational gap between South African Intelligence system and the departments it is a cause for security breaches and the reason foreign spies have exposed the government's secrets. The reported documents allude that South African Intelligence lacks the skills and the well-trained personnel to defend the security of the State, and there are many foreign spies that are operating in South Africa. SAPA (2015) further reports that in 2015, there were an estimated 140 foreign spies operating and gaining access to government departments, ministries, and even the Presidency.

Van Rooyen (2013:156) points out that the attacks on information security and information technology (IT) system, it is more global and it is funded by seriously organised crime institutions. It is no longer easy to prosecute hackers because the investigators cannot link them with critical information that can be used as an evidence in the court of law. In the era of information security breaches, the department requires an advance strategic thinking on how to counter against the highly skilled and innovative criminals.

Du Plessis (2012) reports that the international digital security company providing a software application that has breach level index for tracing the past and the present security breaches that are reported online. The software name is Gemalto, and it was used to discover security breaches that occurred from 2010 to 2012 in South Africa, and it found nine significant breaches. The software indicates that the SAPS was the most infiltrated organization and have lost 15 000 personal records. It further reports that the aggressors were targeting personal information that is used to misrepresent the identities, and the sources of the breach were malicious outsiders.

Saville (2012) reports that three South African government departments were hacked in 2012. The DSD web address population.gov.za opened to a dark page with a window containing the energised realistic site hacked by H4sniper and a realistic delineating a pulsing screen on Sunday morning. The Presidential National Commission and the National Population Unit's site were likewise hacked. At the point when approached about the explanations behind the assault, H4sniper reacted by email: "We as a whole realise that SA is the principal supporter of the Republican Arab Saharawi Democratic and the enemy of Morocco since quite a while and we are programmers and our objective is to safeguard our nation."

The offenders are using sophisticated methods to infiltrate the government system, and that forces the department to acquire effectively and advance security applications. The departments must ensure that these applications are well safeguarded, particularly those that are fundamental to the department’s infrastructure. The department’s operational applications and operating system platforms must be secured, and that includes electronic mails (E-mail) and instant messaging (IM) applications. The government must modernize the information security system and recognize the security practices (Whitman & Mattord, 2015:48). The management in the departments must emphasise that it is a duty of every employee to secure the information of the departments, because of the manner in which information is exchanged on social media. The departments must have mechanisms in place to counter against the unauthorized disclosure of sensitive information (Grama, 2011:2). The researcher collected information on threats and attacks by analysing the content of various literature sources. The categorizations may vary; threats are relatively well studied and equitably well understood.

1.4 AIM AND OBJECTIVES OF THE STUDY

Denscombe (2002:25) alludes that there must be a reason for doing research, to indicate the focus and provide criteria for the evaluation of the outcomes of research. The aim of this research was to evaluate the protection of classified information in the South African Government Departments. The research will follow the Denscombe (2002:27) guidelines:

- To examine the South African legal mandate on protection of security information in the government institutions.
- To describe the existing security risk control measures (SRCM) used for the protection of security information in government departments.
- To determine the local and international best practices on protection of security information.
- To recommend best practices on how to protect the security information of the government department.

The research explores all actions, measures and means employed to achieve and ensure a condition of security commensurate with government classified information.

1.5 KEY THEORETICAL CONCEPTS

Leedy and Ormrod (2010:119) highlight that the purpose of defining of key concepts is to prevent any misunderstanding.

For the purpose of this study, the following key concepts are as follows:

1.5.1 Information

Information is referred to as any recorded or displayed data, knowledge, or content of communication. Regardless of its format, information is defined as the data that have been analysed and synthesised (Van der Westhuizen, Schellnach-Kelly & Geyer, 2010:10). Van Rooyen (2008:218) argues that information relates to any information, which you can hear directly or indirectly, taste, smell, touch or see. It also includes rumours and so-called stories. Ratcliffe (2008:96) refers to information as data, which can produce meaningful evidence during an investigation.

1.5.2 Security Threats

There are various definitions of security threats to information systems. Among these, are examples such as the one presented by Grama (2011:13) and Layton (2007:7) who define security threats as a successful exploitation against vulnerabilities in a system, whether accidentally or intentionally. Talbot and Jakeman (2008:141) define the security threat as anything that has the potential to prevent and hinder the achievement of objectives or disrupt the processes that support them.

1.5.3 Vulnerabilities

Vulnerability is a weakness of flaws in an information system. Vulnerabilities can exploit to harm information security. They may be construction or design mistakes. They also may be flaws in how an internal safeguard is used or not used (Grama, 2011:10). Rogers (2005:109) asserts that vulnerability implies that safety efforts are deficient; for instance, an advantage, for example, money might be presented to a security chance like burglary. Along these lines, vulnerability infers an absence of safety efforts in connection to security chance.

Garcia (2001:303) alludes to vulnerability as an exploitable capacity or an exploitable security shortcoming or lack at an office of security intrigue. Exploitable capacities or shortcomings are those intrinsic in the structure of the office and its assurance or those

currently in view of the inability to meet endorsed security models when assessed against necessities for characterised dangers. In the event that the weakness was identified and misused by aggressors, at that point, it would sensibly be required to result in an effective assault making harm the office.

The threats that are growing in frequency, variety, sophistication, and maliciousness make it difficult to identify security vulnerabilities. It is also difficult for security intelligence units to plan for every threat, or anticipate all forms of risks relate to leaking of classified information.

1.6 THE VALUE OF THE RESEARCH

The research outcome is intended to assist the South African government departments on how to protect the classified state information. This will be achieved by describing the existing security measures, acknowledging the current threats and exploring the national and international best practices. The value of this research will be essential to all the government departments, when dealing with information that has a potential to hurt the RSA, the departments, personnel and its resources. It is the precise procedure of gathering, examining and deciphering information with the end goal to expand scientist's comprehension of a wonder about which they are intrigued or concerned (Leedy & Ormrod, 2010:2).

The study addressed the vulnerability of government employees and the interrelationships that exist between unethical, irregular and unlawful conduct. This will inform them of the obligation to uphold the principles and values of the Constitution, legislation, regulations, or directives relating to secrecy and the safeguarding the government’s classified information. The research will further promote the culture of accountability and effective governance, in particularly the public bodies that specifically dealing with classified information.

It was envisaged that the study would contribute knowledge of the community and the learners who are studying towards security-related field. The research will also be available to the University of South Africa (UNISA) and the academic community and add to the academic body of knowledge.

1.7 RESEARCH DESIGN

The researcher used the systematic review as a chosen research design. The thematic analysis is the process of identifying patterns or themes within qualitative data. Gough, Oliver and Thomas (2012:5) described systematic review as a form of research that identifies, describes, appraises, and synthesises the available research literature using systemic and explicit accountable methods. The researcher followed the Punch's (2014:108) explanation of the criteria of systematic review as well as the steps that should be followed during systematic review that includes pre-specified protocols and formalised tools for searching, screening, coding, weighting, and integrating the literature. Braun and Clarke (2006:78) suggests that system review is the first qualitative method that should be learned as it provides core skills that will be useful for conducting many other kinds of analysis.

The researcher collected data from various literature studies and newspapers from the past and the present. The researcher opted for more available and affordable way by reviewing existing studies. The researcher set aim and objectives of the study by critically analysing the research problem, and then he linked them with research questions to find the search strategy for this study. Neuman (2011:49) describes content analysis as used for examining the content contained in written documents or other communication media.

The content analysis is an exploration strategy for the equitably, methodical and subjective portrayal of the show content correspondence (Bryman. 2012:289). Harris (2001:191) attests that content investigation is an adaptable research approach that can be connected to a wide assortment of content sources, helped by the accessibility of technology. The content analysis can adapt to more information. It may be utilised to research a point longitudinally through the examination of contemporary writings. Content analysis can be viewed as an unpretentious research approach in that it tends to be utilised to dissect normally happening information. Therefore, the content examination might be useful in decreasing the issue of social attractive quality inclination among respondents while exploring delicate themes. Yang and Miller (2008:689) suggest that content analysis is the systematisation of content

examination. It examines the frame and substance of correspondence. Basic implications and thoughts are uncovered through breaking down examples in components of the content, for example, words or expressions.

1.8 POPULATION AND SAMPLING

O'Leary (2014:356) argues that the data saturation is reached when collecting data no longer add additional understanding or aids in building theories. Matthews and Ross (2010:278) indicate that the selection of these newspaper articles for inclusion in the sample is validated stating that the documents are something more than just a source of data since it is possible to research documents in their own right as a field of research. The approach that was used was to outline the keywords to filter information relevant to protection of government-classified information.

Table 1.1 Sabinet Legal Table Frequency of pre-set keywords

Keywords	**Frequency broad scope**	**Percentage**
CLASSIFIED INFORMATION	13797	54%
INFORMATION SECURITY THREATS	4576	18%
SECURITY CLEARANCE	7112	28%
TOTAL	25485	100%

The key terms mentioned in above Table 1.1 reduced to number of information sources and extracts information that could be used in the research in an attempt to answer the research hypothesis. The newspaper articles related to classified government information was found and used as a sample. The articles indicate that from 2012, the SSA and the departments are still struggling with the vetting of government officials. The newspaper articles reports that the thousands of government officials and employees of state-owned companies dealing with supply chain management had not been vetted as a mechanism to tackle corruption, despite a 2014 Cabinet memo instructing the SSA to vet all supply chain employees. Pneumol (2018) defines inclusion criteria as the key features of the target population that the investigators will use to answer their research questions. In this study, the inclusion

criteria are the concepts government departments, security breach, and classified information and security measures. Pneumol (2018) further defines exclusion criteria as features of the potential study participants who meet the inclusion criteria but present with additional characteristics that could interfere with the success of the study or increase their risk for an unfavourable outcome. In this study, the researcher excluded all articles that did not have government departments, security breach, classified information, and security measures in its key concepts.

Table 1.2 Percentage of the inclusion and exclusion criteria

Keywords	Inclusion criteria	Percentage	Exclusion criteria	Percentage	Total
CLASSIFIED INFORMATION	1	0.0039%	13796	54.13%	54.1339
INFORMATION SECURITY THREATS	3	0.012%	4573	17.95%	17.952
SECURITY CLEARANCE	1	0.0039%	7111	27.90%	27.9139
Total	5	0.2%	25480	99.98%	100

The researcher selected newspaper articles that are most relevant to the study and assessed how the decision will affect the validity of the study. The researcher used different variable to define both inclusion and exclusion criteria in Table 1.2, and ensured that they relate to the objective of the study. The table shows less percentage on inclusion criteria because the researcher identified key variables that are needed to make a statement about the validity of the study results.

Table 1.3 Newspaper articles analysed

Author and date	Title of article	Inclusion Criteria
Du Plessis. 2012	Police database hack tops list of SA security breaches.	Government Department Security breach.
Reisinger. 2017	When Government's need for secrecy clashes with the Public's Right to Know	Government Department Classified Information.
SAPA. 2015	Foreign spies hacked SA government computers.	Government Department Security measures.
Saville. 2012	Three SA government websites hacked on Sunday.	Government Department Security measures.
Serrao. 2017	Senior Crime Intelligence Officials without top secret clearances.	Government Department Security Clearances.
Total	5	5

The researcher did not deal with specific individuals in his sampling, but used data primarily from printed mass media reports like newspaper articles related to the topic. Miles, Huberman and Saldana (2013) underscore that the sampling in qualitative research tends to be more purposive than random. The non-probability sampling method includes an element of subjective judgement. The researcher used non-probability sampling and specifically purposive sampling method, and selected data from accessible newspaper articles that relate to the topic. The keywords were outlined from the study as the criteria and the researcher used his personal judgement to select the articles that are relevant to protection of government-classified information.

1.9 DATA COLLECTION

The researcher used media reports as a major database on his study. The researcher collected and identified the material that is relevant to his topic through the newspapers, and the articles that available on public domain. Maxfield and Babbie (2005:209) allude that the value of research depends on how the data are gathered. Mills and Birks (2014:40) accentuate that the newspapers are examples of literature that can provide data for qualitative studies.

Flick (2015:164) opines that some sources see quantitative content analysis rather as a specific method for collecting data while other sources see quantitative content analysis as a mixture of analytic technique and data collection procedure. Flick (ibid) further indicates that it is used for collecting and classifying information, such as in newspaper articles. Although the researcher followed a qualitative approach in this study, the researcher applied a quantitative content analysis to ascertain the frequency of identified themes or categories that emerged in the printed mass media reports within the topic-classified information, information security threats and security clearance (section 1.1, 1.2 and 1.3).

The Department of Justice and Constitutional Development (2014) postulates that during the National Assembly, the political opposition parties requested the status of the Senior Management Service officials of the National Prosecuting Authority (NPA) who have valid security clearances from the Minister of Justice and Correctional Services. The Minister admitted that his Department had a three-year backlog and senior officials were operating without the valid security clearances. The same question was asked to the Minister of Social Development during the National Assembly, and she admitted that not all her staff is vetted, but the South African Social Security Agency has prioritised the officials in sensitive positions such as those in Supply Chain Management, Finance, Grants Administration, and Executive Managers.

1.10 DATA ANALYSIS

Cohen, Manion and Morrison (2000) demonstrate that in qualitative research, data examination starts simultaneously with the procedure of information gathering. They feature the reasons as the findings of early information investigation manage resulting information gathering, which assumes a vital job in information determination and decrease. Early information investigation permits opportune guessing about outcomes. Schwandt (2007) implies that the examination should be thorough, efficient, restrained, and precisely methodologically reported. Subsequently, in qualitative data analysis, the researcher realises the significance of information in an efficient, complete and thorough way.

Holloway and Todres (2003) indicate that qualitative approaches are staggeringly differing, complex and nuanced, and topical investigation ought to be viewed as a primary strategy for qualitative analysis. They further contend that it is the principal qualitative method of analysis that analysts ought to learn, as it gives centre abilities that will be valuable for leading numerous different types of subjective investigation. Braun and Clarke (2006:78) concur with Holloway and Todre (2003) that thematic analysis is perceived as a foundational method for qualitative analysis, and it is used as a method for identifying, analysing and reporting patterns within data. In the same vein, O'Reilly and Kiyimba (2015:75) concur with Braun and Clarke (2006:77-101), by defining the thematic analysis as a method used to identify, analyse and report patterns within a data set, allowing for the descriptive organisation of the data in a way that facilitates interpretation of various aspects of the research topic.

The researcher has read the relevant books, newspaper articles and information on the Internet to get a global perspective of protection of government classified information, and to familiarise himself with the data. The researcher analysed all data he collected and selected only the most relevant data to bring meaning into the research. Data collected forms part of the qualitative approach that were decided on for this research, and further adopted the steps set out in thematic analysis.

Braun and Clarke (2006: 77-101) provide a six-phase guide, which is very useful framework for conducting thematic analysis as follows:

Step 1: The researcher reads the entire data collection carefully to obtain a sense of the whole and made his own notes.
Step 2: The researcher started to organise the data in a meaningful and systematic way. The researcher used coding to reduce huge volumes of data into small chunk to obtain meaning. The method of coding is determined by the researcher's perspective and research objectives.
Step 3: After the reading of data, similarities were identified and grouped together for a theme. The researcher made a list of similar topics and clustered them together. All materials that focus on classified information were put in the same column, and the one focusing on protection of government information was put on another column.
Step 4: The researcher applied the list of topics to the data by using a form of abbreviation as codes, which are written nest to the appropriate columns. The researcher organised the scheme to merge the columns and their codes. The data associated with each theme are read and considered whether they really support the theme.
Step 5: The researcher recognized most distinct working for the points and sorted them. Lines are attracted between classifications to demonstrate the connections. The point is to recognise the substance of what the every them is about, how would they connect and identify with the primary topic, and how do the subject identify with one another.
Step 6: The researcher settled on an official conclusion on the shortened form for every classification and alphabetised the codes. The information is collected and a preliminary analysis is performed. The researcher recodes existing material if essential.

The steps that were followed in this qualitative research allowed the researcher to understand the fundamental of the topic in short period of time. The steps give direction and make it easy to analyse and avoid possible gaps in interpretation of data collected.

1.11 TRUSTWORTHINESS

Denscombe (2002:100) indicates that validity is about the accuracy of the questions asked, the data collected and the explanation offered. According to Creswell (2005: 01) and Leedy and Ormrod (2005:105), terms such as dependability, conformability, verification, transferability, trustworthiness, authenticity, and credibility, are used to describe the idea of validity. However, Creswell (2005:01) asserts that this can also be referred to as the 'qualitative validity' in a qualitative study.

The study is qualitative and therefore in order to ensure that this is fitting, credible and confirmable, the following elements were employed:

1.11.1 Credibility

Polit and Hungler (1999) show that credibility manages the focal point of the exploration and alludes to trust in how well information and procedures of investigation address the expected core interest. The principal question concerning credibility emerges when settling on a choice about the focal point of the study, determination of setting and the way to deal with social affair information. For the purpose this study, the researcher linked the research study's findings with the reality of South African's protection of government-classified information in order to demonstrate the truth of the research study's findings. The researcher further focuses on another important technique of credibility, which is triangulation.

1.11.2 Triangulation

Triangulation as a research tool provides the study with more stringent and reliable validity and credibility as described by Hussein (2009) because the researcher uses multiple sources or multiple approaches to analyse data collected. In this way, the researcher looks for and finds convergence among multiple and different sources of information to form themes or categories in a study, again with the sole purpose of increasing the validity of the study (Creswell & Miller 2000; Guion, Diehl & McDonald, 2011). The study point is to gain good understanding from different perspectives on protection of government classified information. It is more to increase the level of

knowledge about something and to strengthen the researcher's standpoint from various aspects. For the purpose of this research, the researcher used data and theoretical triangulation.

The researcher utilised data analysis triangulation in order to understand the protection of government classified information more fully for school of criminal justice and beyond. For the purpose of this study, the researcher analysed the literature sources from different writers and their findings about the topic. Furthermore, he promoted rigour in qualitative research by using of the analyses outlined in the study.

Theoretical triangulation is defined as the use of multiple theories in the same study for the purpose of supporting or refuting findings since different theories help researchers to find problem at hand using multiple lenses (Thurmond, 2001:253-258). Guion, et al. (2011) assert that theory triangulation involves the use of multiple perspectives to interpret a singles set of data. For the purpose of this study, the researcher analysed and synthesise the description of reported cases where classified information from government departments were not sufficiently protected.

1.11.3 Dependability

Lincoln and Guba (1985:299) indicate that dependability seeks means of considering both factors of instability and factors of phenomenal or design induced changes, that is, the degree to which data change over time and alterations made in the researcher's decisions during the analysis process. For the purpose of this study, the researcher ensured that the study's findings are consistent and repeatable with the raw data he collected and interpreted on protection of classified information.

1.11.4 Transferability

Trustworthiness also includes the question of transferability, which refers to the extent to which the findings can be transferred to other settings or groups (Polit & Hungler, 1999). To facilitate transferability, it is valuable to give a clear and district description of culture and context, data collection and process of analysis. For the purpose of this study, the researcher provide the evidence that could be applicable when dealing with

government classified information, however, he cannot prove that the study's findings will be applicable.

1.11.5 Documents, journal articles and books

Denscombe (2012:21) argues that validity on documents needs to be established and evaluated in relation to authenticity, representatives, meaning, and credibility. Denscombe (2012:22) further alludes that the academic journals and commercial publishers have their material refereed by experts in the field. Therefore, the researcher has some assurance about the quality of their content.

1.12 BRACKETING

Gearing (2004:1430) explains bracketing as a scientific process in which a researcher suspends or holds in abeyance the presuppositions, biases assumptions, theories, or previous experiences to see and describe the phenomenon. Therefore, the researcher will hold his opinions to ensure that his experience in Counter Intelligence and ideas about protection of classified information in South African government clouds his judgement.

The researcher has previously worked for the SAPS from 2002 to 2014. He started his career as a Data Capturer for Crime Intelligence Gathering Unit. He then became an Investigator and gained an extensive background and training in both Criminal and Corporate Investigation. He has also worked for Crime Intelligence Unit, under Counter Intelligence within the SAPS, and he was used as trainer and mentor for new Vetting Officers. During the duration of this study, the researcher is employed at the Department of International Relations and Cooperation (DIRCO) under the Directorate Vetting Field Investigation and Integrity Management.

1.13 ETHICAL CONSIDERATIONS

The researcher must anticipate any ethical issues that may arise during the qualitative research process (Creswell, 2009:20). This section will discuss the ethical considerations in terms of Unisa Policy on Research Ethics (2013). They must look

closely at the ethical implications of what they are proposing to do (Leedy & Ormrod, 2010:100). The researcher has applied for informed consent and he received it from the College of Law Ethical Clearance Committee. The certificate is included attached as Addendum A. The researcher cited in-text references for all the sources observing the policies set by Unisa on Research Ethics (Unisa, 2013). Plagiarism was avoided by acknowledging the entire source and includes the list of references used on the study, and the researcher screened the dissertation through Turnitin to determine the authenticity figure, which amounted to 32%.

1.14 SUMMARY

The researcher introduced the research study and discussed the problem, the research objective, research design, and the methodology. The researcher followed a reliable design for this research, as recommended and described by literature, which ensured that the content analyst is reliable and valid. The researcher found adequate literature to fulfil the research objectives as well as the aim of the research.

CHAPTER 2
THE LEGAL FRAMEWORK OF PROTECTION OF CLASSIFIED INFORMATION OF SOUTH AFRICAN GOVERNMENT

2.1 INTRODUCTION

The amendment of the old apartheid South Africa's legislation on information security is a prerequisite. This incorporates the drafting of a legal framework to regulate the identification and processing of government information that warrants protection against demolition, amendment, and disclosure. The new Acts are meant to regulate the manner in which the government information may be protected. It is likewise to advance honesty and responsibility in administration while perceiving that data might be protected from exposure with the end goal to protect the national intrigue. It builds up general standards as far as which State data might be dealt with and secured in a protected constitutional democracy. The study examines the South African legal framework on the protection of government-classified information and the national policies and procedures that are used to safeguard the information. The study highlights the principal changes in the working draft of the new Protection of Information Act and the need for new information protection mechanism.

2.2 THE ACTS WHICH DIRECT THE PROTECTION OF INFORMATION IN SOUTH AFRICA

Section 209 of the RSA Constitution, 1996, gives provision for intelligence system in South Africa. The SSA, South African National Defence Force and SAPS are the three intelligence bodies empowered by the National Strategic Intelligence Act 39 of 1994 as amended by Act 67 of 2002, to determine security competency of its employees. All the government departments must develop their Information Security Policies and align them with the Constitution of South Africa.

2.2.1 National Strategic Intelligence Act 39 of 1994 as amended by Act 67 of 2002

Section 2A (1) (a) (b) of National Strategic Intelligence Act 39 of 1994 as amended by Act 67 0f 2002 empowers the intelligence bodies with the responsibility of security screening investigation in a prescribed manner for every person who is employed by or is an applicant to an organ of state. The Act focuses on companies which has applied to render services to the government departments, and which services may give them access to information that is classified or to assets that are regarded as critical to the State. The Act gives government departments' powers to conduct background checks on officials of occupies positions that designated as the national key points of the State.

2.2.2 Protection of Information Act 84 of 1982

Section 4 of the Protection of Information Act 84 of 1982 prohibits the disclosure of information that requires protection, however, it contradicts with the constitution of the Constitutional provisions relating to presumptions. The Act does not provide for criteria relating to the presentation of government's information before the courts of law, it further excludes relevant offenses and minimum sentences for offenders (South Africa, 1982).

2.2.3 The National Archives of South Africa Act 43 of 1996

The National Archives of South Africa Act 43 of 1996 is tasked with the mission to protect the rights of the people and to stabilize the national archival heritage for the benefit of all South Africans. The Act is promoting the culture of accountability and the government that is transparent to the people by applying proper management and care of government records. It ensures the efficient and effective services are provided to the public and the national archives have a national identity that the public can relate to and trust. It provides for a corporation and collaboration between National Archives Advisory Council and the South African Heritage Resources Agency on advisory functions, and forms part of the National Estate. The Act provides provision for the protection of records and relies on the assistant of the Public Protector on the

investigation of the unauthorised destruction of records, and the annual business plan must be submitted to the Minister for approval (South Africa,1996).

2.2.4 Intelligence Service Act 65 of 2002

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. Regulations 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 (South Africa, 2002).

2.2.5 Minimum Information Security Standard (MISS) Cabinet Document

On 4 December 1998, the South African Cabinet approved the MISS as the national information security policy. The MISS replaced the former Guidelines for the Protection of Classified 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.

The MISS document (1998) sets out a range of measures to protect classified information, and what type of information needs protection. It provides provision for classification of documents and the reclassification processes. It provides guidance on how classified information must be handled and stored and the processes of removing the documents from the government's premises. Chapter 5 of the MISS gives provision for conducting the personnel security vetting. It states that all government officials must undergo the vetting process and meet the requirement set for security clearance. The security clearance gives the department a guide on the degree of information that an individual can have access to, but this is subject to the need-to-know principle. It further provides the procedures that must be followed when conducting security screening and the validity of the security clearance. Some chapters in the document set out procedures to physical security and how access to classified information must be controlled. It also covers IT and communication security (South Africa, 1998).

The legal status of the MISS is not clear because it is not an approved legislation, but a Cabinet document setting out the national information security policy. All the government departments that handle the government's classified information and assets must adhere to the MISS document (Section 1.2). The MISS document (1998) address all the important applications that must be followed to prevent the disclosure of government information. It provides the four information classification categories, and that includes "top-secret", "secret", "classified" and "restricted". It also explains that personnel confidential, is not a security classification, however, records with this grouping are taken cared of similarly as classified reports. This MISS document is constrained by the unlawfulness of its engaging legislation, and it is planned to give a fleeting national security strategy for South Africa.

The South African Law Reform Commission (2005:13) alludes that it is a global practice for privacy or information protection Acts to have a set of principles that must be adhered to when managing sensitive information. The legalization of management of information privacy has been found to be an appropriate mean of translating the concepts. However, all the legal instruments and policies provide the principles of information privacy. The researcher referred to the MISS (1998), which indicates that the more harmful the information is, the more it has to be protected from transgressors. The South African Law Reform Commission (2005:13) added that security measures must approach every sensitive information separately and grade it according to its merits.

2.2.6 The Public Service Act 103 of 1994

Section 3 (4) of the Public Service Act 103 of 1994 indicates that the Public Service Administration may issue mandates regarding security requirement to which officers and employees shall comply. Section 17 (2) (h) of the Public Service Act provides that an employee may be discharged if their continued employment constitutes a security risk to the State (South Africa, 1994).

2.2.7 The South African Employment Equity Act 55 of 1998

The South African Employment Equity Act 55 of 1998 compels fairness on objectivity when carrying out Personnel Security Vetting. The National Vetting Policy Guidelines issued by National Intelligence Coordinating Committee (NICOC) on 22 January 1997 interprets the directives in the MISS and guides the application of Personnel Security Vetting in institutions. NICOC is the organisation in charge of coordinating the activities and exercises of all of the South African Intelligence Agencies, and examining the processed information received from those Agencies. It reports to Cabinet-level by means of the Minister of State Security. The SSA defines vetting investigation as a systematic process of gathering information about the person who is under investigation to determine their security competence. This is an investigative process carried out to determine the people's security competence by checking their background to determine a person's integrity and reliability regarding classified information as well their loyalty to the Constitution of the RSA. The security competent person is determined by the person's ability to act in a manner that will not cause classified information or material to fall in unauthorised hands. The levels of security clearance are three, which includes confidential, which is valid for ten years. The secret clearance and the top-secret are valid for five years (South Africa, 1998).

2.2.8 Promotion of Access to Information Act of 2000 (PAIA)

PAIA (2000) state that to access any data held by the State and any data that is held by someone else and that is required for the activity or assurance of any rights. The Act facilitates transparency, accountability and good governance. In addition, the Act indicates that once persons have identified the information or record they want or need, they need to request PAIA form that must be completed and submitted to the relevant Information Officer or Deputy Information Officer by post, physical address, fax number, or E-mail address together with the request fee (South Africa, 2000).

2.2.9 Protection of Personal Information (POPI) Act

Welz (2016) indicates that Section 19 Protection of Personal Information (POPI) Act 4 of 2013 stipulates that all officials who are charged with the responsibilities to manage

personal information have a responsibility to follow correct procedures to prevent the loss of information. The officials are expected to handle information in a manner that would prevent the damage and unauthorised destruction of personal information. Furthermore, Welz (2016) alludes that the identification of threats must be established and the security measures must in place as part of the department's risk management. The effectiveness of the security measures must be regularly verified and updated in response to new risks or identify deficiencies in existing security applications.

Section 20 of POPI Act (2013) stipulates that the processing of personal information must be authorised by the employer. The officials execute their functions on behalf of the employer and they need authority to handle and process personal information. The authorisation must be clear on what information they can access and further oblige them to maintain the integrity and confidentiality of the information. The department must implement the effective methods to ensure that all officials from the level of management to entry-level comply with the security measures.

Section 21(2) of POPI Act (2013) postulates that all government officials must sign the declaration of secrecy, that also oblige them to report any security breach or illegal disclosure of State information. Welz (2016) supports Section 21(2) of the POPI Act (2013) and further maintains that the departments must implement this security measures as part of the newly recruited officials' contracts. The contract must bind the officials to notify the department's information regulators of any security breaches, or if they have been approached by any malicious outsider to disclose the State information. This process ensures that the personal information that has been entrusted with the department does not fall on the hands of the aggressors, and the officials themselves are protected. Welz (2016) explains that personal information cannot be provided without the proof of identity, and this information must be provided free of charge. Access to this information is subjected to PAIA, and the details of such information can be obtained through an inquiry. The details of third parties dissemination of such information can be provided.

2.2.10 Protected Disclosures Act 26 of 2000 – The Whistle Blowers Protection Act

The Protected Disclosures Act 26 of 2000 addresses the unlawfulness or irregularities within the public and private sector, and it allows officials with integrity to report such activities. However, the Act does not apply to independent contractors. The Act enables the employer to react on time before the damage has occurred and to apply necessary corrective measures. It encourages honest officials to report wrongdoing and exposes malicious insiders. The Act aims at reducing criminal and corporate offenses that include but not limited to corruption, breach of contract, corporate fraud and forgery, breach of the administrative law, and threats to the environment. It implies to information that is confidential and extends to malpractice occurring overseas (South Africa, 2000).

2.2.11 The principal changes in the working draft of the Secret Bill

The SSA (2010) indicates that the principal changes between the proposed Protection of Information Bill (2010) and the current working draft includes the Chapter 5 of the 2008 and 2010 Bills, which have been deleted. The removed Chapter 5 was widely defined and interested groups described it as a controversial concept in the Bill. A few concerns incorporated the likelihood of classification of material on grounds of the national intrigue and the direction of an expansive scope of preparing of important State data. The meaning of this model continues as before as it was in the 2008 and the 2010 Bills and is generally barely characterized. The main foundation for order is currently national security.

The removal of Chapter 5 means that the Bill no longer serves the broad purpose of regulating the secure processing of valuable state information. In a conventional sense, it is now a narrowed official secret legislation. As was indicated above, the original Bill presented broad information security aspects and was seen to be out of place in the legislation. The removal of Chapter 5 was well received and described as well developed. If the Bill can be enacted, it would repeal the MISS document (1998), and the Protection of Information Act 84 of 1982. This would unregulated the government information that is unrelated to the national security. This is unwanted and

thought ought to be given to what happens to the erased parts of the Bill. The key classification of the Act portraying the criteria for order in the three security levels, which incorporates confidential, secret and top secret.

Higher Education South Africa (HESA) (2012:18) indicates that section 3 of the Bill gives provision on how all government department must protect the valuable information of the State. It further focuses on the functions of the intelligence and oversight structures of the government in relation to classification, reclassification, and declassification of information processes. The government departments must receive directives from the Minister of SSA if they want to classify the information, upon application by an interested department. HESA (2012:18) states that the provision indicates that any department that has demonstrated its capacity to protect the classified State Information can apply for an opt-in clause that would grant them the power of classification. This can amenable the abuse of power, because the provision is too broad and it does not provide for the criteria for granting permission.

2.2.12 The need for new information protection mechanism

SSA (2010) reports that with the absence of a comprehensive statutory framework, the government is producing a high volume of information without a clear provision on which information requires protection. This has resulted in government overspending on resources; create an unstable classification and declassification environment, excessive cost and inappropriate implementation. The government departments have an enormous amount of classified information and documentation, and they lack clarity and direction on what actually requires protection (South Africa, 2010).

The SSA (2010) indicates that the current protection mechanism is inconsistent with the Constitution of the RSA, 1996, and it has inherited the apartheid State approaches that encourage the unnecessary protection of massive amounts of information. There still to some degree a default position of secrecy. The Bill intends to strengthen the protection of State information and give direction on what information needs protection. The aim of the current reforms is to significantly reduce the volume of classified information and balance the presumption of secrecy with a presumption of openness.

SSA (South Africa, 2010) opines that an extensive statutory establishment for the order and declassification of data is probably going to result in a more steady and practical arrangement of approaches and a more predictable use of standards and strategies. An authoritative reason for the classification and declassification system, setting up clear managing standards while holding wide specialist inside government to build up and direct the points of interest of the framework, offers a handy and more unsurprising approach to accomplish important changes. A statutory structure is required, which can manage essential issues and determine what data might be characterized and who may order such data. Therefore, it should be clear on when should classified information be declassified and who can declassify information. The duration of classification should be mentioned and the procedures for classification and declassification (South Africa, 2010).

SSA (2010) indicates that the framework indicates what system should be established to ensure the review of classified information and what criteria or factors should be considered when classified information is reviewed. The variables, for example, what system for the review of classified information ought to be built up and what criteria or elements ought to be viewed as when grouped data is explored. It ought to think about what methodology ought to be made for solicitations for the classified status of information and if so what sort of processes and who may make such applications. It ought to be evident whether the declassified data ought to be discharged to the general population or not. The criteria ought to demonstrate a focal database with all declassified data, which is accessible to people in general, and if this is true, who should build up and keep up such a database. The structure should direction what sort of oversight is required for the arrangement of data insurance, and what ought to be the medicine identifying with State Information amid court procedures (South Africa, 2010).

According to the SSA (2010), the point is to have a statutory framework that gives guidance to those in government who are responsible for information security; significantly decrease the measure of State data that is protected from divulgence. It further gives more insurance to that information that genuinely requires protection; and

to adjust the information protection routine with the qualities, rights, and opportunities cherished in the Constitution.

The Protection of Information Bill is intended to make sure that there is a sound way to deal with the security of State information. This will enable the State to respond to the infiltrations and other related threatening practices. The Bill sets out methodology on how sensitive information that has been classified are dealt with amid court procedures and requires a court to avoid open revelation of classified reports that frame some portion of court records. It additionally provides for particular undercover work and related offenses, for example, block attempt of or impedance with classified information, the arrangement of false data to a National Intelligence Structure and denial of exposure of a State security matter. A first draft Bill was distributed in the Gazette for remarks amid March 2008 (South Africa, 2010).

The Protection of Information Bill's point is to make sure that there is an intelligent way to manage and secure the information of the State. It also provides clarity and direction on how to conduct the process of classifying and declassifying of State information. It creates a legislative framework for the State to react to malicious undercover work and related antagonistic exercises that aimed at compromising the classified information of the State. The Bill, as it is known, sets out systems on how classified documents are to be taken care of amid court procedures, and expects courts to counteract open divulgence of characterized archives that shape some portion of court records (South Africa, 2010).

On the one hand, the objective the of Protection of Information Bill is to create a statutory framework that would protect the government departments and the information that is generated by all the organs of State. It is also to set out criteria and processes in terms of which State Information may be protected from destruction or from unlawful disclosure. The framework would set out criteria and processes in terms of which information which is protected from disclosure and which is classified may be declassified. It also creates offenses and proposed minimum sentences for unlawful disclosure of information, including the crime of espionage and to make it an offense for an individual to knowingly supply false information to the national intelligence structures and to establish guidelines for the treatment by courts of classified

documents (SSA:2010). On the other hand, the Protection of Information Bill (2010) provides for the Minister for State Security to issue regulations on information security across government, and repeal the existing Protection of Information Act 84 of 1982.

These constitutional obligations were 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.

2.3 SUMMARY

The chapter discussed the South African framework on protection of government-classified information to obtain an understanding of the legislation in place. The chapter includes the national laws and regulations prohibit the disclosure of certain information. The researcher commenced the chapter with the Constitution of South African and the laws that talk to protection of information. The next chapter focuses on the literature perspectives on protection of classified information.

CHAPTER 3
LITERATURE REVIEW

3.1 INTRODUCTION

The chapter focuses on what has been written about the protection of government-classified information in the form of journals, books, newspaper articles, and legislation as sources. The researcher used the objectives of the study to explore the chasm in the protection of classified information in South African government departments. The researcher describes the existing SRCM used for the protection of security information in government departments, and further determines the local and international best practices for the protection of security information.

3.2 SECURITY RISK CONTROL MEASURES

Hagen, Albrechtsen and Hovden (2008:377-397) report that the Norwegian organisations have implemented successful technical administrative security measures and policies for the protection of government information. Based on the organisational assessment tool, the awareness programs have been proven more effective security measures than the technical administrative.

The departments can achieve its strategic goals and objectives through effective security measures, and identify areas of weakness in their information security system. If the departments' information security measures are effectively implemented, it can ensure accountability from management and officials tasked with the responsibility to prevent security breaches and none-compliance. This measurement programs can ensure that the departments' classified information is secured and the security agency can accomplish its mandate. If this security measures can be implemented and maintained, it would demonstrate the departments' compliance with the Constitution and the relevant laws of the country (Chew, Swanson, Stine, Bartol, Brown, & Robinson, 2008).

Alshboul (2010) indicates that the departments must understand their business vision and align their security requirements with what the department want to achieve. If the department values their information, security it is important to implement the appropriate security measures. The information security breaches can be prevented only if the department put in place systems that would ensure compliance from the employees. The department must respond to challenges that are presented by new technologies, software applications and network devices by developing security policies and new security measures that can address the new threats. The attacks on the departments' information security system have huge financial implications, negative impact on customer confidence and it damages the reputation of the department. The challenges and threats must be analysed, and the departments must be determined if these threats are coming from inside or outside aggressors.

Eduardo and Santos (2014) allude that to protect information and other associated assets, organisations have to have a set of information security measures that are recommended by international standards and models widely accepted by professionals and organizations around the world. Eduardo and Junior (2014) prefer these controls, including organisational security measures, and further, describe them as a clear and strategic method to secure information and the assets of the department against threats that exploit the vulnerabilities of the employees. If these practices can be implemented and well maintained, it can minimize the risk and the impact of exploitation.

Harris (2013) reports that most departments overlook the technicalities and administrative elements that physical security has on the departments. The departments' physical security is often ignored when discussing the information security because the focus is always on the technology-oriented security countermeasures. Brotby (2006:8) concurs with Harris (2013) that information security is not only a technical issue and government challenge that involves sufficient risk management. Brotby (2006:8) adds that the active involvement of senior officials on the assessment of emerging threats and the departments' response them, would ensure effective protection of classified information and encourage accountability. Ghernaouti-Helie (2007) underscores that if the departments can minimise the level in which the security incidents are happening and the damage that is causing to the

normal operations, they would ensure achieve their mandate. In that way, it would educate government departments that security is not only a technical matter, but also it has a direct impact of the day-to-day running of the departments.

Nkwana (2015:vi) shares the same view with Brotby (2006:8) that the departments' executives and management staff must be committed to security risk controls of the departments. The management must be directly involved in the assessment of emerging threats that the departments are facing and provide support and sufficient resources. They must provide strategically and continues initiatives to establish the effective protection of security information.

Perkel (2010) points out that there are problems in protecting information in these organisations because IT professionals attempt to protect information and knowledge, as researcher, students and research project teams have specific needs and demand the freedom to develop their activities. Thus, Eduardo and Santos (2014) point out that each organisation has its own characteristics that lead to particular information security needs. The Brazilian standard that is identical to international ISO/IEC 27002 expressed the same understanding by proposing that organisations need to conduct a risk analysis and assessment to identify vulnerabilities, threats, the probability of occurrence, and potential impact, allowing them to select which measures are necessary to their own reality. However, the adoption of information security measures may not be the result of strategic decisions by an Information Security Governance structure. Adoption may be a result of the regulation by the Government and other agencies responsible for its importance for IT managers and professionals because these measures are recommended by international standards widely adopted.

They are associated with a training and certification market that may lead organisations to hire consulting services, professionals and managers with a homogeneous understanding about information security measure's needs. Also, measures adopted by leading organisations in academia or public sector may be imitated by public sector and public research institutes because of uncertainties about Information Security risks to which they are exposed (Albuquerque-Junior & Santos, 2014). Therefore, these organisations may adopt measures that do not meet the

needs identified after a risk analysis, but that are responses to external forces to which they are subject.

Goodbody (2003:22) identified the security measures that can be applied for the protection of security information against files containing sensitive information are stored in lockable steel filing cabinets; unauthorised access, alteration, disclosure, or destruction ensure that:

- The business premises that house the personal information of employees is controlled by cards and it requires passwords to access the information.
- The only relevant official has access to the secure store that holds files with sensitive information.
- Officials need passwords to access electronic files.
- There is a security measure in place to ensure that personal information is accidentally disclosed to the public, and that included areas where computer screens are located, showrooms and waiting rooms.
- The officials have been well developed on issues of security and protection of sensitive information and the consequences of non-compliance.

The authorities are granted powers to draw up an information handling policy, which is brought to the attention of all employees responsible for handling personal information. The policy should indicate the consequences of not adhering to the set policies. The policies should be in line with the Constitution of South Africa.

Kam, Katerattanakul, Gogolin, and Hong (2013) note that external pressures influence Information Security in academic organisations and that this influence may be understood from the perspective of institutional theory approach suggested by Bjorck (2004). As information is an extremely important asset for public research institutes and as the protection of information is a necessity or even an obligation, and in the characteristics of these organisations.

Govendor (2012: v) asserts that the departments need people who have the expertise in information security system so that correct judgments can be made and the

operations can be effectively and efficiently executed. The departments' assets can be negatively affected if the threats and vulnerabilities are effectively managed, and the SRCM must have information on these incidents.

This study explores security measures, which are designed to enable the government departments to counter against the threats and vulnerabilities that they are facing. It shows the importance of active management on the issues of security and the importance of bringing the most appropriate security measures. Consequently, the study shows that relationship between the policymaking, implementation of relevant security measures, analysing the effectiveness of the security measures and the maintenance of security measures.

3.3 INTERNATIONAL BEST PRACTICES ON PROTECTION OF SECURITY INFORMATION

The government departments are using information and communication technologies as part of their information system and it is expected that every department should have security measures. The management must not only focus on developing the best policies without having methods or programmes to ensure that they are implemented. It is important that the employees are well aware of its existence so that the practices are standard. The researcher managed to collect and analyse information regarding the international best practices on control and handling of classified information. The section also covers the levels of classification.

The relationship between security objectives and practices are complicated but important to understand (Dhillon & Backhouse, 2001). In addition, Byrnes and Procter (2002) concur with Dhillon and Backhouse (2001) that some practices only contribute to a particular security objective. Therefore, it is important for security managers to have the expertise to allocate appropriate resources to countermeasure and diagnose the threat. This would indicate the impact that management practices has on the protection of government information. To understand how the management has an influence on the objective of information security it is important to explore the interrelationships between security objectives and the management practices.

Ma and Pearson (2005) indicate that the implementation of information security initiatives needs more research. The departments must understand the foundational structure of their security system by identifying the inter-relationships among security practices. The departments do not share the same challenges and priorities when comes to the implementation of security practices. In this way, Ma and Pearson (2005) assert that they are of the same view with Dhillon & Backhouse (2001) that the department can effectively implement the information security practices if the security practitioners associate them with the security objectives. However, other external influences have an influence on the success of security practices implementation. Ma and Pearson (2005) further point out the issue of senior management endorsement, financial availabilities, departments' policies and the organisational culture of the department.

Barlette (2006) identified remedies to the departments when implementing information security practices. The process must have a hierarchy influence; computerization, ethical codes, support to the users, and constant security awareness. Barlette (2006) maintains that the key factor in the implementation of information security practices is the support and commitment of senior management. The management's involvement would have a positive influence and affect the success of the implementation.

Ma and Pearson (2005) opined that the consequence results from the management who do not want to comply with the security practices of the departments. The management's involvement in the protection of information is very important. Stoll and Breu (2012:261) concur with Ma and Pearson (2005) that policy development is the point of departure if the departments want to implement the best practice in information security. The department must consult with their regulatory requirements, corporate with their partner departments, and establish the security policy. The departments that have a clear vision and operational policy produce strategic practices and objectives.

Ma and Pearson (2005) further indicate that the Information Security Policy must clearly specify the responsibilities of the employees on Information Security, and illustrate the importance of security to the departments. The department must appoint managers who are responsible for updating and maintaining the security policies and support the information security programmes. They alluded that the next phase

involves organisational security, which includes the authorisation of the Information Security Management Committee. The Committee is responsible for advising the department and business units on Information Security Management.

Stoll and Breu (2012:261) recommend that the departments must conduct a risk assessment to establish a risk treatment plan to reduce the security risk to an acceptable level of risk. For the identified remaining risk, a department's continuity plan is developed, implemented, maintained, tested, and updated regularly. The authors added that the department's process objectives are assumed from the corporate objectives by regarding the specific business, contractual, legal, and regulatory requirements for the single process. The authors further analyse and optimise all business processes in a strategically aligned way. In that, the stakeholder's requirements together with information security are improved. The information security measures and controls, identified in the risk assessment and business continuity planning, are suitably integrated into the operational processes.

Stefanek (2002:68) argues that Control Access Information is a government designation for computer security that requires computers to have the ability to control access to the computer via usernames and passwords, and protect files by assigning ownership and access rights. Stefanek (2002: 68) recommends the desktop operating systems to have at least the Control Access Information compliance that ensures the safety of individual's information. These security features would ensure the aggressors do not physically access the information on individual's computers systems.

The California Polytechnic State University (CAL POL) (2018) concurs with Stefanek (2002:68) that the use of a strong password is important to control access to the computer system. They further opined that most officials reuse the passwords on their computer system, whilst others use the same password for everything. The reusing of one password for more than one computer, account, website, or other secure systems, will be only as secure as the least secure systems. The aggressor would be able to unlock all the security systems with one password, and this includes the officials who never change their password.

CAL POL (2018) is of the view that the officials must back up their important information and ensure that it can be restored when needed. They must avoid using storing information on inaccessible devices; this can be caused by virus infection, hardware failure, and other causes. The officials must protect their personal and employer's information by ensuring that their system is updated and the information is backed-up regularly. California Polytechnic State University (2018) further indicates that the officials must take full control of their official emails, by not responding to emails that require personal information. The must be alert at all times and avoid suspicious links or unknown messages from banks, competition vouchers or fake websites that want the confirmation of identity or account number. All government officials must be security conscious.

The development and maintenance of the system that stores classified information is an important factor of information security as indicated by Ma and Pearson (2005). The classification control must clearly be labelled based on the level of confidentiality, clearly classified with a simple, effective system, and be recorded based on ownership. The departments Information Computer Technology (ICT) Business Units must have a formal procedure to maintain the security of application software. The confidentiality, authenticity, and the integrity of information must be protected by means of cryptographic techniques. They must protect system files by controlling program source libraries in the development process to system development and maintenance. They should be formal procedures to maintain the security of application software.

Merkow and Breithaupt (2014) indicate that some of the preserved confidentiality, integrity and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the internet or stored on digital media. Therefore, the government department should implement the periodically testing system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss access by personnel. Talbot and Jakeman (2008:32) agree with Merkow and Breithaupt (2014), and the researcher concurs, that the information of vulnerabilities should be emphasised in specific security control measures, projected through people assets, information assets, physical information and communication technology.

Fomin, de Vries and Barlette (2008) focus on a different theory in protection of classified information, but within the Information Computer Technology Business Unit in departments. Barlette and Fomin (2009) identified many theories and models developed in order to understand employee's behaviour in the ICT field. They classified them within three main families and that includes behavioural theories, technology and computer acceptance theories, and theories linked to psychology, morals and ethics. The authors suggest that the intentions come from attitude towards behaviour, and subjective norms and intention lead to behaviour.

The study explored the interrelationship between the government departments' security objectives, security policies and management practices. It respond to the questions on how the departments' information security objectives are influenced by the interaction of the policies and management practices. It also identifies which practices contribute to which information security objectives of the department. The study indicates how much each of the management practices contributes to the total security goal of the department.

3.4 SECURITY CONTROLS AND HANDLING STANDARD FOR CLASSIFICATIONS

In order to strengthen security controls and handling standards for classifying information, stringent modes of control are vital especially in an environment where there is sensitive information (Linder & Carter 2017). Rules govern how such information is stored, handled and transmitted. Classified information is typically stored in safes, vaults, or vault-type rooms. Specific features required for storage facilities are governed by the classification level and category of documents to be stored. Storage of Controlled Unclassified Information is much less rigorous, but storage in locked cabinets and rooms is usually required. Restrictions on where and how sensitive material can be handled are tied to level of sensitivity and handling can be limited to sensitive Compartmentalised Information Facilities to Limited Areas, or to Property Protection Areas.

In addition, storage and handling of sensitive computer files are under analogous restrictions, and computer networks at various levels of security are used as appropriate. Various networks are carefully isolated from each other, including by electronic isolation and by control of movement of recordable media. Access to such networks is also tightly controlled. Information protection hygiene requires that prior to review, documents in preparation be controlled and handled at the highest level of protection likely to be needed. The transmission of sensitive information is similarly regulated according to level and category, with requirements ranging from transmission via secure networks or channels down to use of encryption to move certain Controlled Unclassified Information on open networks (ibid).

CAL POL (2018) reports that applying a classification label to each piece of information, an important part of information classification involves identifying the security controls that can consistently be applied to each level. For purposes of this research, strict provision is available by regulation and law that the departments shall establish the appropriate technical and organisational controls to prevent the unauthorised or unlawful processing or disclosure or information. The departments shall ensure that the security controls in terms of physical security such as control access to buildings or rooms correctly handle and dispose of printed material containing personal information. The departments shall control the administration processes by restricting access based on role or authority and restrict password. They must also use technical controls such as storing personal information on a secure server; make use of privacy enhancing technologies. The technical controls are appropriate for the information being processed and maintained:

- Information security controls need to be implemented commensurate with information value, sensitivity and risk. Information in each classification level will require varying security controls appropriate to the degree to which the loss or corruption of the data would be harmful to individuals, impair the business or academic functions at department, result in financial loss, or violate law, policy or the department’s contracts.

- Information security controls need to include, but not be limited to, an appropriate combination of the following: Physical Access Control, Administrative Access Control, and Technical Access Control.
- The Information Authority and the Information Security Officers collectively will determine the appropriate information security controls required for each classification level.

As stated in the MISS document (1998), all organisations have at their disposal information that is to some extent sensitive in nature and obviously requires security measures. The degree of sensitively determines the level of protection, which implies that information must be graded or classified according to it. Every classification necessitates certain security measures with respect to the protection of sensitive information, which will be known as classified information.

The MISS (South Africa, 1998) alludes that the responsibility for the grading and regarding or of document classifications rest with the institution where the documents have their origin. This function rests with the author of the classified document or head of the institution or his delegates. The classifications assigned to documents shall be strictly observed and may not be changed without the consent of the institution or his delegate. Where applicable, the author of a classified document shall indicate thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event. This option is to be applied consistently upon the award of a classification higher than restricted. Should the author of a document on which there is no embargo to reclassify such document, he must inform all addressees of the new classification. The MISS (South Africa, 1998) further stipulates that the receiver of a classified document who is of the opinion that the document concerned must be reclassified must obtain oral or written authorisation from the author, the head of the institution or his delegates. Such authorisation must be indicated on the relevant document when it is reclassified.

The classification, document, or file will be determined by the highest graded information it contains. The same classification as that of the original must be assigned to extracts from classified documents, unless the author consents to a lower

classification. Every document must be classified on its own merit and in accordance with the origin of its contents, and not in accordance with its connection with or reference to some other classified document. However, the mere existence of a document referred to is in itself information that calls for a higher security classification that the document must be classified accordingly. The author of document must guard against the under classification, over-classification or unnecessary classification of documents. The head of an institution or her delegate must on a regular basis test classifications of documents generated in her institution against the criteria applicable to the relevant classification.

All incoming classified documents, including official, classified post marked “Personal” must be received and noted in a register by persons with the appropriate clearance. The object of such registration is to enable total control over such documents. This provision does not apply to document bearing a restricted classification. The officials who usually receive the incoming post of an institution must hand the unopened inner envelope of incoming classified correspondence to the appropriate officials who are authorised to open correspondences in a certain category. The letters are responsible for entering the correspondence concerned in the prescribed register (South Africa, 1998).

The MISS Cabinet document (South Africa, 1998) states that the departments must ensure formal control by recoding all classified information that is distributed within the department and the information that is sent out of the department. The departments must have security systems in place to ensure that procedures are followed when classified information is dispatched to another department, and informal exchange of information must be avoided. Some departments have control measures to manage the registration of incoming and outgoing classified postal materials, and they are labelled according to their level of classifications. This provision can be applied to all government documents, not only on restricted material.

The registers must include the following particulars:

- The Particulars of incoming post: serial number of the entry; date of receipt; from whom received; registered postal material and reference number; Classification;

Subject/heading; Disposal: File number, Recipient signature; further dispatch and destruction.

- Particulars of the outgoing post: serial number of the entry; date of dispatch; reference number and date of the document; Classification; subject / heading; dispatch / addressing to; nature of dispatch; the registered number of postal material; signature of the recipient; receipt number; the date when the receipt was obtained.

The security controls include the standards and the policies that must be adhered to when working with sensitive information that is deemed classified. In addition, the study discusses the socio-cultural measures that support technical security methods so that the information security becomes a natural aspect in the daily activity of every government employee. The study further discusses the protection of personal information and the legislation and policies that guide the employee's government.

3.5 THE LEVELS OF CLASSIFICATION

The CAL POL (2018) has identified three classification levels that are referred to as Level 1, Level 2 and Level 3. Although all the enumerated information values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values. All the government information should be reviewed on a periodic basis and classified according to its use, sensitivity and importance. The level of security will depend in part on the effect that unauthorised access or disclosure of those data values would have on the operations, functions, image or reputation, assets, or the privacy of individuals.

This information requires a substantial degree of protection, as a compromise of the information could cause serious damage to the State, the government, commercial entities or members of the public is the one that is viewed as carrying the highest risk. The information requires a high level of confidence in the identity of the individual accessing the information. For instance, compromise could threaten life directly, seriously prejudice public order and substantially damage government finances or economic and commercial interests (Latham, 2014:7).

San Jose State University (SJSU) (2015) is of the same view with CAL POLY (2018), when it comes to the level of classification. Both institutions have categorised their information classification in Confidential, Internal Use Only and Public Available. They both recommend the confidential information shall be limited in distribution to those with an established business need-to-know. They indicated that the information should be kept to a minimum, and should be accessed from its original source and copies or printed versions.

The information may be classified as confidential based on criteria including the severe risk such as the information whose unauthorised use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the department. SJSU (2015) avers that confidential information can cause the most serious harm to individuals and the department because of unauthorised access to information intended solely for use within the department, its auxiliary employees, contractors, and vendors covered by a confidentially-security agreement and limited to those with a business “need-to-know”.

Chapter 2 of the MISS Cabinet document (South Africa, 1998) differs from CAL POLY (2018) and SJSU (2015) when it comes to levels of classification. It indicates all government department must have security measures in place and sensitive official material must be classified as restricted, secret or top-secret. The system would prescribe with information requires protection and classification. It would also give guidance regarding the documents that must be downgraded or upgraded. The departments must adhere to the policy requirements to maintain the same standard of classification. The documents must be classified in accordance with the level of protection warranted by the contents and nature of the documents.

The MISS Cabinet document (South Africa, 1998) indicates that in South Africa, the most severe level of classification is top-secret. The MISS (South Africa, 1998) stipulates that the Top-Secret classification be given to information that contains material that can neutralize the vision and mission of the departments and the national security. If this information can be infiltrated, the outcome thereof can lead to the declaration of war and damage the diplomatic relations between States. It can affect the inspirations of socio-economic development of the country, and encourage conflict

over collaborations and encourage a civil war. The departments must ensure such information can only be circulated between officials who are directly involved in the operations and have undergone the vetting process to determine their level of security competency. Top-secret information is managed from the executive level and by highly trained intelligence officials. This requires tested officials with integrity and loyalty to the Republic (South Africa, 1998).

SJSU (2015) and CAL POLY (2018) share another view on a level two classification, which is meant for Internal Use Only. The two institutions described the second level as moderate risk. The sensitivity of information that is classified as internal use only may include information protected owing to proprietary, privacy concern, ethical, and contractual. The limited use of this information may be intended solely for use within the department and the employees can only have access to relevant information that would assist them to execute their functions. A need-to-know principle would be applied to service providers.

The MISS Cabinet document (South Africa, 1998) further differs from CAL POLY (2018) and SJSU (2015), in terms of the level of classification. The second level of classification in South Africa is Secret. This is information that contains information that could have a direct impact on the planning, policy development and functions of the departments. It this information is compromised, the departments would face difficulties to efficiently and effectively execute its mandate, and that would affect the operational relations between departments. It would further have a negative impression on the State, and weaken the diplomatic relations between the affected government and interested countries. Because of the seriousness of Secret Information, people's life can also be endangered (South Africa, 1998).

Latham (2014:6) describes the second high-risk level of classification as Protected. The classification label differs but the description of risk is similar to that of the MISS Cabinet Document of South Africa (South Africa, 1998). This is information that could cause damage to the reputation of the State, departments, and the country's international relations with other countries. If this information is comprised, it would affect the country's economic and political growth by creating uncertainties in the

business community and foreign investors. In democratic countries, this can also affect the confidence public and result in violence.

The MISS Cabinet document (South Africa, 1998) uses the term confidential as a low-risk classification in compare to SJSU (2015) and CAL POLY (2018). In South Africa, if the information is capable of being utilised by aggressors to hurt the mandate of the departments and the Republic, it is classified as Confidential. This is information that has the substance to frustrate or interrupts the normal proceedings of the departments. It can also damage the personal and professional reputation of individuals; the formal administrations of the department, and have a negative effect on operational relationships between government departments. Compromising such information may have financial implications on the departments or its personnel, but it can be overcome (South Africa, 1998).

SJSU (2015) and CAL POLY (2018) further present the level three of classification as Publicly Available. It is information intended to be publicly available or provided to the public. If this information were leaked, it would not have financial implications to the department, diminish reputation, or jeopardise the security of information data. The MISS (South Africa, 1998) does not have the classification that encourages public participation. Its lowest risk classification is Restricted, which is the information that could inconvenience the government department's operations and effect its personnel. The disclosure of such information would not damage the reputation of the State and its officials, however, if restricted information can be compromised, it would affect daily operations of the departments. South Africa depends on PAIA to accommodate the public participation.

Latham (2014:4) concurs with SJSU (2015) and CAL POLY (2018) with the Public classification level that allows the public access to information with the authority of the custodian. Latham (ibid) further indicates that the integrity of public information needs to be maintained and protected by the agencies charged with the responsibilities of national security. The information must be restricted with none-public security classification until the public is authorised to access such information. There are requirement or assurances that reveals the identities of people who have an interest in viewing the information.

The Protection of Information Bill (2010) indicates that if the State is of the opinion that the information they have is likely to cause demonstrable harm to the security of the government and the department if disclosed to unauthorised people, they may classify the information as Confidential. It adds that if the State believes that the sensitivity of the information is capable of causing serious demonstrable harm to the national security of the RSA if disclosed, the State may classify the information or material as Secret. The Bill further provides the State with the provision to classify the information as a Top Secret, if they reasonably believe that the sensitivity of the information could demonstrably cause serious damage to the Republic and further damage the government's diplomatic relations with other countries.

HESA (2014) highlights the concern on the classification regime provided by the Bill, and describe the criteria of classification as unclear. The Bill does not specify or give direction on what material requires classification and to what level of extent, and it further leaves the classification to the discretion of the classifying official. HESA (2014) questions the accuracy and objective when making a distinction between what information and material that is regarded as demonstrable harmful, serious demonstrable or irreparable harm to State security. This questions how the Bill justifying the classification of information into a top secret, secret or confidential.

Olsen (2010:89) recommends the following levels of classification for protection of the information:

- Classified: It refers to a highly sensitive information that is prohibited from sharing with anyone who is not who is not authorized or is part of the mission. Such information requires high protective measures.
- Confidential: It refers to information that is restricted for officials who are directly working with such information. The officials, who are not part of such operations, cannot be allowed to access information.
- Sensitive: It refers to information that is shared with the employees and is not allowed to be disclosed to outsiders. Such information is sensitive but it is communicated to a larger scale of the department.

- Unrestricted: it refers to information that has little consequence to the department or its personnel. Such information can be shared with the members of the public.

The study shows that countries and institutions differ when coming to information classification and the value of that information. It highlights that different countries and institutions approach the protection of classified information in accordance with the use, sensitivity, and importance. The study discusses the level of classification and the harm that cause if it is handed to the aggressors. The study further shows the seriousness attached to the classification of government information.

3.6 PERSONNEL SECURITY VETTING

Molapo (2017) indicates that the security screening investigation commonly known as Security Vetting was introduced in government departments with the objective of ensuring that all the individuals employed in government with access to classified information. The process is meant to ensure that the employees possess qualities that will enable them not to disclose the government's classified information to the hands of the aggressors, and compromise the security of the State. In addition, the government departments carry the operational mandate, which includes vetting administration and fieldwork investigation. The SSA carries the legal mandate, which includes the polygraph examination, evaluation and the decision whether to issue or deny. Molapo (2017) argues that regardless of the devolution of the operations of vetting by the SSA, the departments are still experiencing challenges with the current vetting approach.

The MISS document (South Africa, 1998) defines the security vetting as a methodical process to determine the person's security competency when placed in positions that have access to sensitive information. The position that the person is applying for or occupying, determines the level of security clearance. The vetting process ensures that the officials do not occupy the government's position with misrepresented academic qualifications and criminal records. This gives direction to the department on how officials that carries the security clearance can be utilised. The hiring department must issue the declaration of secrecy forms to the application as part of the employment process, and this should be included in all government positions. The

President of the RSA is the only one who can give authority to conduct the vetting investigation on the political appointees, such as the Director-General and the Ambassadors. All officials from the highest rank of Deputy Director-General to lowest ranked officials that have access to government information must undergo the vetting process.

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) Security Sector Reform Working Group (2006) alludes there are similarities and differences in how countries approach their vetting process. For the department to commence with the vetting process, the applicant must submit the disclosure form. The form requires the applicants to disclose their full particulars, including their prior names, current and previous residential address, financial information, overseas trips and information on legal convictions. Furthermore, the disclosure forms require applicants to disclose any conflict of interest, misrepresentation of the information that they have provided or intentionally omitting the information. In addition, the applicant in made aware that misleading the vetting process could constitute grounds for a negative outcome such as dismissal or not be employed by the screening department.

Molapo (2017:11) concurs with DCAF (2006) that vetting practice is not the same around the world. Every State has their own methods of vetting that is more suitable for them. This refers only to the process and not the contents itself because the objective is to conduct background checks. Maizland (2017) concurs with Molapo (2017:11) when arguing the vetting investigation test more different things through the background checks. The investigators examine all factors that carry weight, such as allegiance to foreign countries, foreign influence, and financial background. They follow the concept of the “Whole Person” approach, which requires them to look at all the information together and determine whether the person is acceptable. It is designed to get a sense of an individual’s veracity, whether one is truthful with the government departments and whether or not there are areas of vulnerability that could lead to the exploitation by a foreign power. The Vetting Investigators are tasked to determine the likelihood that the individual could leak sensitive information to the public or to a foreign government and whether the individual might be susceptible to blackmail and to get a good understanding of the person’s overall character.

DCAF (2006) highlights that institutions such as Human Rights and Governance have expressed their dissatisfaction on how the vetting investigation is invading the privacy of the officials. The vetting process is an intelligence-driven investigation that systematically searches the private lives of the officials. The officials are required to apply for a security clearance and give approval to the vetting unit to conduct their background check investigation. The only government official officials whose consent may not be required are military conscripts. Another challenge that the vetting process is facing, is the vetting units and the vetting officers who abuse their powers. The influence that the vetting officers have over the personal lives and the careers of the officials who are vetted is huge. The vetting officers undergo a regular intensive vetting process and they are reinvestigated to prevent them from abusing the authority that has been installed in their positions. The process further covers the lifestyle audit of vetting officers, to prevent them from participating in corruption activities.

Herman (2017) alludes that the then Minister of State Security, Advocate Bongo agreed with Fraser, by pointing out the issue of accountability when comes to conducting vetting of senior government officials. Herman (2017) reports that the SSA and Parliament's Joint Standing Committee on intelligence is in the process of introducing new regulations that would enforce compliance and that will include sanctions. Herman (2017) further indicated that the then Head of SSA, Arthur Fraser refused to give the details of the draft, but assured the Parliament that it would address the issue of none-compliance.

3.7 SECURITY CLEARANCE

Homeland Security (2005) shares the same view with the MISS (South Africa, 1998) that the sanctity of the classification programme is dependent upon the suitability, integrity, trustworthiness, and reliability of the persons to whom access to classified information is granted. The MISS (1998) opines that a security clearance does not give official rights to all classified information, but it gives direction on how an official can be utilised. As such, prior to being granted access to classified information, each person would go through the vetting process and polygraph examination, and the SSA would formally issue the security clearance to those persons deemed worthy of such trust.

Maizland (2017) concurs with Homeland Security (2005) that the levels of security clearances must correspond to the level of sensitivity of information the individual needs to access for their job. The levels of security clearance include Confidential, Secret, and Top Secret clearance. However, having a security clearance does not mean that the officials can get an access to the entire department's classified information or attend to all classified meetings. Each department strategically approaches their operations different and sensitive information is shared on the need-to-know basis.

Serrao (2017) concurs with the MISS (South Africa, 1998) that the level of clearance must correspond with the level of sensitivity of information that the individual needs to access for their jobs. The officials get access to classified information and subjected to need-to-know principles based on their level of security clearance. Serrao (2017) maintains that senior SAPS Crime Intelligence officials are operating without security clearances, and they get access to highly classified information on a daily basis. Most of these senior officials have never been through the vetting process and some are operating with expired security clearances.

Enochs (2016) further notes that the security clearances are not granted to people; they are attached to the people's occupations. At government departments, human resources officials determine the responsibilities attached to the occupation and the level of sensitive information that the official will access. The officials would then be vetted on an appropriate security classification.

The MISS document (South Africa, 1998) indicates that the heads of the departments must ensure that the correct processes are followed and the officials comply with the security policies of the departments. The accounting officer must ensure that the officials are vetted, and those in a position of top secret and secret clearances are re-vetted every five years. The officials in a position of confidential clearances are re-vetted every ten years; however, the vetting unit would liaise with the authorized supervisor every five years. In the case where the supervisor discover new vulnerabilities or an official has been moved to a more sensitive environment, the vetting unit may conduct re-vetting before the security clearance of the official laps.

The MISS document (1998) shares the same view with Enochs (2016) that a security clearance issued in respect of officers while they are attached to particular institutions. The MISS document (1998) further alludes when the government officials move to another department; it is the responsibility of the receiving department to determine whether to recognise the existing security clearance or conduct another vetting of the official. However, security clearance can be transferable, for the purpose of operational function and meetings. It is the responsibility of the new employer to report the details of the security clearance to the chairperson of that meeting in writing, and that includes the level of clearance and the validities.

3.8 SUMMARY

The chapter presented the discussion of the current vetting processes and its challenges. The chapter also highlighted similarities and differences on how countries approach the vetting process. It highlights that the security clearance is attached to the people's occupations and the sensitivity of the information they access on their positions. It also explains that the security clearance is just an indication of how an official can be utilised by the deparment, and the officials get access to classified information and subjected to need-to-know principles based on their level of security clearance. The discussion in this chapter also shows that the South African government departments are responsible for vetting fieldwork investigations of their own personnel, but they do not have the legal mandate to issue or deny security clearances. The SSA carries the legal mandate to issue, downgrade, deny, and handle the appeal process.

CHAPTER 4
SUMMARY, RECOMMENDATIONS AND CONCLUSION

4.1 INTRODUCTION

The research was conducted because of the high volume of classified information that is leaked by government department officials, whether internationally or nationally. The officials get access to sensitive information and critical systems that have the ability to harm the RSA, the department, its personnel, and its resources. The research also shows that the departments do not maintain uniformity with respect to the classification system. Therefore, the security breaches of government classified information remains a national threat.

4.2 SUMMARY

The research was conducted to explore the chasm in the protection of classified information in South African government departments. This was conducted in order to gain knowledge of the content and to reach the objective of the research. In the first chapter, researcher set the objectives of the study and the methodology that he used to achieve them. The researcher covered the legal framework and the Acts, which direct the protection of information in South Africa in Chapter 2. The researcher presented current information protection regime and the legal mandate, the principal changes in the working draft of the new protection of Information Act, and the need for new information protection mechanism. In Chapter 3, the researcher described the existing SRCM used for the protection of security information in government departments. He further determines the local and international best practices on the protection of security information, which dealt with aspects of information classification, security controls and handling standard for classifications. Chapter 3 also covered security clearance and vetting. The final chapter draws together the research objectives, the research findings, conclusion, and recommendations emerged from the study. These recommendations focus on aspects deduced from content analysis.

4.3 FINDINGS

The researcher formulated findings, to address the objectives of the research. The research findings are based on the objectives of the study. Based on findings, the recommendations will be made.

4.3.1 Objective 1:To examine the South African legal mandate on protection of security information in the government institutions

The study revealed that the lack of quality in the application of classification and declassification process, it is a consequence of a lack of a comprehensive statutory framework in the protection of classified information. That has destabilised the government agencies that are tasked with the responsibility to manage classified information, and it has a direct negative impact on the departments. The current methods of protection of information reflect the mechanism that was used by the apartheid State, which encourage the government to unnecessary classify the massive amounts of information. The departments are experiencing the backlogs and the pressure to handle a massive amount of classified information. They also lack clarity on what information requires protection and how to declassify State Information.

4.3.2 Objective 2: To describe the existing security risk control measures used for the protection of security information in government departments

The findings allude that the government departments have evaluated their SRCM; it was found that the technical measures are not as effective as the awareness programmes. The outcome of these assessments also indicates that the departments are not implementing the recommended organisational information security measures. These have resulted in excessive costs because the methods that have been found to be more effective and efficient to the organisational information security are not implemented.

The researcher found that the departments have spent a lot of money on security applications that are not working or are wrongly implemented; however, it is difficult to hold someone accountable for wasteful expenditure. It was found that the

department's adoption of information security measures is a result of the management's strategic decisions guarded by an Information Security Governance structure. The department has identified measures to deal with cybersecurity concerns but they do not have a common policy framework and the implementation strategy.

4.3.3 Objective 3: To determine the local and international best practices on protection of security information

The findings indicate that the departments do not have the suitable technical and organisational controls to prevent the unauthorised or unlawful processing or disclosure of personal information. It was found that the departments have information that is to some extent sensitive in nature at their disposal but they are not sure who is responsible for grading of document classifications.

The researcher found that the people's personal information is processed without the departments' permission. It was found that the officials who are dealing with classified information in the departments do not have valid security clearance and some did not go through the vetting process.

The study revealed that the officials make mistakes when marking classified information. The safes that are used to store information do not meet the requirements to secure sensitive information, and the electronic records are secured on unprescribed networks. The departments allow officials access to all sensitive information because they have appropriate clearance or other qualifications. The Departments are struggling to establish the Need-to-Know Principle to control the access to specific sensitive information.

4.4 RECOMMENDATIONS

Hofstee (2006:159) asserts that recommendations are called suggestions for the application of research and must be feasible to implement and clearly useful. Based on the findings of this study, the following recommendations can be made:

4.4.1 The need to examine the South African legal mandate on protection of security information in the government institutions

From the findings, it is recommended that the government must finalise the approval of Protection of Information Bill, to stabilise the classification and declassification of information mechanism. The departments need a comprehensive statutory framework that would give provision on how the department must manage the State classified information. This will create an environment that is clear on what is expected from them and it would have a positive impact on departments' security policy developments. The statutory framework would provide direction on what information needs to be protected and that subsequently reduce the unnecessary massive amount of information that the government department process. It would ensure the South African Constitutional values are adhered to and provide an effective and efficient protection of classified information.

The current protection of information mechanism is the MISS document (South Africa, 1998) and the entire government department must adhere to it. This document is aimed at providing the necessary procedures and measures to protect the government information, its personnel and its resources. The departments should, therefore, compile their own rules of procedure to fit their own circumstances and operations.

4.4.2 The value of understanding the existing security risk control measures used for the protection of security information in government departments

The recommendation that emanates from the findings is that the departments should implement the proper security measures that are both administrative and technically effective. The newly developed technologies have presented the government with new threats that need urgent development of security policies and strategies that equal the nature of these threats.

The departments should conduct a regular risk control assessment that would help them to find the specific threats and the people who are possibly involved in this problems, this would allow them to select measures that are necessary to their own reliability. The risk analysis would improve the relationship between the department's

security policies; information security measures the effectiveness of the organisational information security measures.

The departments should further implement the security measurement programme that can enable them to check progress in their attempt to protect the information that the State is producing, and whether the State Security Agency is achieving its mandate. The implementations of these security measurements would give clear indication on whether the departments are complying with the Constitution of the Republic, relevant Legislations and standard working procedures. The adoption of security measures by the departments must be a result of the regulation by the government and other agencies responsible of its importance for IT managers and professionals because these measures are in compliance to international standards.

Another recommendation that emanates from the findings is that the department must develop a strategy, which directly deals with Cyber Security. The departments, SSA, Special Investigations Unit and the State IT Agency must jointly develop a common vulnerability assessment methodology for the public service.

The departments must identify the need for a common policy on information security across the public service. They must use the International Standard Operational Standard on information security aimed at ensuring the protection of government and citizen information by safeguarding its confidentiality, integrity and availability.

The government departments should not use the security measures to cover up maladministration, misrepresentation, corruption, or to protect officials involved in criminal activities. The security measures must be in the best interest of the department and the RSA.

4.4.3 The importance of aligning national best practices on the protection of security information to international best practices

Another recommendation that emanates from the findings is that the departments shall control the administration processes by restricting access based on role or authority and restrict passwords. They must also have technical controls such as storing

personal information on a secure server and make use of privacy enhancing technologies. They must ensure that the technical controls are appropriate for the information being processed and maintained.

The departments must have security measures with respect to the protection of sensitive information. The responsibility for the grading of document classifications rests with the author or head of the department where the documents have their origin. The classifications assigned to documents shall be strictly observed and may not be changed without the consent of the institution or delegate.

It is recommended that all officials processing personal information on behalf of an employer must have the necessary authorisation from the employer to do so. Such an official must have a written contract with their employer in which they are specifically obliged to maintain the integrity and confidentiality of the personal and to implement the established safeguards against identified risks.

Another previous recommendation is that all government officials must undergo the vetting process and be graded according to the level of information that they get access to. It is also recommended that officials who deal with highly classified information should be reviewed on an annual basis to ensure that the access to this much information is still needed.

There is a wide set of rule and restrictions that must adhere to when controlling sensitive information, and the officials must respect the procedures. It is recommended that engineering controls and operational procedures must be adhered to in order to minimise mistakes. The officials must utilise the electronic monitor to provide layer of verification, and physically inspect the safes and ensure that the government information is properly secured.

The last recommendation to be made is that the departments must establish a Need-to-Know requirement and formal processes to manage those who possess sensitive information. The approval from the authorised officials would be required to ensure that the officials who are in positive of classified information satisfy the requirements.

It is further recommended that those who are authorised to manage sensitive information must ensure that the functions of the officials require them to access such information and they are qualified.

The SSA and government departments must meet regularly to discuss the threats and vulnerabilities within national, provincial and local government. The SSA, as the custodian of protection of government of information, should clear the confusion by setting the standard that would ensure that all department manages the classification system the same.

4.5 CONCLUSION

The research was conducted to explore the chasm in the protection of classified information within South African government departments. This was conducted in order to gain knowledge of the content and to reach the objective of the research. Based on the findings of the study, it can be concluded that the government departments are not familiar with the complex nature of protection of classified information. The study also observed that the absence of a comprehensive statutory framework has resulted in an unstable and inconsistent classification and declassification environment. In the context of security vetting, the study shows that the departments are not adhering to the basic things such as security policies and the standard working procedures, and that constitute security risk. The security controls in the government departments are either implemented incorrectly or are ineffective. The recommendations in this study are equivalent to international standards and they can help South African government departments to secure the classified information.

LIST OF REFERENCES

Albuquerque Junior, A. E., & Santos, E. M. 2014. *Adoption of Information security measures in Public Research Institution.* Bahia: University of Federal da Bahia.

Alshboul, A. 2010. Information Systems Security Measures and Countermeasures: *Protecting Organizational Assets from Malicious*. Chicago: Argosy University.

Barlette, Y. 2006. *Information Security of Companies Actors*. Montpellier: Montpellier University.

Barlette, Y., & Fomin, V.V. 2009. *The adoption of Information Security Management Standard: A Literature Review*. Montpellier: Montpellier University.
Accessed on: 14/09/2018. [Online]: Available at:
https://www.researchgate.net/publication/260019491_The_adoption_of_Information_Security_Management_Standards_A_Literature_Review

Bjorck, F. 2004. *Institutional Theory: A New Perspective for Research in IS/IT Security in Organisations*. Stockholm: Stockholm University.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77-101.

Brotby, W.K., 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management*. (2nd Edn.). Rolling Meadows: IT Governance Institute.

Bryman, A. 2012. *Social Research Methods*. (4th Edn.). New York: Oxford University Press.

Byrnes, F.C, & Proctor, P.E. 2002. *The Secured Enterprise: Protecting Your Information Assets*. New Jersey: Prentice Hall.

California Polytechnic State University (CAL POLY). 2018. Standard: Information Classification and Handling. San Luis Obispo, California. Accessed on 21/05/2018. [Online]: Available at: https://security.calpoly.edu/content/policies/standards/classification/section_e

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. 2008. *Performance measurement guide for information security*. MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Gaithersburg. Accessed on 31/07/2018. [Online]: Available at: https://www.nist.gov/publications/performance-measurement-guide-information-security

Cohen, L., Manion, L, & Morrison, K. 2000. *Research Methods in Education*. (5th Edn.). London: Routledge Falmer.

Creswell, J.W. & Miller,D.L. 2000. Determining validity in qualitative inquiry. *Theory into Practice*, 39(3). Columbus: College of Education. The Ohio State University.

Creswell, J.W. 2005. Educational Research: *Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, NJ: Pearson.

Creswell, J.W. 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. (3rd Edn.) Los Angeles: Sage Publications.

Currie, I. 2003. *Scrutiny: South Africa's Promotion of Access to Information Act*. Johannesburg: European Public Law.

DCAF Security Sector Reform Working Group. 2006. *Vetting and the Security Sector.* Geneva: Geneva Centre for Democratic Control of Armed Forces.

Denscombe, M. 2002. *Ground rules for good research: A 10 point guide for social researcher*. Philadelphia: Open University Press.

Denscombe, M.2012. *Research Proposals: A practical guide*. London: McGraw-Hill Education.

Department of Justice and Constitutional Development. 2014. *National Assembly Question for written reply.* Parliamentary Question no: 1542

Dhillon, G. & Backhouse, J. 2001. Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 11, 127-153.

Du Plessis, D. 2012. *Police database hack tops list of SA security breaches*. General news. Accessed on 31/07/2018. Available at: www.htxt.co.za/2015/09/09/police-database-hack-tops-list-of-sa-security-breaches

Eduardo, A., & Santos, E.M. 2014. *Adoption of Information Security Measures in Public Research Institutes.* Bahia: University Federal da Bahia.

Enochs, K. 2016. How the Government grants Security Clearances.
Accessed on 18/09/2018. Available at: https://www.voanews.com/a/security-clearance-explainer/3602747.html

Flick, U. 2015. *Introducing Research Methodology*. (2nd Edn.). Thousand Oaks: CA: Sage Publications.

Fomin, V.V., de Vries,& H.J., Barlette,Y.2008. YO/IEC 27001 *information systems security management standard: Exploring the reasons for low adoption*. In:
EUROMOT 2008 Conference, Nice. Accessed on 31/07/2018. [Online]: Available at: https://pdfs.semanticscholar.org/2be0/f60530378b5595cb6138be39a13c0fa60e13.pdf

Garcia, M.L. 2001. *The design and evaluation of physical protection systems*. Boston: Butterworth Heinemann.

Gearing, R. 2004. Bracketing in Research: A typology. *Qualitative health research* 14(10) 1429-52.

Ghernaouti-Helie, S. 2007 *Security metrics to improve information security management*: (6th Edn.). Las Vegas: Annual Security Conference. Accessed on 31/07/2018. Available at:
https://pdfs.semanticscholar.org/7ccd/0015c9b2420e004ebf90697c738a49ebc386.pdf

Goodbody, L. 2003. *A Practical guide to Data Protection Law in Ireland.* Dublin: Round Hall Ltd. Publisher.

Gough,D. Oliver, S. & Thomas, J.2012. *An introduction to systematic reviews*. London: Sage Publications.

Govendor, D.2012. *Management of security information in the security industry*. Unpublished Master's dissertation. Pretoria: UNISA

Grama, J. 2011. *Legal Issues in Information Security*. Sudbury, MA:
Jones & Bartlett Learning.

Guion, L.A., Diehl, D.C., & McDonald, D. 2011a. *Triangulation: Established the Validity of Qualitative Studies*. Gainesville, Florida: University of Florida.
Accessed on 10/11/2013. [Online]: Available at: http://edis.ifas.ufl.edu/pdffiles/FY/FY39400.pdf

Guion, LA., Diehl, D.C., & McDonald, D. 2011b. *Conducting an In-depth Interview*. Gainesville: University of Florida. Assessed on: 31/07/2018. Available at: http://edis.ifas.ufl.edu/pdffiles/FY/FY39300.pdf

Hagen, J.M., Albrechtsen, E. & Hovden, J. 2008. Implementation and effectiveness of organizational information security measures: *Information Management & Computer Security*. 16(4): 377-397.
Accessed on 31/07/2018 [Online]: Available at: https://doi.org/10.1108/09685220810908796

Harris, H. 2001. Content analysis of secondary data: A study of courage in managerial decision-making. *Journal of Business Ethics*, 191 -208.

Harris, S. 2013. *Physical and Environmental Security.* In CISSP Exam Guide. (6th Edn.). New York City: McGraw-Hill.

Herman, P. 2017. New SSA Vetting Sanctions in the pipeline. *Mail and Guardian*. Accessed on 14/09/2018. [Online] Available at: https://mg.co.za/article/2017-12-07-new-ssa-vetting-sanctions-in-the-pipeline-fraser

Higher Education South Africa. 2012. *The protection of State Information Bill B6-2010.* Pretoria: Universities and Academic Freedom.

Hofstee, E. 2006. *Constructing a good dissertation*. Sandton: EPE.

Holloway, I., & Todres, L. 2003. The status of method: Flexibility, consistency and coherence. *Qualitative Research,* 3(3): 345-357

Homeland Security. 2005. *Security Safeguarding Classified and Sensitive but Unclassified Information*. Washington, D.C: Department of Homeland Security. Accessed on 14/09/2018. [Online]: Available at: https://homeport.uscg.mil/Lists/Content/Attachments/2110/SecurityReferenceStateLocalTribalPrivateSector.pdf

Hussein, A. 2009. The Use of Triangulation in Social Sciences Research: Can Qualitative and Quantitative Methods be Combined? *Journal of Comparative Social Work,* 4(1). Accessed on 31/07/2018. [Online]: Available at: http://journal.uia.no/index.php/JCSW/article/view/212/147

Kam, H.J., Katerattanakul, P., Gogolin, G., & Hong, S. 2013. Information Security Police compliance in higher education: a neo-institutional perspective. *Proceedings of Pacific.* Accessed on 31/07/2018. [Online]: Available at: https://pdfs.semanticscholar.org/8aeb/f5ed99ca53b3660bd745ff14d8cbf53dd09c.pdf

Latham, R. 2014. *Information Management Advice 33 Implementing Information Security Classification: Implementing Information Security Controls*. Tasmania: Information Strategy Unit Tasmanian Archive and Heritage Office.

Layton, T.P. 2007. *Information Security: Design, implementation, measurement, and compliance*. New York: Auerbach Publisher.

Leedy, P.D., & Ormrod, J.E. 2005. Practical research: Planning and design (8th Edn). Upper Saddle River, NJ: Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2010. *Practical research: Planning and design*. (9th Edn.). Upper Saddle River, NJ: Prentice Hall.

Lincoln, Y.S. & Guba, E.G. 1985. *Naturalistic Inquiry*. London: Sage Publications.

Linder, D. & Carter, W. 2017. *Control of Sensitive Information: Policy, Procedure, and Practice in a National Security Context.* California: Sandia National Laboratories.

Ma, Q. & Pearson, J. M. 2005. ISO 17799: "*Best Practices" in Information Security Management?* Omaha, NE Communications of the Association for Information Systems.

Maizland, L. 2017. *Security Clearance and how it could be revoked, explained*. Accessed on: 14/09/2018. [Online]: Available at: https://www.vox.com/policy-and-politics/2017/7/14/15964338/jared-kushner-security-clearance-explained

Matthews, B. & Ross, L. 2010. *Research Methods*. London: Pearson Longman.

McKinley, D.T. 2003. *The State of Access to Information in South Africa*. Johannesburg: Centre for the Study of Violence and Reconciliation.

Maxfield, M.G. & Babbie, E.R. 2005. *Research Methods: For Criminal Justice and Criminology.* Stanford: Cengage Learning.

Merkow, M.S. & Breithaupt. J. 2014. *Information Security: Principles and Practices*. (2nd Edn.). Indianapolis: Pearson Education.

Miles, M.B., Huberman, A.M., & Saldana J. 2013. *Qualitative Data Analysis*: A Methods Sourcebook. (3rd Edn.). Thousand Oaks. CA: Sage Publications.

Mills, J. & Birks, M. (eds). 2014*. Qualitative methodology. A practical guide*. Thousand Oaks, CA: Sage Publications.

Molapo, K. 2017. *Security Vetting in the Department of Home Affairs*. Unpublished Master's Dissertation. Johannesburg: University of Witwatersrand.

Nathan, L. 2009. *Lightning up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness.* Cape Town: University of Cape Town.

Neuman, W.L. 2011. *Social Research Methods: Qualitative and Quantitative Approaches.* (7th Edn.). Pearson: University of Wisconsin.

Nkwana, M.J. 2015. *Protection of security information within the government departments of South Africa.* Unpublished Master's Dissertation. Pretoria: UNISA.

O'Leary, Z. 2014. *Essential guide to doing research*. (2nd Edn). London: Sage.

Olsen, W, P. 2010. The Anti-Corruption Handbook: *How to protect your business in the Global Marketplace*. Canada: John Wiley & Sons Inc. Publishers.

O'Reilly, M. & Kiyimba, N. 2015. Advanced Qualitative Research. (1st Edn). London: Sage Publications.

Peltier, T.R. Peltier, J & Blackley, J. 2005. *Information Security Fundamentals*. Washington DC: Auerbach Publications.

Perkel, J. 2010. Cybersecurity: *how safe are your data? Nature*, 464, 1260-1261. Accessed on 31/07/2018. Available at: https://www.nature.com/news/2010/100428/full/4641260a.html

Pneumol, J.B. 2018. Inclusion and exclusion criteria in research studies: definitions and why they matter. *Jornal Brasileiro de Pneumologia* 44(2): 84. Assessed on: 18/10/2018. [Online]: Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044655/

Polit, D.F., & Hungler, B.P. 1999. *Nursing Research: Principles and Methods*. (6th Edn.). Philadelphia: J.B. Lippincott Company.

Price, S.M. 2009. *Information Security Management Handbook: Security Weaknesses of system and Application Interfaces used to Process Sensitive Information*. New York: Auerbach Publications.

Proctor, P.E., & Byrnes, F.C. 2002. The Secured Enterprise: Protecting your Information Assets Paperback. Assessed on: 31/07/2018. [Online]: Available at: https://www.amazon.com/Secured-Enterprise-Protecting-Information-Assets/dp/013061906X

Punch, K.F. 2014. *Introduction to social research. Quantitative & Qualitative approaches.* (3rd Edn.). Thousand Oaks, CA: Sage Publications.

Ratcliffe, J.H. 2008. Knowledge management challenge in the development of intelligence- led policing. *The handbook of knowledge-based Policing*. Chicago: John Wiley and Sons.

Reisinger, S. 2017. When Government's need for secrecy clashes with the Public's Right to know. *The National Law Journal*. Accessed on: 31/07/2018. [Online]: Available at: https://www.law.com/nationallawjournal/sites/nationallawjournal/2017/04/25/when-governments-need-for-secrecy-clashes-with-the-publics-right-to-know/

Rogers, F.C.2005. Security Practice III/ Security Risk Management IV: SEP361S/SRM401S. (2nd Edn). Florida: Technikon SA.

San Jose State University (SJSU). 2015. *Information Classification and Handling*. California. Accessed on 31/07/2018. [Online]: Available at: http://its.sjsu.edu/docs/security/Standard_Information_Classification_Handling.pdf

Saville, M. 2012. *Three SA government websites hacked on Sunday*. Accessed on 09/12/2012. [Online]: Available at: https://mg.co.za/article/2012-02-09-three-government-websites-hacked.

Schweitzer, J.A. 1996. *Protecting Business Information: A manager's Guide*. West Yorkshire: British Library Cataloguing Publisher.

Serrao, A. 2017. *Senior crime intelligence officials without top secret clearance.* News24. Accessed on 01/08/2018. [Online]: Available at: https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130

Schwandt, T.A. 2007. *The SAGE Dictionary of qualitative inquiry*. (3rd Edn.). Los Angeles: Sage Publication, Inc.

South Africa. 1982. *Protection of Information Act 84 of 1982*. Pretoria: Government Printer.

South Africa. 1996. *The Constitution of the Republic of South Africa, 1996*. Pretoria: Government Printer.

South Africa. 1998. *Minimum Information Security Standards*. Pretoria: Government Printer.

South African Law Reform Commission. 2005. *Privacy and Data Protection*. Pretoria: Government Printer.

South Africa. 1994a. *National Strategic Intelligence Act 39 of 1994*. Government Gazette 161228. Pretoria: Government Printer.

South Africa. 1994b. *Intelligence Service Oversight Act 40 of 1994*. Pretoria: Government Printer.

South African Press Association (SAPA). 2015. *Foreign spies hacked SA government computers*. Accessed on 01/08/2018. [Online]: Available at: https://businesstech.co.za/news/general/80719/security-flaws-leave-south-african-secrets-exposed/

Southall, R. 2012. Secrecy Bill less about media freedom, more about National Security State.
Accessed on 01/08/2018. [Online]: Available at https://constitutionallyspeaking.co.za/secrecy-bill-less-about-media-freedom-more-about-national-security-state/

State Security Agency. 2010. The Summary of the Protection of Information Bill. Accessed on 11/09/2018. [Online]: Available at http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2010/Summary%20of%20the%20Protection%20of%20Information%20Bill.pdf

Stefanek, G.L. 2002. *Information Security Best Practices. 205 Basic Rules.* Oxford: Butterworth Heinemann.

Stoll, M., & Breu, R. 2012. Information security governance and standard based management systems. *Strategic and practical approaches for information security governance: technologies and applied solutions*. PA: Hershey.

Talbot, J. & Jakeman, M. 2008. *Srmbok: Security risk management body of knowledge*. Sydney: Ligare Pty Ltd.

Tesch, R., 1992. Qualitative Research: *Analysis types and software tools*. New York: Falmer.

Thurmond, V.A. 2001. The point of triangulation. *Journal of Nursing Scholarship*. 33, 3, 253-258.

Torkzadeh, G. & Dhillon, G. 2002. Measuring Factors that Influence the success of internet commerce. *Las Vegas: Information System Research*, 13, 187-204.

UNISA, 2013. *Policy on research ethics*. Pretoria: UNISA Press.
Accessed on 01/08/2018. [Online]: Available at:
https://www.unisa.ac.za/static/corporate_web/Content/Colleges/CGS/documents/Policy-on-Research-Ethics-rev-appr-Council-20.09.2013.pdf

Van der Westhuizen, A., Schellnack-Kelly, I. & Geyer, R. 2010. *Basic Archives and Records Management*. Pretoria: UNISA Centre for Applied Communication.

Van Rooyen, H.J.N. 2008.*The Practitioner's Guide to Forensic Investigation in South Africa.* Centurion: HJN Training, Henmar
Publishers.

Van Rooyen, H.J.N. 2013. *Investigate Corruption*. Centurion: HJN Training, Henmar Publishers.

Wasserman, H.2017. *Thoughts on the media in Africa and the Global South*.
Johannesburg: Media in the South.

Welman, C., Kruger, F. & Mitchell, B. 2005. *Research Methodology*. (3rd Edn.). Cape Town: Oxford University Press.

Welz, D. 2016. A summary of “POPI” the Protection of Personal Information Act no.4 of 2013. Accessed in 01/08/2018. [Online]: Available at https://www.miltons.law.za/2016/

Whitman, M.E. & Mattord, H.J. 2015. *Principles of Information Security*. (5th Edn.). Boston: Cengage Learning.

Yang, K. & Miller, G.J. 2008. *Handbook of research methods in public administration*. (2nd Edn.). New York: M. Dekker.

ADDENDUM

Addendum A: Ethical clearance certificate

UNISA university of south africa

UNISA CLAW ETHICS REVIEW COMMITTEE

Date 20171010

Reference: ST56 of 2017
Applicant: LW Mahlatsi

Dear Mr Mahlatsi

Decision: ETHICS APPROVAL
FROM 10 OCTOBER 2017
TO 9 OCTOBER 2020

Researcher(s): Lehlohonolo Wonderboy Mahlatsi

Supervisor (s): Prof HF Snyman

An evaluation of the protection of classified information in the South African government department

Qualification: MTech in Forensic Investigation

Thank you for the application for research ethics clearance by the Unisa CLAW Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **negligible risk application** was reviewed by the CLAW Ethics Review Committee on 10 October 2017 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision was ratified by the committee.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Open Rubric

3. The researcher will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
7. No field work activities may continue after the expiry date of 20 September 2020. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:
The reference number ST56 of 2017 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

PROF D GOVENDER

Chair of CLAW ERC

E-mail: govend1@unisa.ac.za

Tel: (012) 429-9482

PROF OS SIBANDA

Executive Dean: CLAW

E-mail: sibanos@unisa.ac.za

Tel: (012) 429-8374

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Addendum B: Editing and proofreading certificate

EDITING AND PROOFREADING CERTIFICATE

7542 Galangal Street

Lotus Gardens

Pretoria

0008

27 October 2018

TO WHOM IT MAY CONCERN

This certificate serves to confirm that I have edited and proofread Mr LW Mahlatsi's dissertation entitled, **"An exploration of the chasm in the protection of classified information in South African government departments".**

I found the work easy and intriguing to read. Much of my editing basically dealt with obstructionist technical aspects of language, which could have otherwise compromised smooth reading as well as the sense of the information being conveyed. I hope that the work will be found to be of an acceptable standard. I am a member of Professional Editors' Guild.

Hereunder are my particulars:

Jack Chokwe (Mr)

Contact numbers: 072 214 5489

jackchokwe@gmail.com

Professional EDITORS Guild

Open Rubric