Intelwatch NPC (2022/337833/08) | intelwatch.org.za

14 February 2024

To: The Ad Hoc Committe on the
General Intelligence Laws
Amendment Bill of 2023
National Assembly
Parliament of South Africa

Intelwatch:
Submission on the General Intelligence Laws Amendment Bill of 2023 (GILAB)

About Intelwatch

Intelwatch is a non-profit organisation dedicated to research, policy work and advocacy to strengthen public oversight of state and private intelligence agencies in Southern Africa and around the world. Founded in 2022 in South Africa, Intelwatch aims to carry forward the work of the Media Policy and Democracy Project, which was a research collaboration between the Department of Communication and Media, University of Johannesburg and the Department of Communication Science, University of South Africa, and which contributed important policy research on surveillance issues in Southern Africa, and South Africa especially.

For more information, visit Intelwatch.org.za

Foreword

We at Intelwatch sincerely hope that this submission will assist the Ad Hoc Committee in making history by amending the intelligence legislation that has contributed to the heavy price South Africa paid for the State Capture era. While it is important to look to international legal practice, we must bear in mind that, whether we look to the East, West, North, or South, intelligence services the world over are usually in the news for all the wrong reasons – illegal interception, clandestine and unauthorised operations, extralegal renditions, torture, illegal detentions, misinformation campaigns, and the infiltration of civil society are only some examples of the lawlessness that plagues intelligence services in even the world's most advanced democracies.

Major democracies, such as the United Kingdom, United States, and countries in the European Union have, despite years of legislative reforms, still not solved the problem of keeping intelligence services from carrying out illegal and unethical intelligence activities. Thus, while we should look for solutions in other democracies, we should also not shy away from home-grown solutions to our legal problems pertaining to intelligence.

South Africa has a robust legislative system with many legal instruments at our disposal to rectify the past wrongs that have cost our country so dearly. The Ad Hoc Committee has the power to seize upon this opportunity for South Africa to become a world leader by producing intelligence legislation that is truly fit for a democratic country.

Guide to navigating this submission

This submission consists of several documents, which are meant to be read together.

The first document, Part 1 of this submission, is the legal analysis component of Intelwatch's submission, written by Advocate Vicky Heideman (Rivonia Group of Advocates). She served as an evidence leader at the Zondo Commission into State Capture, and played a key part in drafting the legal team's submissions to the Chief Justice in respect of the SSA evidence.

The second component, is Intelwatch's General Submission, containing recommendations with an emphasis of what, in practice, GILAB should facilitate in order to uphold the recommendations and findings of the various panels and commissions that have investigated problems within the intelligence community.

This second component has several annexures to assist the Ad Hoc committee in its redrafting of GILAB, which we hope will be extensive. These include:

- A policy brief on mass surveillance by Prof Jane Duncan, titled: *The future of bulk interception of digital communication: issues and policy options.*

- A special legal analysis containing recommendations for reforms regarding the Secret Services Account and the Security Services Special Account, also by Adv. Heideman, titled: *Secret Funding and the State Security Agency: Holding Intelligence Services Accountable (Recommended changes to funding and accountability mechanisms for South Africa's state intelligence services based on international trends)*

Submissions in respect of the General Intelligence Laws Amendment Bill published in Notice No 4067 in Government Gazette 49717 dated 14 November 2023.

PART 1: LEGAL ANALYSIS AND RECOMMENDATIONS

by Advocate Vicky Heideman

for

INTELWATCH

INTRODUCTION

1 The General Intelligence Laws Amendment Bill ("*the Bill*")[1] seeks to amend several pieces of intelligence-related legislation, including the National Strategic Intelligence Act 39 of 1994, the Intelligence Services Act 65 of 2002 and the Intelligence Services Oversight Act 40 of 1994, among others. The last General Intelligence Laws Amendment Act was Act 11 of 2013.

2 Much has happened since 2013, and there is an urgent need to amend the intelligence legislation in light of revelations and recommendations of the High Level Review Panel ("*HLRP*") and the Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector Including Organs of State ("*the Commission*").

3 According to the media statement released by the Presidency, the Bill seeks to implement the recommendations of the Commission and the HLRP.[2] It also seeks to do the following:

- restructure the intelligence services to provide an institutional architecture that enables effectiveness and efficiency by establishing the domestic intelligence agency and the foreign intelligence service;

- remedy the defects on the functioning of the Signals Intelligence Capacity as confirmed by the Constitutional Court;

- address the weaknesses identified through the Financial Action Task Force ("*FATF*") process, including measures to combat money laundering and terrorist financing by empowering the national security structures to investigate and conduct a security assessment if a person or institution is of national security interest;

1Notice No 4067 in Government Gazette 49717 dated 14 November 2023.
2Para 2.1 at p12 of Statement on the outcomes of the Cabinet Meeting of Wednesday, 24 May 2023, available at https://www.ssa.gov.za/Portals/0/SSA_Docs/MediaReleases/2023/Final%20Cabinet%20Statement%20of%2025%20May%202023.pdf?ver=bJy2pN_ZUDfbFQTCCNiOUw%3d%3d

- strengthen measures to regulate and coordinate the private security industry as part of a broader national security approach; and

- put in place measures to regulate the conduct of former members of the service and others with access to intelligence information.

4 The media statement further claims that the Bill will ensure that the services of the State Security Agency ("*SSA*") are not abused to serve the interests or agenda of certain individuals, and that "*the amendments will strengthen the oversight of the intelligence agencies by bodies such as the Inspector-General of Intelligence, the Joint Standing Committee on Intelligence and the Auditor-General of South Africa*."[3]

5 The goals of the Bill are therefore ambitious, and seek to address a variety of different issues. However, the Bill in its current form fails to address the most urgent and pressing issues that it ought to address, namely those identified by the HLRP and the Commission. Instead, some of the measures the Bill seeks to introduce will make the intelligence structures more open to the kinds of abuse identified by the HLRP and the Commission.

6 This submission will focus on 3 main problematic aspects of the Bill. These include the following:

- Changes to the provisions regarding security assessments (or "*vetting*");

- The inadequacy of the new bulk communications interception provision; and

- Recommendations of the HLRP and the Commission which have not been provided for in the Bill.

3Statement on the outcomes of the Cabinet Meeting of Wednesday, 24 May 2023 para 2.4 at p 13.

7 According to the statement on the outcomes of the Cabinet Meeting of Wednesday, 24 May 2023, the Bill seeks to "*address the weaknesses identified through Financial Action Task Force ("FATF") process, including measures to combat money laundering and terrorist financing by empowering the national security structures to investigate and conduct security assessment if a person or institution is of national security interest"*.

8 In early versions of the Bill, it sought to do this by mandating the intelligence structures to conduct security assessments on religious institutions and Non-Profit Organisations ("*NPOs*"). In the latest version, it mandates the security structures to vet persons and institutions of "*national security interest*".

9 As will be shown below, this amendment makes changes to the current system of vetting which are nonsensical, contrary to international vetting practices and which do not actually address the concerns of FATF.

The current system of vetting

10 The current system of vetting is governed by s2A of the National Strategic Intelligence Act. This section is not extensive. For example, it does not go into any detail regarding the different levels of security clearance. This detail is given in the Minimum Information Security Standards ("*MISS*") Document.[4]

11 The MISS Document was approved by Cabinet on 4 December 1996 as national information security policy. It does not appear to have been replaced with a more recent document dealing with information security.[5]

12 The MISS Document deals with document security, communication security, computer

4Available at https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf

5Certainly Dr Isaac Dintwe made reference to the 1996 MISS Document in his evidence before the Commission in 2021. See Exhibit YY15 and Day 393.

security and physical security measures. It is in this context that the MISS Document also deals with personnel security, and as such it provides guidelines with respect to security vetting.[6]

13 Vetting procedure, at present, therefore forms part of the policy to protect information. Of significance, the MISS document specifies in its preface that "[*o*]*ur security policies must realistically match the threats against the country and its people*."[7]

14 The purpose of security vetting is given quite succinctly in the following subparagraphs of the MISS Document:

"1.1 Security vetting is the systematic process of investigation followed in determining a person's security competence.

1.2 The degree of security clearance given to a person is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied by the person.

1.3 A clearance issued in respect of a person is merely an indication of how the person can be utilised, and does not confer any rights on such a person.

…

1.6 A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle."

15 The levels of security clearance available appear to correspond to the levels of classification of documents, namely "*Confidential*", "*Secret*" and "*Top Secret*".[8] The MISS Document also specifies that where a government department or institution wishes to employ private contractors in a role where there are security implications, such department

6From page 42 and following.
7MISS Document preface bullet point 3.
8MISS Document paragraph 3.1 read with paragraphs 3.1 to 3.3 on page 41.

or institution must specify the level of security clearance required in the tender document itself. Such clause must read as follows:

"Acceptance of this tender is subject to the condition that both the contracting firm and its personnel providing the service must be cleared by the appropriate authorities to the level of CONFIDENTIAL/SECRET/TOP SECRET. Obtaining a positive recommendation is the responsibility of the contracting firm concerned. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor.

Acceptance of the tender is also subject to the condition that the contractor will implement all such security measures as the safe performance of the contract may require."[9]

16 As can be seen from the Minister of State Security's response to Dr PJ Groenewald on 20 August 2020 in relation to the security clearance of Mr Robert McBride, the process required to obtain security clearance currently involves the following:

"1.1 Verification of the subject's/applicant's records as reflected in databases:

- *criminal records;*
- *financial records;*
- *personal information; or*
- *any other information that is relevant to determine the security clearance of a person.*

1.2 The positive outcome following a vetting fieldwork investigation. For a Top-Secret Security Clearance, the process entails the following:

i. Full record checks on databases (as mentioned above);
ii. A subject/applicant interview;
iii. Two (2) interviews with references;
iv. One (1) work enquiry; and

9MISS Document paragraph 5.1 at page 44.

v. *A polygraph examination and evaluation"*[10]

17 These reports will be sent to the Evaluation division where an evaluator will consider the candidate's risk summary based on the following:

vi. Integrity;

vii. Loyalty to the State and the relevant institution; and

viii. Non-susceptibility to extortion and blackmail;

ix. Non-amenability to bribes and non-susceptibility to being compromised due to his or her behaviour or vulnerabilities

18 It is therefore not unheard of for an entity as well as an individual to be vetted by the SSA. However, the process is geared primarily toward assessing whether a person ought to be put in a position where they have access to classified information, and the level at which they can have such access. This is consistent with the approach adopted by other democratic countries, as will be discussed below.

Proposed changes to vetting practices

19 The Bill makes certain changes to the security structures' mandate to provide vetting investigations. Ostensibly, the amendment to this section is meant to "*enable*" the Intelligence structures "*to conduct security assessments and investigations on institutions that may be used illegally for terror financing and money laundering.*"[11] It would appear that this amendment, more than any other, is the proposal which is meant to "*address the weaknesses identified through Financial Action Task Force process, including measures to combat money laundering and terrorist financing*."[12]

20 The Bill changes the previously hortatory language in s2A(1)(a) of the National Strategic

10Question NW1666 to the Minister of State Security, 20 August 2020 available at https://pmg.org.za/committee-question/14365/ .
11Item 1.5.1 at page 35 of the Bill.
12Para 2.2 at page 12 of Statement on the outcomes of the Cabinet Meeting of Wednesday, 24 May 2023, available at https://www.ssa.gov.za/Portals/0/SSA_Docs/MediaReleases/2023/Final%20Cabinet%20Statement%20of%2025%20May%202023.pdf?ver=bJy2pN_ZUDfbFQTCCNiOUw%3d%3d

Intelligence Act to mandatory: rather than providing that the Security Service "*may*" conduct vetting investigations, they now "*must*" do so on certain persons.

21 The reason for this change is unclear. Certainly, the explanation offered at item 1.5.1 at page 35 of the Bill does not give any clarity: a change from "*may*" to "*must*" does not assist the security structures in combatting terror financing and money laundering.

22 Apart from the change from "*may*" to "*must*", another major change to this section is the addition of a category of persons and institutions who the intelligence structures must vet, namely "*a person or institution of national security interest in terms of Section 4(2)(a)(i) of the [National Strategic Intelligence] Act*."

23 The proposed definition of "*person or institution of national security interest*" is as follows:

> *'' 'person or institution of national security interest' means any person or institution, identified by the Agency in the form and manner prescribed, that conducts himself/herself or itself or engages in activities that are inconsistent with the principles set out in section 198 of the Constitution including any person or institution that engages in activities that are defined as a threat to national security in terms of this Act;''*[13] (our emphasis)

24 However, s4(2)(a)(i) of the National Strategic Intelligence Act currently reads as follows:

"4(2) The functions of Nicoc shall be—

(a) to coordinate the intelligence supplied by the members of the National Intelligence Structures to Nicoc and interpret such intelligence for use by the State and the Cabinet for the purposes of—

(i) the detection and identification of any threat or potential threat to the national security of the Republic;" (our emphasis)

13Section 1(p) of the Bill.

25 Read together, these provisions are not very clear: the proposed definition of "*person or institution of national security interest"* seems to imply that the Agency may determine who ought to be vetted, while the cross reference to s4(2)(a)(i) of the National Strategic Intelligence Act seems to suggest that Nicoc will be responsible for such a determination.

26 The principles set forth in s198 of the Constitution also do not assist in providing any further clarity. Section 198 reads as follows:

"Governing principles.*—The following principles govern national security in the Republic:*

(a) National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life.

(b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.

(c) National security must be pursued in compliance with the law, including international law.

(d) National security is subject to the authority of Parliament and the national executive."

27 The purpose of such vetting also remains unclear. As mentioned above, the proposed amendment ostensibly enables the Intelligence structures to conduct security assessments and investigations on institutions that may be used illegally for terror financing and money laundering.[14] But the inclusion of the additional category of persons does not fit with current vetting practices or make any sense as a measure to counter money laundering or terror financing.

14Item 1.5.1, 3rd bullet point on page 35.

28 In the ordinary course of events, the purpose of vetting investigations is encapsulated by subsection 6, namely in order to "*issue, degrade, withdraw or refuse to grant security clearance.*" The consequence of having security clearance or not would only be relevant to an individual who is required to have such security clearance, however.

29 Section 2A(1)(a) itself makes it clear that it only applies to "*a prescribed category of persons or institutions who must have security clearance*". The first three subcategories include persons who require such security clearance:

- in order to be employed by an organ of state;[15]
- in order to render a service which may result in that person having access to classified information and intelligence in the possession of that organ of state;[16]
- in order to have access to areas designated as critical infrastructure areas in terms of the relevant law;[17]

30 The addition of the fourth category of persons and institutions makes little sense in this context. However, the implication appears to be that Nicoc and/or the Agency itself may determine which category of persons or institutions are required to have security clearance. In a previous draft of the Bill, these categories included NPOs and religious institutions. In its current form, these entities (as well as any other) may yet be required to obtain security clearance for their activities if Nicoc or the Agency deems them to be "*of national security interest*."

31 This would give Nicoc and the Agency the power to harass persons and institutions at their discretion by requiring them to undergo security investigations. While not currently provided for in the Bill, future legislation or regulations may require entities such as NPOs and churches to obtain security clearance in order to carry out their work. The revocation

15Section 2A(1)(a).
16Section 2A(1)(b)(i).
17Section 2A(1)(b)(ii).

of such security clearance may then also be used as a weapon against such institutions.

32 This is even more concerning given that the revocation of security clearance has been used as a weapon in the past to silence those who opposed state capture. For example, it was alleged at the Commission by the then Inspector General of Intelligence ("*IGI*"), Dr Isaac Dintwe, that the vetting system was abused in order to thwart investigations by Mr Robert McBride when he was head of IPID,[18] and Mr Mxolisi Nxasana when he was National Director of Public Prosecutions.[19] Dr Dintwe's own security clearance was revoked by Mr Arthur Fraser when Mr Fraser became aware that Dr Dintwe had re-opened the investigation into the Principal Agent Network ("*PAN*") Programme.[20]

33 Therefore, while the proposed amendment to s2A of the National Strategic Intelligence Act may seem as innocuous as it is absurd, it has the potential to place power in the hands of the Agency and Nicoc to harass and undermine persons and institutions at their own discretion. Such a discretion is also not consistent with current vetting practices, nor is it consistent with vetting practices in other democratic countries.

Benchmark jurisdictions

34 In its Memorandum, the Bill states as follows:

"This approach of having security checks for access to intelligence is followed by the major countries like United States, Canada, United Kingdom, Germany and New Zealand. This approach is consistent with our laws and the counter-intelligence mandate of protecting critical information and intelligence."[21]

- As will be shown below, this statement is not untrue. Like our current system of vetting, vetting investigations in the countries cited is conducted for the purpose of protecting classified information and intelligence. However, allowing the Agency and Nicoc the

18Commission Report Part 5 Volume 1 para 378 at page 153.
19Commission Report Part 5 Volume 1 para 379 at pages 153-154.
20Commission Report Part 5 Volume 1 paras 385 to 388 at pages 156-158.
21The Bill para 1.6.3.2 at p36.

discretion to choose who ought to be vetted and conflating vetting investigations with criminal investigations is not consistent with these jurisdictions.

35 For example, in the United Kingdom ("*UK*"), vetting is conducted by United Kingdom Security Vetting ("*UKSV*"). Significantly, this body is separate from the security services. The security services appear to conduct their own vetting investigations for individuals to be employed by them.

36 What is clear from the policy of the United Kingdom is that the purpose of vetting investigations is to determine whether or not an individual can be trusted with sensitive Government information or assets.[22] Categories of individuals affected include the following:

i. *"Crown servants, including*
ii. *Civil servants;*
iii. *Members of the security and intelligence agencies;*
iv. *Members of the armed forces;*
v. *The police;*
vi. *Employees of certain other non-government organisations which are obliged to comply with the Government's security procedures;*
vii. *Employees of contractors providing goods and services to the Government*."[23]

37 There is no obligation for individuals to go through the vetting process. However, it is required for individuals working in government to have access to certain buildings and IT services.[24] The common feature among the persons required to be vetted is their degree of access to government information and facilities.

38 There appear to be four levels of security clearance in the UK: Accreditation Check ("*AC*"), Counter-Terrorist Check ("*CTC*"), Security Check ("*SC*") and Developed Vetting

22Houses of Parliament "National Security Vetting: Your Questions Answered" (2017) available at https://www.parliament.uk/globalassets/mps-lords--offices/offices/pass-office/psd-national-security-vetting-booklet.pdf at p5.
23Houses of Parliament "National Security Vetting: Your Questions Answered" (2017) at p.7.
24"National Security Vetting" p. 13.

("*DV*"). DV appears to be the highest level of security clearance, required only where an individual's post requires them to have access to top secret assets or they will be working in the security and intelligence agencies.[25] For each of the categories, however, it is clear that the goal of the vetting process is to determine whether an individual is trustworthy enough to have access to varying degrees of confidential or classified information.

39 Vetting appears to also be required where individuals work in the aviation industry where CTC clearance is required. Vetting in this industry appears to be conducted by the UK's Civil Aviation Authority.[26]

40 The UK's Police Service is also subject to vetting. Governed by the Police Act of 1996, the Police Service conduct their vetting investigations themselves in accordance with their own Vetting Code of Practice.[27]

41 In all of the above circumstances, vetting of individuals is carried out to certain specifications depending on the role in which an individual seeks to be employed. Those who are considered "*critical suppliers to government*" are required to be vetted in terms of Schedule 7 of the National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021. According to this Schedule, contractors who process or store material which is classified as secret or top secret are required to be vetted above the level of "*Security Check*".

42 The requirements for obtaining security clearance depends on the level at which it is sought. At the highest (DV) level, the following is required:

i. "successful completion of the Baseline Personnel Security Standard
ii. completion, by the individual, of a DV security questionnaire
iii. a departmental/company records check which will include personal files, staff reports, sick leave returns and security records

25"National Security Vetting" p. 11.
26https://www.caa.co.uk/commercial-industry/security/national-security-vetting/
27Statutory Code of Practice and guidance setting out the principles and ethical standards relating to vetting (20 July 2023) available at https://www.college.police.uk/guidance/vetting-code-practice .

iv. a check of both spent and unspent criminal records
v. a check of credit and financial history with a credit reference agency
vi. a check of Security Service (MI5) records
vii. a full review of personal finances
viii. a detailed interview conducted by a trained Investigating Officer
ix. further enquiries, including interviews with referees conducted by a trained Investigating Officer
x. checks may extend to third parties included on the security questionnaire
xi. the full review of personal finances will include an assessment of an individual's assets, liabilities, income and expenditure both on an individual basis and taking into account the joint position with a spouse or partner.[28]

43 These requirements are similar to those required by our current vetting system for Top Secret security clearance.

44 What is clear from the above is that the UK's system of security vetting is similar to our own at present. Security clearance is required depending on the nature of the work to be conducted by the individual and the access to classified information they may have. There is, however, no particular body who may deem a person or institution to be of national security interest and require them to be vetted as such.

45 Similarly, in Canada, security screening is a process conducted on individuals who will have access to sensitive information, assets or facilities depending on the nature of their work for the Canadian government.

46 Security screening is conducted by the Canadian Security Intelligence Service ("*CSIS*") and is governed by the Standard on Security Screening of 20 October 2014.[29] According to the Security Screening Model in Appendix B to the Standard, "*security screening requirements are determined by the duties to be performed and by the sensitivity of*

28National security vetting: clearance levels (2 December 2022) available at https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels
29Available at https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=28115#appB

information, assets or facilities to be accessed, and in accordance with the Position Analysis tool and guidance issued by the Secretariat."

47 The Standard provides for two levels of screening: Standard and Enhanced. According to the definitions, standard screening is conducted where a person's duties and access to information, assets and facilities are not directly related to the security and intelligence functions. Enhanced screening, on the other hand, is required when the duties and access to information, assets and facilities are directly related to the security and intelligence functions.

48 According to the Security Screening Model in Appendix B:

"Enhanced screening is conducted in limited and specific circumstances, and in accordance with the following criteria:

49 *When duties or positions involve, or directly support, security and intelligence (S&I) functions, including access to sensitive law enforcement or intelligence-related operational information, (i.e., sources or methodologies);*

50 *When duties or positions involve direct joint operational activity with S&I departments or agencies;*

51 *When duties or positions involve the provision of services to S&I departments or agencies which include management of, or access to, an aggregate of S&I information; or*

52 *When duties or positions, and related access to sensitive information, create a high risk that an individual may be influenced by criminal or ideologically motivated persons or organizations."*

53 Therefore, like in the UK, security screening in Canada is required depending on an individual's access to classified information, assets or facilities. There is no provision for a body to decide that a person or institution requires security clearance based on its

"*national security interest*".

54 The proposed inclusion of s2A(1)(a)(iv) of the National Strategic Intelligence Act does not align with practices in either the UK or in Canada – both of which have been cited by the Bill as benchmark jurisdictions.

55 In fact, the proposed amendment appears to be an attempt to shoehorn additional investigative powers on the SSA through the vetting process in order to appear to be complying with FATF's requirements.

What does FATF require?

56 What is clear from the above is that the amendment to the vetting mandate is not in line with international practice. The amendment also appears to conflate the process of vetting with other forms of investigation.

57 According to the FATF Follow-Up Report & Technical Compliance Re-Rating of November 2023[30] ("*the Follow-Up Report*"), South Africa is now considered partially compliant with recommendation 8 (relating to NPOs):

> *"Since the MER, South Africa, has amended the NPO Act. The main improvement has been to require the registration of a certain category of NPOs at risk so that accounting and reporting measures can be implemented against them. South Africa has also started taking steps to address administration and management of NPOs to mitigate TF risks. South African authorities also have the range of investigative powers to investigate suspected TF activities involving NPOs. However, South Africa still needs to work on assessing the TF risk and threats of NPOs as well as to review whether the measures taken, address these risks. For certain categories of NPOs, the 2022 amendments to the NPO Act creates obligations for registration. However, as the work on the identification of NPOs exposed to TF risk is still on-going, not all*

30Available at https://www.fatf-gafi.org/content/dam/fatf-gafi/fur/South-Africa-FUR-2023.pdf.coredownload.inline.pdf

relevant NPOs may be covered by the obligations under the NPO Act. Recommendation 8 is re-rated as Partially Compliant."[31] (our emphasis)

58 FATF has therefore acknowledged the steps taken in amending the NPO Act to require registration, but more work is required in assessing terror financing risks and vulnerabilities in the NPO sector.[32] Such assessment will be a function of research or, as FATF points out, discussions need to be had with NPOs in order to refine best practices to address terror financing risks and vulnerabilities (in which respect we remain non-compliant).[33] This will not be achieved by vetting investigations conducted on NPOs.

59 Importantly, it should be noted that FATF now views Criterion 8.5 b&c to be met as follows:

"Criminal investigations (R.30-31) would be carried out in the same way as for other suspicions of TF and there are no limitations imposed by the NPO Act. The SAPS: DPCI have the capacity to investigate suspected TF activities, including through NPOs. The FIC has access to any public register under the FIC Act. In addition, DSD is in the process of appointing a panel of Forensic Investigators and Data Analyst to conduct preliminary investigations on suspicious NPOs."[34]

60 What is clear, therefore, is that FATF no longer requires South Africa to enhance its investigation capacity in order to counter possible terror financing in the NPO sector. Any amendments to the vetting provisions in the intelligence legislation is therefore not for the purposes of FATF compliance.

61 It is likely that this requirement has been met due to amendments to other legislation that have been enacted recently, such as amendments to the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004. Further amendments to the intelligence legislation at this stage is therefore unnecessary to meet this requirement.

31Paragraph (g) at p17.
32See in particular Criterion 8.2 paras (b) a. and b. at p15.
33Criterion 8.2 para c. at p15.
34At p16.

Conclusion

62 The Bill proposes to empower the intelligence structures to conduct vetting investigations on any person deemed to be of national security interest. How such a person is deemed to be of national security interest remains opaque, and seems to be subject to the whims of either Nicoc or the intelligence structures themselves. This does not address the concerns of FATF. Indeed, FATF's concerns regarding criminal investigations in the NPO sector have already been met and there is no need to amend the intelligence laws for this purpose.

63 The provision also seems to try to extend the purpose of vetting in such a way that it now encompasses investigations better suited to be carried out by the police service or the Hawks. The purpose of vetting in South Africa and worldwide is to assess an individual's competence to be exposed to classified material, not to investigate possible terror financing. The proposed amendment is therefore non-sensical in this context.

64 Rather, by leaving the definition of "*national security interest*" in the hands of Nicoc and the intelligence services, the proposed amendment leaves vetting investigations open to possible abuse by the security structures.

SIGNALS INTELLIGENCE AND THE NATIONAL COMMUNICATIONS CENTRE

65 As mentioned above, the Bill also attempts to "*remedy the defects on the functioning of the Signals Intelligence Capacity as confirmed by the Constitutional Court*". This it does by adding a subsection empowering the use of signals intelligence (or bulk interception of communications) by the security structures. As will be shown below, this provision does not go far enough to address the issues raised by the Constitutional Court and High Court on this issue.

The proposed amendment

66 The Bill makes the following provision for the National Communications Centre ("*the Centre*" or "*NCC*") to gather Signals Intelligence by adding the following subsection to the National Strategic Intelligence Act:

"2(2B)(1) The Centre shall, in a prescribed manner, and with regard to foreign signals, communications and non-communications—

(a) gather, correlate, evaluate and analyse relevant intelligence in order to identify any threat or potential threat to national security subject to—

(i) submission of bulk interception application in the form and manner, as prescribed for approval by a retired Judge appointed by the President, after consultation with the Chief Justice;

(ii) two advisory interception experts appointed by the Minister based on his or her relevant qualifications and experience in the field; and

(iii) the Centre supplying relevant intelligence to the national intelligence structures."

67 Ostensibly, this provision is meant to address the High Court and Constitutional Court's rulings that bulk surveillance activities and foreign signals interception undertaken by the NCC are unlawful and invalid.[35]

68 The rulings in question are the cases of *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others*[36] and *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice*

35The Bill para 1.4.2 at p34.
362021 (3) SA 246 (CC) (4 February 2021).

and Correctional Services and Others,[37] the Constitutional Court and High Court judgments respectively.

69 The drafters of the Bill appear to have interpreted both Courts' decisions as indicating that bulk interception activity is outlawed until such activities are provided for in law.[38] This is an unfortunate oversimplification.

The requirements set out by the High Court and Constitutional Court

70 While the Constitutional Court ultimately found that the practice of bulk surveillance was unlawful and invalid because s2 of the National Strategic Intelligence Act did not provide for it,[39] this is not the only finding of significance. For example, the Constitutional Court also found that "*without doubt*" bulk surveillance constitutes the exercise of public power, and that power can only be exercised in a constitutionally compliant manner.[40] They also point out that the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("*RICA*") contains an express prohibition against communication interceptions without interception directions.[41] The Constitutional Court therefore interpreted s2 of the National Strategic Intelligence Act in light of that prohibition as well as the right to privacy contained in the Bill of Rights in determining that it did not provide for bulk interception of communications.

71 Significantly, the Constitutional Court's order relating to the provisions of RICA regarding targeted interception of communications would also have application in the drafting of legislation providing for bulk interception of communications. For example, the Constitutional Court confirmed the High Court's declaration of unconstitutionality of the provisions of RICA to the extent that it fails to provide safeguards to ensure the Judge designated in terms of s1 is "*sufficiently independent*".[42] According to the Constitutional Court, RICA lacked provisions to ensure the structural, operational and perceived

372020 (1) SA 90 (GP) (16 September 2019)
38The Bill para 1.4.3 at p34.
39Para 135.
40Para 130.
41Para 133.
42Item 6(a) of the Order.

independence of the designated judge, especially given that directions are sought and issued in complete secrecy.[43] The same would be true of bulk communications interception.

72 The High Court went further in elaborating on what provisions relating to the independence of the designated judge would look like. For example, Sutherland J points out that a non-renewable term of office is already a well-known measure to bolster independence.[44] Appointment of the designated judge by the Judicial Services Commission was found to be a possible measure to ensure independence, rather than appointment by the Minister. This was not made part of the interim order because a governing process would need to be put in place.[45] However, the principle is nonetheless relevant to the present legislation: more care needs to be taken in drafting provisions which set out processes to ensure independence of the designated judge in order for those provisions to be Constitutionally compliant.

73 Both judgments also emphasized the value of having a panel of persons to evaluate such applications in order to add to the adversarial nature of the process.

74 In its current form, the section in the Bill is ambiguous as to the role and nature of the "*two communications experts*". Despite being mentioned in the section, the section may be interpreted to mean that only the judge need be approached for the interception direction.

75 The High Court also pointed out that, while bulk communication interception is meant to address foreign threats, it is common cause that communications between persons in South Africa's borders would be covered where the server is located outside of our borders.[46] What this means is that bulk interception of communications may be used to spy on the communications of South African citizens communicating with each other, and not just foreign threats. This is the same concern raised by Mr Edward Snowden with

43Para 93.
44Para 66.
45Para 70.
46Para 145.

regard to the National Security Agency's practices of bulk communications interception.[47] As such, bulk communications interception is also a clear breach of the right to privacy, and circumstances in which such a breach would be justified should be clearly defined.

76 The proposed amendment regarding bulk communications interception is also somewhat sparse when compared to the equivalent provision in RICA. Section 16 of RICA sets out the required contents of the interception application, as well as the grounds upon which the designated judge may make his/her decision. The same sort of detail is not present in the proposed provision in the Bill: the provision simply provides that the NCC may conduct bulk interception of communications subject to an application to the designated judge. The provision does not even require that such application be granted and on what grounds. On this basis alone, it seems unlikely that the proposed provision would pass constitutional muster.

77 Both the High Court and the Constitutional Court found that s16 of RICA contained inadequate safeguards to protect the right to privacy when targeted communications are intercepted. It seems likely that the Courts will also rule the proposed section regarding bulk interception of communications to be unconstitutional.

The dangers of further Regulations

78 It seems to be the intention of the drafters of the Bill to supplement the sparsity of the proposed s2(2B)(1) with regulations made by the Minister. Section 6 of the Bill proposes to add additional broad powers to the Minister to make regulations in terms of s6 of the National Strategic Intelligence Act. Included in this list is the proposed subsection (fE) which empowers the Minister to regulate the manner and form in which the Service, Agency and the Centre shall be coordinated.

79 Another notable inclusion is subsection (fK) which empowers the Minister to regulate "*the manner and form in which the Intelligence Services shall supply post-interception*

47See Jane Duncan "Bulk communication surveillance in South Africa – fix it or nix it" (30 September 2019) *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2019-09-30-bulk-communication-surveillance-in-south-africa-fix-it-or-nix-it/

reporting to the Judge referred to in section 2(2)(B)". This appears to imply that the Minister has a discretion as to how much information the signals intelligence judge has access to after bulk communications have been intercepted.

80 The danger which is apparent from this provision is that that the judge him/herself may be left in the dark as to the real consequences of an application granted for such interception.

81 This has implications for the effectiveness of the oversight to be provided by such a judge. It also flies in the face of the recommendations of the HLRP and the Commission that executive interference in the functioning of the intelligence structures ought to be limited.[48] It further adds to the very real fear that such a judge will be lied to or be misled by the intelligence structures – as the judge granting the application to intercept the communications of Hofstatter and Wa Afrika was lied to in the *Amabhungane* case.[49]

82 Overall, the provision for oversight of signals intelligence is inadequately drafted and unlikely to pass constitutional muster in its current form. It also flies in the face of principles laid down by our courts and recommendations made by the HLRP and the Commission.

83 As to how this provision may be amended, some guidance may be found in s16 of RICA to the extent that it has been found to be constitutionally compliant. Some guidance may also be found in systems in place in other jurisdictions.

Guidance provided by the Grand Chamber of the European Court of Human Rights

84 The question of what constitutes sufficient safeguards regulating bulk communications interception has fairly recently been considered by the Grand Chamber of the European Court of Human Rights ("*ECHR*") in the *Case of Big Brother Watch and others v United Kingdom*.[50] This case centred around the question of whether the United Kingdom's

48As discussed below.
49High Court judgment, para 20.
50Applications nos 58170/13, 62322/14 and 24960/15, handed down on 25 May 2021, available at

practice of bulk communications interception was compliant with the EU's Article 8 right to privacy.

85 Prior to this case, the Grand Chamber had considered the same question with respect to targeted interception of communications (similar to our *Amabhungane* case) in the decisions in *Weber and Saravia v Germany*[51] and *Liberty and others v the United Kingdom*.[52] In these decisions, the ECHR laid out six procedural standards (the "*Weber minimum safeguards*") which each EU state's domestic law authorizing surveillance must specify, namely:

"the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[53]

86 In our domestic law, s16 of RICA contains some of these principles. Those not contained in RICA were challenged in *Amabhungane*, which resulted in our Constitutional Court including the following in its order:

> *"6. The declaration of unconstitutionality by the High Court is confirmed only to the extent that the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA) fails to—*
>
> *(a) provide for safeguards to ensure that a Judge designated in terms of section 1 is sufficiently independent;*

https://www.brickcourt.co.uk/images/uploads/documents/Big_Brother_Watch_GC_Judgment_-_25-5-21.pdf

51Application no 54934/00 of 29 June 2006, available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76586%22]}

52Application no 58243/00 of 1 October 2008, available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-87207%22]}

53*Weber and Saravia v Germany* at para 95.

(b) provide for notifying the subject of surveillance of the fact of her or his surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated;

(c) adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte;

(d) adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data; and

(e) provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist".

87 It can therefore be seen that South African jurisprudence on this issue is very much in line with that of the ECHR and the Weber minimum safeguards.

88 In the Case of *Big Brother Watch and others v United Kingdom,* the ECHR reconsidered the Weber minimum safeguards in the context of bulk interception of communications. The court found that, given the nature of bulk communications interception, the first two of the Weber safeguards do not find application, namely the need to specify the nature of the offences which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped. However, the ECHR specified as follows:

"Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may

resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorized and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments – that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed – are equally relevant to bulk interception.

…

In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process)."[54]

54 *Big Brother Watch and others v United Kingdom* paras 348 to 350.

89 Ultimately, the ECHR found that the United Kingdom's bulk surveillance regime was a violation of the Article 8 right to privacy, except insofar as information sharing with other states was concerned.[55]

90 By contrast, the ECHR in the case of *Centrum för rättvisa v. Sweden*[56] found that the main features of the Swedish bulk interception regime met the Convention requirements and in most aspects kept within the limits of what is "*necessary in a democratic society*".[57] A summary of the ECHR's findings are as follows:

> *"367. The review of the Swedish bulk interception system in the present case has revealed that it is based on detailed legal rules, is clearly delimited in scope and provides for safeguards. The grounds upon which bulk interception can be authorised in Sweden are clearly circumscribed, the circumstances in which communications might be intercepted and examined are set out with sufficient clarity, its duration is legally regulated and controlled and the procedures for selecting, examining and using intercepted material are accompanied by adequate safeguards against abuse. The same protections apply equally to the content of intercepted communications and communications data.*
>
> *368. Crucially, the judicial pre-authorisation procedure as it exists in Sweden and the supervision exercised by an independent body in Sweden serve in principle to ensure the application of the domestic legal requirements and the Convention standards in practice and to limit the risk of disproportionate consequences affecting Article 8 rights. Notably, regard must be had to the fact that in Sweden the limits to be observed in each bulk interception mission, as well as its lawfulness and proportionality in general, are the subject matter of judicial pre-authorisation proceedings before the Foreign Intelligence Court, which sits in the presence of a privacy protection representative defending the public interest.*

55Items 1 to 5 of the order at pages 156-157.
56Application no. 35252/08 delivered 25 May 2021, available at https://hudoc.echr.coe.int/fre#%7B%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-210078%22]%7D
57Para 373.

369. The Court noted three shortcomings in the Swedish bulk interception regime: the absence of a clear rule on destroying intercepted material which does not contain personal data (see paragraph 342 above); the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration is given to the privacy interests of individuals (see paragraphs 326-330 above); and the absence of an effective ex post facto review (see paragraphs 359-364 above)."

91 Both of these judgments refer to the 2015 Report of the European Commission for Democracy through Law ("*the Venice Commission*") on the Democratic Oversight of Signals Intelligence Agencies.[58] Some of the relevant parts of the Venice Commission Report cited by the ECHR include its finding that the two most significant safeguards in signals intelligence were the authorisation (of collection and access) and the oversight of the process. Oversight in particular, has to be performed by an independent, external body. Where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage.[59]

92 The Venice Commission found that notification of the subject of interception was not an absolute requirement of Article 8 of the Convention, since a general complaints procedure to an independent oversight body could compensate for non-notification.[60] In South Africa such a body could be the IGI.

93 The Venice Commission found that a "*primary safeguard*" would be the internal controls of the intelligence services themselves. Recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.[61]

94 Like in the *Amabhungane* case, the Venice Commission considered the special position of journalists. It accepted that they were a group which required special protection, since

58Available at https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e
59*Centrum för rättvisa v. Sweden* para 87.
60*Centrum för rättvisa v. Sweden* para 88.
61*Centrum för rättvisa v. Sweden* para 89.

searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so.[62]

Conclusion

95 What can be seen from the above is that the proposed new sections dealing with signals intelligence are not only unconstitutional, but they are also woefully inadequate when compared to standards set in other democratic countries.

96 The section on bulk communications interception needs significant revision, in line with the Amabhungane judgments, in order to provide sufficient safeguards and oversight mechanisms within the legislation itself. It is not sufficient to leave the details of such safeguards to be regulated by the Minister.

RECOMMENDATIONS OF THE HLRP AND THE COMMISSION

97 Both the HLRP and the Commission made several recommendations for improvement for the security services. However, only one of these recommendations seems to have made it into the Bill, namely the splitting of the SSA into two: foreign and domestic intelligence.

Notably absent from the Bill are the following:

- Measures to strengthen and increase the independence of the Office of the Inspector General of Intelligence ("IGI").[63]

62*Centrum för rättvisa v. Sweden* para 90.
63Commission Report Part 5 Vol 1 para 932 at p350. This has also been pointed out by the OIGI itself: see https://www.news24.com/news24/politics/parliament/spy-bill-inspector-general-of-intelligence-concerned-about-bill-weakening-its-independence-20231208.

- Regarding the independence of the IGI, the Chief Justice made reference to the Constitutional Court decisions of *Hugh Glenister v President of the Republic of South Africa and others*[64] and *Robert McBride v Minister of Police and others*[65] when elucidating on the meaning of "*independence*".[66]

- In particular, the Chief Justice pointed to the fact that the IGI uses the SSA's ICT infrastructure and server which the SSA had access to. He further stated that the IGI must appear to be independent as well as be truly independent.[67] The sharing of ICT infrastructure undermines this perceived independence.

- To this end, the HLRP recommended that the IGI should be established as a separate entity with its own administration and budget,[68] and that it should be given legislated status.[69]

- Measures to allow the IGI greater access to classified information and the activities of the intelligence services.[70]

- Measures to prevent interference by the Minister in charge of intelligence and the President in the operations of the intelligence services.[71]

- As was pointed out by the HLRP, "[t]*he current legislative provisions regarding the role of the Minister of State Security vis-à-vis the department itself give too much scope for a Minister to interfere in the administration and operations of the department*."[72] Not only does the Bill not remedy this problem, but it gives the Minister even greater powers. This will be discussed in more detail below.

---

64 2011 (3) SA 347 (CC).
65 2016 (2) SACR (CC).
66 Commission Report Part 5 Vol 1 paras 935 to 938 at pages 351-353.
67 Commission Report Part 5 Vol 1 para 936 at p352.
68 HLRP Report para 1.11.1.6 at p15.
69 HLRP Report para 1.11.1.9 at p15.
70 Commission Report Part 5 Vol 1 para 880 at p332; para 939 at p350.
71 Commission Report Part 5 Vol 1 paras 857 to 858 at p326, at para 883 at p328.
72 HLRP Report para 1.7.1.1 at p11.

- Measures to give adequate access and top security clearance to certain staff at the Auditor General ("*AG*") such that they may audit the intelligence services more effectively.[73]

- Measures to enhance the oversight roles of the IGI, the AG and the Joint Standing Committee on Intelligence ("*JSCI*") to promote greater transparency.[74]

98 The Chief Justice further recommended that there should be no executive involvement in recruitment at the security services.[75] This mirrors the recommendations of the HLRP.[76]

99 One of the recommendations of the HLRP which very clearly has not been taken into consideration is the problematic Security Services Special Account Act 81 of 1969 and the Secret Services Act 56 of 1978. The HLRP found that these pieces of legislation are "*apartheid-era pieces of legislation designed at the time to facilitate the regime's secret operations such as sanctions-busting, assassinations, propaganda etc and have no place in our constitutional democracy*."[77] Rather than repealing these Acts as recommended by the HLRP,[78] the Bill has only made amendments to them to accommodate the splitting of the SSA into the Agency and the Service.

100 Not only have these recommendations not been implemented in the Bill, but, as will be shown below, the spirit of these recommendations have not been echoed in some of the other amendments to the legislation as proposed by the Bill.

Proposed amendments contrary to the spirit of the HLRP and Commission's recommendations.

101 As mentioned above, the HLRP pointed out that legislation currently allows for political interference in the functioning of the intelligence service. In particular, the HLRP made reference to s12 of the Intelligence Services Act which reads as follows:

73Commission Report Part 5 Vol 1 para 881 at p333; para 940 at p353.
74Commission Report Part 5 Vol 1 para 885 at p334.
75Commission Report Part 5 Vol 1 para 896 at p339.
76HLRP Report para 1.7.1.1 at p11.
77HLRP Report para 1.5.1.15 at p9.
78HLRP Report para 1.5.2.12 at p10.

"12. General powers of Minister.—

(1) The Minister may, subject to this Act, do or cause to be done all things which are necessary for the efficient superintendence, control and functioning of the Agency.

(2) Without derogating from the generality of his or her powers in terms of subsection (1), and notwithstanding anything to the contrary contained in any other law, the Minister may —

(a) acquire any immovable property, with or without any buildings thereon which is necessary for the efficient functioning of the Agency and, subject to section 70 of the Public Finance Management Act, 1999 (Act No. 1 of 1999), supply guarantees, indemnities and securities for that purpose;

(aA) erect or maintain buildings on the property so acquired;

(b) sell or otherwise dispose of immovable property which is no longer required for any purpose contemplated in paragraph (a);

(c) acquire, hire or utilise any movable property and any other equipment which may be necessary for the efficient functioning of the Agency;

(d) sell, let or otherwise dispose of anything contemplated in paragraph (c), which is no longer required for the said purposes. (emphasis added by the HLRP)"

102 The HLRP found that this section gave the Minister too much scope to interfere in the administration and operations of the department.[79] This had disastrous consequences during the state capture years.

103 The Bill in its current form amends this section only to the extent that it now allows

79HLRP Report para 9.4(a) at p101.

the Minister to interfere in the Intelligence Services, Centre and Academy.[80] This concern of the HLRP has therefore not been addressed.

104 Not only this, but the warnings of the dangers of Ministerial involvement sounded by the HLRP and the Chief Justice have not been heeded. The Bill makes provision for an amendment to s6 of the National Strategic Intelligence Act such that the Minister is empowered to promulgate Regulations on an extensive array of matters, including the following subsections:

"(fE) the manner and form in which the operations of the Service, the Agency and the Centre shall be co-ordinated;

…

"(fH) the manner and form in which policy and legislative compliance monitoring shall be enforced by the Minister in the exercise of Ministerial control and direction as envisaged in the Constitution;"

105 The highly problematic subsection (fD) also remains in place, which provides that the Minister may regulate "*any matter necessary for the effective execution and administration of counter-intelligence functions and the co-ordination and interpretation of intelligence products*."

106 Read together, these provisions provide the Minister with broad and far-reaching powers to interfere in the operations of the intelligence structures in violation of the recommendations of the Commission and the HLRP.

107 The Bill also seeks to amend s8 of the Intelligence Services Oversight Act by giving even more control to the Minister over the functions of the IGI: s12 of the Bill proposes to mandate the Minister to make regulations regarding the performance of the functions designated to the IGI. The previous version of the Act stated that the Minister "*may*" make

80Section 23 of the Bill.

such regulations. This is clearly against the recommendations of the Commission and the HLRP, both of which called for greater independence for the IGI.

CONCLUSION AND RECOMMENDATIONS

108 The Bill in its current form is problematic in a number of respects. This submission has only focussed on three of these, namely changes to the security vetting regime, the provision relating to signals intelligence, and the extent to which the recommendations of the Commission and the HLRP have not been incorporated in the proposed amendments. In all of these respects, the Bill requires significant revision. In particular the following is recommended:

Regarding security vetting:

109 All proposed amendments to s2A(1)(a) of the National Strategic Intelligence Act ought to be abandoned.

110 There is no reason to include the additional category of persons and institutions of national security interest into the section. To do so would be contrary to our current system of vetting and international practice. It would further open the vetting process for abuse. It is also not necessary to amend this section to comply with FATF requirements.

Regarding signals intelligence:

111 he proposed s2(2B)(1) of the National Strategic Intelligence Act must be significantly revised.

112 The revised provision must contain at a minimum the following provisions (in line with the *Amabhungane* judgments and international practice:

- safeguards to ensure that the designated Judge is sufficiently independent;

- safeguards to address the fact that interception directions are sought and obtained *ex parte* – in particular, the role of the communications experts must be detailed;

- detailed grounds upon which bulk interception of communications may be authorised;

- provision for notifying the subject of surveillance of the fact of her or his surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated;

- procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data;

- safeguards where the subject of surveillance is a practising lawyer or journalist;

- provision for independent *ex post facto* review of bulk communications interception, such as by the IGI.

113 The process of signals intelligence must also be shielded from executive interference. As such, the proposed s6(1)(fK) of the National Strategic Intelligence Act ought to be deleted from the Bill.

Regarding the recommendations of the HLRP and the Commission:

114 The Bill presents an opportunity to implement the recommendations of the HLRP and the Commission. In particular, the Bill ought to include the following provisions:

- Provision ought to be made for greater independence of the IGI.

- Provision ought to be made for enhanced oversight by the IGI, JSCI and AG by granting better access to classified information by these bodies.

- Powers of the Minister to interfere with the operations of the security services ought to be limited. In particular, s12 of the Intelligence Services Act ought to be amended.

- **The Security Services Special Account Act 81 of 1969 and the Secret Services Act 56 of 1978 ought to be repealed in their entirety.**

Submissions in respect of the General Intelligence Laws Amendment Bill published in Notice No 4067 in Government Gazette 49717 dated 14 November 2023.

PART 2: ADDITIONAL PRACTICAL CONSIDERATIONS AND ACCOMPANYING RECOMMENDATIONS

INTELWATCH

Table of Contents

Note:

Throughout this document, whenever we refer to the "intelligence services", we mean the following: the South African Intelligence Agency; the South African Intelligence Service (as provided for in GILAB 2023); the Crime Intelligence Division of the South African Police Service (CI), and the intelligence division of the South African National Defence Force (DI)

When we refer to "intelligence entities" we mean the National Communications Centre (NCC) (as provided for in Gilab 2023), the Office of Interception Centres (OIC) (as provided for in RICA), and the South African National Academy of Intelligence (SANAI) (as provided for in Gilab 2023).

When we refer to intelligence services and entities, or the services and entities, or the intelligence community, we referring to the Agency, the Service, CI, DI, the NCC, the OIC, and SANAI.

When we speak of "intelligence oversight" we are referring to all oversight of any and/or all of these entities.

When we speak about intelligence oversight structures, we mean the Office of Inspector General of Intelligence (IGI), the Joint Standing Committee on Intelligence (JSCI), the Auditor-General, and the Evaluation Committee.

COMMENTS ON THE GENERAL INTELLIGENCE LAWS AMENDMENT BILL OF 2023

1. Problematic legal definitions of core concepts

1.1 The definition of national security

The Bill provides highly problematic definitions for a number of core constructs that will be central to the Bill's interpretation once enacted. These include the definitions of 'national security,' 'opportunity or potential opportunity,' and 'threat to national security'. These definitions, discussed below, are vague, overly broad, and often rely on circular reasoning (which detracts from their meaningfulness). The net result, is that various aspects of the Bill that rely on the meaning of these definitions are open to unacceptably wide interpretations by the state intelligence services and entities. Such potential interpretations leave room for a wide scope of abuses by the services and entities.

The Bill's definitions for these three concepts are as follows:

“national security” is defined as “the capabilities, measures and activities of the State to pursue or advance—

(a) any threat;
(b) any potential threat;
(c) any opportunity;
(d) any potential opportunity
(e) the security of the Republic and its people,
in or outside the Republic in accordance with section 198 of the Constitution;’’

“opportunity or potential opportunity” is defined as follows: “subject to the Bill of Rights and the principles enshrined in the Constitution, such capability, measure or activity employed to pursue and advance national security in accordance with section 198 of the Constitution;”

“threat to national security” is defined as follows:

“‘threat to national security” includes any action or omission which may potentially cause damage, harm or loss to the national security, which includes—

(a) any activity that seeks to harm the advancement and promotion of

equality and equitable access to opportunities by all South Africans

as provided for in section 9 of the Constitution;

(b) any activity that seeks to harm the advancement and promotion of

peace and harmony and freedom from fear and want for South

Africans;

(c) use of force or violence against the people of the Republic or the territorial integrity of the Republic;

(d) foreign hostile acts directed at undermining the constitutional order of the Republic;

(e) terrorism, terror financing, illicit money flows, money laundering, corruption or terrorist-related activities

(f) subversion and undue influence by hostile interests on government processes, policies and the sovereignty of the State and its organs;

(g) espionage, including acts of unauthorised access, disclosure and exposure of a state security matter, exposure of economic, scientific or technological secrets vital to the Republic;

(h) serious acts of violence, intimidation and sabotage directed at harming security of the Republic, its people and national critical infrastructure as well as acts directed at overthrowing the constitutional order of the Republic;

(i) acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of force and carrying out of its 60 constitutional responsibilities and any legal responsibilities to a foreign country and international organisation in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not, but does not include lawful political activity, advocacy, protest or dissent;

(j) threats or potential threats of calamity or any harmful or contagious episode or pandemic which occurs naturally or artificially induced or declared in law as a national state of disaster;

(k) acts of theft or siphoning of state financial resources and its related corrupt activities"

The problematic aspects of these definitions are discussed in more detail in the next section.

1.2 Conflation and circular reference errors

While each of these three definitions are problematic in and of themselves (as will be discussed below), their conflation greatly exacerbates their respective shortcomings. The Bill's definition of "national security" relies on the definition of "opportunity or potential opportunity" as well as the definition of "threat to national security". However, it is evident that the latter two definitions rely on the definition of "national security" for their meanings. This conflation has resulted in circular reference errors, which leave the interpretations of these core intelligence concepts, as well as their impact on the services' day-to-day operations, open to debate and the imaginations of intelligence officials and the relevant minister/president. If the Bill is passed leaving these errors in

tact, another amendment will possibly need to be drafted to correct this situation.[81]

1.3 Vagueness

The above situation is exacerbated by the vagueness the each of the three definitions[82].

The definition of *"national security"* relies on the interpretation of section 198 of the Constitution. This section reads as follows:

The following principles govern national security in the Republic:

1. *(a) National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life.*
2. *(b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.*
3. *(c) National security must be pursued in compliance with the law, including international law.*
4. *(d) National security is subject to the authority of Parliament and the national executive.*

It is evident that section 198 explicates principles. As it stands, it does not provide clarity as to what exactly the *"capabilities, measures and activities of the State"* that encompass *"national security"* entail. In other words, what these capabilities, measures and activities of the intelligence services and entities will be comprised of, in practicality, will ultimately be left up to the discretion of the government of the day and its intelligence community.

Similarly, the definition of *"opportunity or potential opportunity"* refers to "*such capability, measure or activity employed to pursue and advance national security"*. Once again, the concepts *"capability" , "measure" and "activity"* are not clearly defined, but instead rely on the broad governing principles of the Constitution and, again, on section 198 in particular. Thus, state intelligence services will be allowed to assign any number of meanings to these three concepts.

The definition of "*threat to national security"* does include more specificity regarding aspects

81 See, for instance, Nicholas Carrol *"Adjusting a definition"* . 12 October 2023. Cliffe Dekker Hofmeyr Incorporated. Available at https://www.cliffedekkerhofmeyr.com/news/publications/2023/Practice/Tax/tax-and-exchange-control-alert-12-october-adjusting-a-definition

82 Pierre De Vos, *"New intelligence bill is anti-democratic, and a unique mix of malice and stupidity".* 7 September 2023. The Daily Maverick. *A*vailable at https://www.dailymaverick.co.za/article/2023-09-07-new-intelligence-bill-is-a-unique-mix-of-malice-and-stupidity/

comprising threats. (For example, the definition refers to "*the use of force or violence against the people of the Republic"* and "*terrorism and terror financing"*.) However, vagueness in parts of the definition makes it difficult to establish what truly constitutes a threat. Once again, this creates an opportunity for abuse because no clear limits are placed on intelligence services and entities.

Although this is not an exhaustive list, the following aspects are particularly problematic:

A threat to national security can be:

(i) *"any action or omission which may potentially cause damage, harm or loss to the national security":*

> The definition is immediately overly broad, given the vague definition of national security (discussed above), and the conflation of these two definitions (as discussed above). Exacerbating this, is the use of the phrase ***"any action or omission"*** (own emphasis), as well as the word ***"potentially"*** (own emphasis). This definition allows for virtually any action (or lack thereof) to be interpreted as a "*threat"* by state intelligence services.

(ii) *"any activity that seeks to harm the advancement and promotion of equality and equitable access to opportunities by all South Africans as provided for in section 9 of the Constitution"*

> Section 9 of the Constitution deals with equality and, as such, with discrimination. It reads as follows:
>
> > *"1) Everyone is equal before the law and has the right to equal protection and benefit of the law.*
> >
> > *2) Equality includes the full and equal enjoyment of all rights and freedoms. To promote the achievement of equality, legislative and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination may be taken.*
> >
> > *3) The state may not unfairly discriminate directly or indirectly against anyone on one or more grounds, including race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth.*
> >
> > *4) No person may unfairly discriminate directly or indirectly against anyone on one or more grounds in terms of subsection (3). National legislation must be enacted to prevent or prohibit unfair discrimination.*
> >
> > *5) Discrimination on one or more of the grounds listed in subsection (3) is unfair unless it is established that the discrimination is fair."*
>
> It is unclear why a threat to national security would only be framed in terms of section 9, and not in terms of the entire Bill of Rights as contained in chapter two of South Africa's

Constitution.

iii) "subversion and undue influence by hostile interests on government processes, policies and the sovereignty of the State and its organs"

The inclusion of the broad terms *"government processes" and "policies"*, as well the introduction of the concept of *"hostile interests"* (which is undefined), creates an opportunity for those in control of government to label as a "*threat"* the legitimate political activities (including advocacy and protest action) aimed at governmental policy change. This, in turn, would open the path for state intelligence services to act against such *"threats"*.

(iv) *"espionage, including acts of unauthorised access, disclosure and exposure of a state security matter, exposure of economic, scientific or technological secrets vital to the Republic"*

The current definition of "*state security matter"* as provided for in the National Strategic Intelligence Act of 1994 (as amended s. 1 (k) of Act No. 11 of 2013) is as follows:

'"state security matter" includes any matter which has been classified in terms of any national law and which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency'

Given this already broad definition combined with the Bill's new, expansive definition, there is no clear legal framework with which to evaluate whether or not espionage has in fact been committed. It leaves wide room for interpretation, and thus for abuse by the services. It also creates the risk that whistleblowers or journalists reporting on issues that place the government of the day in a poor light, could be accused of espionage, since evidence and information related to matters in the public interest could be classified as state security matters. This has grave consequences for South Africans' constitutional right to freedom of expression.

Furthermore, the Bill already provides a clear definition for espionage as follows:

> *"'espionage' means the unlawful and intentional communication, delivery or making available of classified information to directly or indirectly benefit a foreign state, persons or institutions''*

It is unclear why the drafters of this Bill deemed it necessary to further expand – thereby introducing vagueness – to the proposed definition of the concept.

(v) *"acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of force and carrying out of its constitutional responsibilities and any legal responsibilities to a foreign country and international organisation in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not,* ***but does not include lawful political activity, advocacy, protest or dissent****"(own emphasis)*

It is unclear why the exclusion of legitimate lawful political, advocacy and protest activities

are only explicitly mentioned in 1(t)(i) of the Bill, and why such activities are not clearly defined and explicitly excluded from the entire definition of 'threat to national security'. This lack of explicit exclusion of these activities, coupled with the vagueness of the definition of national security, leaves room for abuse by the intelligence services.

1.4 Policy shift away from public safety and international obligations

Another problem relating the new definition of *"national security"* (given the inclusion of the concepts of *"threat"* , *"potential threat"* (the latter of which remains undefined), *"opportunity",* and *"potential opportunity"*) is that it broadens the mandate of state intelligence services and entities, allowing them to pursue matters not essential to promoting the safety and security of people in South Africa.

This policy shift away from the guarding of public safety and national interest is evident when one examines the current definition of *"national security"*, as provided for in the National Strategic Intelligence Act (Act 39 of 1994), as amended by the General Intelligence Laws Amendment Act s. 1 (g) of Act No. 11 of 2013).

The currently definition is as follows:

""**national security**" includes the protection of the people of the Republic and the territorial integrity of the Republic against—

(*a*) the threat of use of force or the use of force;

(*b*) the following acts:

(i) Hostile acts of foreign intervention directed at undermining the constitutional order of the Republic;

(ii) terrorism or terrorist-related activities;

(iii) espionage;

(iv) exposure of a state security matter with the intention of undermining the constitutional order of the Republic;

(v) exposure of economic, scientific or technological secrets vital to the Republic;

(vi) sabotage; and

(vii) serious violence directed at overthrowing the constitutional order of the Republic;

(c) acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of, force and carrying out of the Republic's responsibilities to any foreign country and international organisation in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not, but does not include lawful political activity, advocacy, protest or dissent;"

It is clear that the business of national security is currently one of promoting the safety of South African people as well as protecting the country's' resources and assets. In addition, there is a clear respect for the sovereignty of other nations, since national security also takes into account the "Republic's responsibilities to any foreign country and international organisation".

The Bill's definition of *"national security"*, however, omits this emphasis on the Republic's commitment to the safety of its people. Instead, the definition opens the door for intelligence services to pursue activities not necessarily related to public safety and international commitments.

This is exacerbated by the fact that the definition of *"national security"* allows for *"opportunities or potential opportunities"* and *"threats or potential threats"* to be pursued or advanced outside of South Africa's borders. The Bill's definition of *"threat to national security"* still refers to South Africa's "*legal responsibilities to a foreign country and international organisation"*, however, as it stands, the Bill could be interpreted in a way that allows for state intelligence services and entities to conduct activities in other countries that would benefit South Africa, while posing harms to those countries, or at the very least disregarding their sovereignty. This approach to intelligence is reminiscent of the tactics used by the United State's (US) Central Intelligence Services (CIA), a vehicle through which that country has in the past exercised its influence in foreign countries in secret, frequently to the detriment of local populations. This paradigm runs contrary to the changes envisioned for state intelligence in the post-apartheid era, as contained in the Intelligence White Paper.[83]

This represents a marked shift in the policy of South Africa's state intelligence services from a focus of safety and meeting one's international obligations, to a focus seeking to pursue the country's *"opportunities"* (whatever that may entail). There is no guarantee that such pursuits, which undoubtedly will be carried out in secret, won't be detrimental to South Africans and citizens of other countries.

1.5 A cascading effect

The vaguely crafted and overly broad definitions of the core concepts that underpin the Bill – *"national security" , "opportunity"* and *"potential opportunity"*, and *"threat to national security"* – have a cascading effect: all other definitions and sections in the Bill of which the meanings and interpretations hinge on these concepts, are affected. The effect, is that these other definitions are imbued with the similar vagueness and lack of clarity.

The following definitions in the Bill are therefore all overly broad, vague, and open to abusive interpretations by the intelligence services:

---

83 Government of South Africa, Intelligence White Paper of 1994, available at https://www.gov.za/documents/white-papers/intelligence-white-paper-01-jan-1995; see also Lauren Hutton,"*Overview of the South African Intelligence Dispensation",* (n.d.), Institute for Security Studies

- ‘domestic intelligence’
- ‘foreign intelligence’
- intelligence gathering’
- ‘national critical information infrastructure’
- ‘national security intelligence’
- *'person or institution of national security interest’*
- *'security competence test’*

In addition, every provision in the Bill that refers to the definitions of *“national security” , “opportunity”* and *“potential opportunity”*, and *“threat to national security”* are equally afflicted.

1.6 Conclusion:

Ultimately, the day-to-day work of the intelligence services and entities are delimited by the legal definition of *“national security”*; the criteria tied to this definition impact on what projects are carried out, what intelligence is gathered, what intelligence is shared, who's communications are intercepted, which surveillance operations are carried out, what operational actions are taken, who is assigned or contracted to do work for or with the intelligence services, who the services partner with, and where funds are directed (and which amounts). As it stands, the Bill's definitions of *“national security”*, *“threat to national security”* and “*opportunity or potential opportunity”* are simply too broad and do not provide sufficient clarity to ensure that state intelligence services and entities do not operate outside of their Constitutional mandate.

This state of affairs is particularly concerning, given the findings on malfeasance at the State Security Agency by the 2018 High Level Review Panel (HLRP) investigation of SSA, as well as the Judicial Commission of Inquiry into State Capture (the Zondo Commission).

1.7 Recommendations

(a) In order to curb abuse (or “potential abuse”) by the state intelligence services, the following definitions must be redrafted in a manner that clearly and reasonably limits their interpretation:

i. 'national security'
ii. 'threat to national security'
iii. 'domestic intelligence’
iv. ‘foreign intelligence’
v. 'intelligence gathering’

vi. ‘national critical information infrastructure’

vii. ‘national security intelligence’

viii. ‘person or institution of national security interest’

ix. ‘security competence test’

x. 'espionage'

(b) The concepts of *“opportunity”* and *“potential opportunity”*, along with their definition in the Bill, must be discarded in their entirety and all references removed from the Bill. Likewise, references to “*potential threat”* must also be removed entirely from the Bill.

(c) The concepts of *“lawful political activity”, “advocacy”, “protest”* and *“dissent”* needs to be clearly defined, and the definition of *“threat to national security”* should make explicit that these activities are *not threats to national security.*

(d) In the unfortunate event that any of these definitions are clarified in regulations drafted after the Bill is enacted, these regulations should be made public as soon as they are established, and should at no time be classified.

2. New security competence testing provisions: Targeting of NGOs and FBOs

The current version of the Bill, if enacted, will allow the state's intelligence services to conduct security competence tests/vetting investigations in order to issue or decline security clearance on any *"person or institution of national security interest"*. Thus far, there is every reason to believe that this provision will enable the state intelligence services, at their discretion, to conduct vetting investigations on: non-governmental organisations (NGOs) (including non-profit organisations, business entities, academic institutions and political parties/opponents) as well as Faith-based Organisations (FBOs) (including religious institutions, schools for religion, and churches).

There are several reasons underpinning this belief. They are set out below.

2.1 The wording of the first draft version of the Bill

The first factor substantiating the concern that NGOs and FBOs could be illegitimately targeted by the state intelligence services, relates to the wording of the first draft version of the Bill.

The first publicly available version of the Bill[84], which was made available by the Presidency to this organisation in July 2023, introduced the following provision:

> *"The functions of the Agency shall, subject to section 3 and in a prescribed manner, be to;*
>
> *(a) fulfil national counter-intelligence responsibilities and for this purpose to conduct and coordinate counter-intelligence and to gather, correlate, evaluate, analyse domestic intelligence in order to:*
>
> ...
>
> *(xi) conduct security competence test on categories of applicants and employees of organs of the State including persons who seek to establish and operate Non-Governmental Organizations, Churches or Religious Institutions , and Departments of Sate identified by the Minister and issue or decline to issue a security clearance certificate."*

84 General Intelligence Laws Amendment Bill 2022, also available at https://18a66295-3a0f-41fb-a13d-9849edd3b2a3.usrfiles.com/ugd/18a662_fdb5b053d2a749c7bf12c9eb1e5b3d04.pdf

In addition, the Bill introduced the following provision:

> *The relevant members of the National* ***[Security]*** *Intelligence Structures* ***[may]*** *must conduct a vetting investigation in the prescribed manner to determine the security competence of a person, if such a person—*
>
> *(a) falls within a prescribed category of persons who must have a security clearance in order to:*
>
> *i. be employed or render a particular service to an organ of state;*
>
> *ii. have access to classified information and intelligence in the possession of that organ of state; or*
>
> *iii. have access to areas designated as national key points or critical infrastructure areas in terms of the relevant law;*
>
> *iv. Seeks to establish and operate a Non-Governmental Organization or Religious institution;*
>
> *v. Seeks to establish a private security company in the Republic"*

Following the publication of this first version of the Bill, there was widespread criticism from the civil society and religious sectors.[85] While there were concerns about various aspects of the Bill, the above amendments pertaining to NGOs and FBOs were viewed as being particularly threatening to the continued functioning of non-profit and religious organisations. In addition, since the term 'non-governmental organisation' is not defined in South African law, this term could be taken to mean any entity that is not a government institution, including political parties, academic institutions, and think-tanks critical of the government of the day.

The intention of the intelligence services to conduct security vetting investigations into NGOs and FBOs were then confirmed publicly by the Minister in the Presidency responsible for state security, Khumbudzo Ntshavheni, when in September 2023 she informed the public that security

85 See Cosatu media statement, *"COSATU rejects the General Intelligence Laws Amendment Bill's shocking undermining of the Constitution". August 2023. A*vailable at https://mediadon.co.za/2023/08/17/cosatu-rejects-the-general-intelligence-laws-amendment-bills-shocking-undermining-of-the-constitution/ ; Civil society joint statement on the General Intelligence Laws Amendment Bill, 6 December 2023. Available at https://intelwatch.org.za/2023/12/06/endorse-gilab-statement/ ; Heidi Swart *"Democracy Down: Ramaphosa's proposed State Security vetting of NGOs an onslaught on SA's future".* 26 July 2023. Available at https://www.dailymaverick.co.za/article/2023-07-26-democracy-down-ramaphosas-proposed-state-security-vetting-of-ngos-is-onslaught-on-sas-future/

competence tests would be reserved for non-governmental organisations suspected of certain financial crimes. At the time, the Minister was quoted by the media outlet, Eyewitness News[86], as having said: "*We will subject those who pose [a risk] to national security interests."*

2.2 The wording of the current version of the Bill

The second factor substantiating the concern that NGOs and FBOs (in all their various manifestations) could be illegitimately targeted by state intelligence services, relates to the wording of the second (and current) version of the Bill, on which this submission is delivering comment.

Perhaps in response to the widespread criticism of the first draft version of the Bill, the current Bill saw the removal of explicit references to non-governmental orgnisations, churches and religious institutions. However, the Bill now makes provision for vetting investigations to determine the security competence of another broad category of entities, namely persons or institutions of national security interest.

The current version of the Bill provides the following definition of "*person or institution of national security interest"*:

> *'any person or institution, identified by the Agency in the form and manner prescribed, that conducts himself/herself or itself or engages in activities that are inconsistent with the principles set out in section 198 of the Constitution including any person or institution that engages in activities that are defined as a threat to national security in terms of this Act;'*

Since the definitions of *"national security"* and *"threat to national security"* are, as set out previously exceedingly broad, and given that section 198 of the Constitution does not provide clear criteria, but merely principles, the Bill in its current form does not sufficiently limit the state intelligence services from categorising a wide variety of institutions and persons as being of *"national security interest"*. This means that non-governmental organisations, religious organisations, churches, business sector entities, political opposition parties, academics and academic institutions (etc.) could be labelled by the intelligence services as being *"of national security interest",* even if they posed no threat to public safety or national interest.

The Bill then goes further and makes it an explicit function of the newly provided-for State Intelligence Agency to conduct security competence tests on such persons and institutions that are of national security interest. Thus, the National Strategic Intelligence Act of 1994 is amended by the Bill to include the following:

"The functions of the Agency shall, subject to section 3 and section 2(2)(B) and in a prescribed manner.

---

86 See Lindsay Dentlinger, "*No reason for Civil Society to Fear new Intelligence Bill*-Ntshavheni*"* EWN. 9 September 2023. Available at https://web.archive.org/web/20231127082757/https://ewn.co.za/2023/09/09/no-reason-for-civil-society-to-fear-new-intelligence-bill-ntshavheni

(a) be to fulfill national counter-intelligence responsibilities and for this

purpose to conduct and coordinate counter-intelligence and to gather, correlate, evaluate, analyse information regarding counter-intelligence and domestic intelligence in order to—

...

(xi) conduct security competence test on categories of persons or institutions referred to in section 2A of the Act in order to issue or decline to issue a security clearance certificate."

Accordingly, the Bill also provides for the following:

"(1) The relevant members of the National [Security] Intelligence Structures [may] must conduct a vetting investigation in the prescribed manner to determine the security competence of a person, if such a person—

(a) falls within a prescribed category of persons or institutions who must have a security clearance —

(i) in order to be employed or render a particular service to an organ of state;

(ii) in order to have access to classified information and intelligence in the possession of that organ of state;

(iii) in order to have access to areas designated as critical infrastructure areas in terms of the relevant law; or

(iv) if a person or institution of national security interest in terms of Section 4(2)(a)(i) of the Act"

Here, the Bill sows further confusion over the meaning of the words *"person or institution of national security interest"* and thus increasingly muddies the waters by allowing for a wider interpretation of who can be vetted: For one, this new provision does not refer to the Bill's newly proposed, equally vague, definition of *"person of national security interests"*. Secondly, the Bill amends section 2A of the National Strategic Intelligence Act of 1994 to include compulsory vetting investigations by the Agency of ***"a person or institution of national security interest <u>in terms of Section 4(2)(a)(i) of the Act</u>"****. (own emphasis)*

Section 4(2)(a)(i) of the National Strategic Intelligence Act of 1994 (as amended), reads as follows:

2. The functions of Nicoc shall be—

(a) to co-ordinate the intelligence supplied by the members of the National Intelligence Structures to Nicoc and interpret such intelligence for use by the State and the Cabinet for the

purposes of—

(i) the detection and identification of any threat or potential threat to the national security of the Republic

It seems that section 4(2)(a)(i) is in some manner meant to qualify the meaning of what constitutes a 'person or institution of national security interest' by placing it within the context of NICOC's functions. However, as the Bill stands, NICOC's role as it pertains to identifying and vetting persons or institutions of national security interest remains unclear. For instance:

What, if any, is NICOC's role in the initial identification of persons and institutions of national security interest?

What, if any, is NICOC's role in assessing or deciding whether or not a person or institution identified by the agency as being of national security interest is, in fact, of national security interest?

As the Bill currently stands, it creates an opportunity for state intelligence forces – be it members of the newly proposed Agency or of NICOC – to broadly interpret the meaning of *"person or institution of national security interest".* This, in turn, makes it possible to target virtually any person or organisation – including activists, academics, pastors, political opponents, businesses and protesters – for a vetting investigation.

2.3 The Financial Action Task Force's grey-listing of South Africa

There is a third factor indicating that the security competence testing/vetting investigation provisions in the Bill are in fact intended to target NGOs and FBOs, despite their explicit exclusion from this second version of the Bill. These factors relate to the role played by the State Security Agency in implementing, in South Africa, the international Financial Action Task Force's recommendations to combat money laundering and terrorisms financing. (The FATF is a watchdog body that sets international standards for in-country legislation to curb terrorism financing.)

In October 2021, the FATF published a report[87] following a mutual evaluation (conducted with the country) of South Africa's measures to stymie terrorism financing. A key finding included the country's weakened institutional capacity to address such crimes following State Capture. The report put forth recommended actions specific to South Africa to remedy the shortcomings.

However, South Africa was placed on a grey list early in 2023 because it failed to fully implement, within the period allotted by the FATF, all the recommendations that were prescribed following that body's evaluation of the country's laws, policies and institutions.

One of the recommendations that had not been satisfied during the first evaluation in 2021, dealt with strengthening laws that counter the abuse of non-profit organisations[88] to facilitate terrorism

87 Financial Action Task Force (FATF)"Anti-money laundering and counter-terrorist financing measures (South Africa): Mutual Evaluation Report" October 2021. Available at https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-South-Africa.pdf

88 See FATF recommendation 8, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-combating-abuse-non-profit-organisations.pdf

financing.

Following the release of the first version of the Bill, and the public criticism about provisions regarding vetting investigations of NGOs and FBOs, Minister in the Presidency responsible for State Security, Khumbudzo Ntshavheni, assured[89] civil society organisations that they did not need to fear the being vetted, and that the provisions to conduct vetting investigations on NGOs and religious organisations were necessary to remove South Africa from the grey list.

Arguably, the use of vetting investigations by intelligence services to address FATF concerns is excessive for two reasons:

2.3.1. New legislation in response to FATF recommendations has already been enacted

Firstly, to explicitly address the FATF grey-listing, South Africa enacted[90] two successive laws in 2022: The General Laws (Anti-money laundering and combating terrorism financing) Amendment Act 22 of 2022[91], and the Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Act 23 of 2022[92].

Taken together, these acts (22 and 23) have strengthened the investigative powers of the South African Police Services' Directorate for Priority Crime Investigation's (DPCI, or Hawks) and the Financial Intelligence Centre (FIC), in order to facilitate criminal investigations into of persons and organisations suspected of involvement in terrorism financing. In particular, Act 22 amends the 1997 Non-profit Act; organisations donating to entities outside South Africa and who provide "humanitarian, charitable, religious, educational or cultural services outside of the Republic's borders" must register with the Directorate of Non-profit Organisations within the Department of Social Development (DSD).

Registered non-profits (including churches) must now annually submit additional information (the exact nature of which will be determined in consultation with the FIC and the minister of finance) about their office bearers, control structures, management, and operations to the DSD.

Additionally, Act 22 introduces several criteria for the disqualification of NPO office bearers. Some of these include being an unrehabilitated insolvent and committing various offences governed by a slew of financial laws. Theft, fraud, forgery and perjury can all prohibit one from taking up a position on an organisation's board.

Despite these laws, the new Bill adds additional provisions amplifying the role of the state intelligence services in the fight against financial crimes by giving these services sweeping,

---

89 See Lindsay Dentlinger, *"No reason for Civil Society to Fear new Intelligence Bill*-Ntshavheni*"* EWN. 9 September 2023. Available at https://web.archive.org/web/20231127082757/https://ewn.co.za/2023/09/09/no-reason-for-civil-society-to-fear-new-intelligence-bill-ntshavheni

90 National Treasury of the Republic of South Africa. Media Statement. 6 January 2023. Available at https://www.treasury.gov.za/comm_media/press/2023/2023010601%20MEDIA%20STATEMENT-ENACTMENT%20OF%20KEY%20ANTI-MONEY%20LAUNDERING%20AND%20COMBATING%20OF%20TERROR%20FINANCING%20LAWS%20.pdf

91 General Laws (Anti-Money Laundering and combating Terrorism Financing) Amendment Act, 2022. Available at https://www.treasury.gov.za/public/47815%2029-12%20Anti-MoneyLaunderingAct22of2022.pdf

92 Protection of cOnstitutional Democracy against Terrorist and Related Activities Amendment Act, 2022 Available at https://www.treasury.gov.za/public/47803%202912%20ProtectionofConstiDemocracyagainstTerroristRelatedActivAmendmentAct%2023_2022.pdf

secretive powers that bypass the legislative processes that bind other responsible entities such as the Hawks and the FIC. This will be discussed in greater detail the section below.

2.3.2 Vetting investigations bypass the judicial process

Acts 22 and 23 alone do not preclude the SSA's involvement in terrorism financing investigations into NGOs and FBOs. It is, however, unusual and excessive to conduct vetting investigations for the purpose of addressing a crime defined in law (such as money laundering or terrorism financing).

A vetting investigation, on the other hand, is essentially a risk assessment that asks: Can a government employee on contractor be trusted to manage sensitive and classified state information, or are they likely to be blackmailed or bribed? Security clearance is then accordingly revoked or granted to a certain degree (depending the classification status of the information, as determined by the state's Minimum Information Security Standard)s.[93] Until now, vetting investigations by the State Security Agency have served this purpose, and this purpose is still provided for in the new Bill. This use of vetting is also the norm in democratic countries such as the United States and Great Britain.[94]

However, the Bill now also provides for the possibility of conducting vetting investigations into persons or institutions of national security interest. Given that it clearly is the intention of the state intelligence services to vet NGOs, FBOs and persons who may be in these organisations' service, it is apparent that the Bill repurposes vetting into a preemptive criminal investigative tool; normally, if an organisation or person is suspected of involvement in terrorism financing, money laundering, or any crime for that matter, state law enforcement would investigate it as a crime, with the relevant administrative and judicial protections – a case number, court orders, evidence preservation, court proceedings, witness statements, and so forth.

On the other hand, the security competence tests and vetting investigations proposed in the Bill would be a response to a potential threat to national security, as identified by the intelligence services. However, intelligence services can potentially classify all information related to their operations – including the reasons for a vetting investigation and information about the procedures and outcomes related to such an investigation. This creates an opportunity for the services to operate outside the constraints of the judicial system by removing, for the vetting subject, all statutory protections that a legal criminal investigation affords a person or organisation accused or suspected of criminal involvement.

2.4 Vetting and surveillance

The fourth factor motivating the concern that NGOs and FBOs could be illegitimately targeted by the intelligence services, relates to the nature of vetting investigations.

---

93 Minimum Information Security Standards. Available at https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf

94 See https://www.state.gov/security-clearances as well as https://www.gov.uk/government/publications/vetting-explained-and-our-vetting-charter/vetting-explained

Vetting is a highly invasive process that disregards the right to privacy. This is made clear by the current definition of 'vetting investigation' as it stands in the National Strategic Intelligence Act of 1994 (as amended). Section 2A provides for the following:

(4) (a) In performing the vetting investigation contemplated in subsection (1), the relevant members of the National Intelligence Structures may use a polygraph to determine the reliability of information gathered during the investigation.

[Para. (a) substituted by s. 3 (d) of Act No. 11 of 2013.]

*(b) For the purpose of this section, "**polygraph**" means an instrument used to ascertain, confirm or examine in a scientific manner the truthfulness of a statement made by a person.*

(5) The relevant members of the National Intelligence Structures may, in the prescribed manner, gather information relating to—

1. *(a) criminal records;*
2. *(b) financial records;*
3. *(c) personal information; or*
4. *(d) any other information which is relevant to determine the security clearance of a person:*

Provided that where the gathering of information contemplated in paragraphs (c) and (d) requires the interception and monitoring of the communication of such a person, the relevant members shall perform this function in accordance with the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002)."

Thus, the Bill could allow the intelligence services to, under the ruse of a security competence test/vetting investigation, conduct surveillance of communications and access to all personal and organisational records (with no obligation on the intelligence services to notify the vetting subject about the data and information unearthed through these investigative activities).

Compulsory vetting could therefore, in practice, result in a surveillance operation (which could include the interception of communications and the entry of private property and cyberspace to gain access to information) for which the intelligence services would not need a warrant from the court; the vetting subject, be it a person or organisation, would be forced to comply. A vetting investigation would therefore present a way for intelligence services to circumvent the provisions of the Regulation of Interception of Communications and Provision of Communications-related Information Act of (2002) (as amended) (RICA). This is particularly concerning, given the fact that the Department of Justice in 2023 amended RICA to remedy several portions of the act which were struck down by the Constitutional Court (see *National Communication Centre and Bulk Surveillance* below).

2.5 Consequences of failing a security competence test

The fifth factor motivating the concern that NGOs and FBOs could be illegitimately targeted by the intelligence services, relates to the potential consequences of failing a security competence test.

The Bill currently does not clarify what the consequences of failing a security competence test will hold for a person or institution subjected such a test. The Bill simply states that, following a security competence test, intelligence services can *"issue or decline to issue a security clearance certificate."* It is therefore unclear if such an entity would be forced to cease or limit their work or operations. Once again, there is room for a very broad interpretation by the intelligence services, creating the risk of abuse.

2.6 ANC and SSA's past treatment of NGOs and political opposition

The sixth factor underlying the concern that NGOs and FBOs could be illegitimately targeted by the state intelligence services, relates to the ANC and SSA's past treatment of and references to NGOs and even other political parties and movements. Within the context of the African National Congress' past and recent tendencies to view non-governmental organisations and related role players as potential foreign agents aiming to instigate dissent, it is not unreasonable to question whether the ruling party opted for the inclusion of these vetting provisions in order to gain leverage over organisations and individuals who are critical of their policies and programmes.[95] This is particularly concerning given the fact that this Bill is being pushed through parliament prior to 2024 elections, during which the ANC is projected by some observers to suffer an unprecedented defeat.

In addition, the emergence of the State Security Agency's so-called 'Boast Report' during the inquiry of the Judicial Commission on State Capture into the SSA, revealed a number of operations undertaken by the SSA to serve the political ends of former President Jacob Zuma, including the targeting of political movements and non-governmental organisations[96]:

> *"The report was read into the record It is lengthy and detailed It shows, amongst others, that there was an operation to impede the distribution of the CR17 regalia, the transportation from Gauging of groups apparently supportive of the CR17 campaign; to ensure cancellation of the President's visit to America; infiltration of the Zuma Must Fall campaign; dissemination of misinformation to supporters of the campaign; initiation of media campaigns; generally infiltration of groups considered hostile; infiltration of trade unions which resulted in minimal support for those campaigns, active monitoring of some NGO's such as the South Africa First, Right to Know, CASAC and Green Peace. The document was boasting of the above "achievements", hence it was referred to by witnesses as the "Boast Report". – Justice R.M.M. Zondo, Chief Justice of the Republic of South*

95 See Jane Duncan, "*Why South Africans should be worried by ANC talk of a 'colour revolution' "*The Conversation. 14 November 2017. Available at https://theconversation.com/why-south-africans-should-be-worried-by-anc-talk-of-a-colour-revolution-87019 ; Ranjeni Munusami *"Mr Bombastic: Kebby Maphatsoe's top-secret guide to political relevance'.* The Daily Maverick. 10 September 2014. Available at **https://www.dailymaverick.co.za/article/2014-09-10-mr-bombastic-kebby-maphatsoes-top-secret-guide-to-political-relevance/** and more recently Christen Engel,"*Mantashe has NGOs in crosshairs (again) and wants them to declare their funding sources'"*11 October 2023, available at **https://www.dailymaverick.co.za/article/2023-10-11-mantashe-has-ngos-in-crosshairs-again-and-wants-them-to-declare-their-funding-sources/**

96 See Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector Including Organs of State Report: Part V Vol. 1: State Security Agency, and Crime Intelligence, para 770 pp293-294.

Africa.

The ANC and the SSA have a history of contempt and disrespect for the NGO sector's legitimate opposition to failed policies. Given this history, the Bill's security competence testing/vetting investigation provisions are highly concerning, as the ANC and the SSA have by no means proven that they can be trusted with such powers. However, should the ANC lose its majority, there is still absolutely no guarantee that a new government would not abuse the Bill's new vetting provisions. This is a systemic issue that the Bill must rectify.

The vetting provisions currently envisaged by the Bill is reminiscent of legislation found in authoritarian states, such as Russia and China, and have absolutely no place in our young democracy.

2.7 Conclusion:

Combined, all of the above-mentioned concerns give rise to serious questions as to whether or not the Bill, once enacted, can and will be abused by intelligence services in order to oppress dissent and stifle protest actions against the government of the day.

2.8 Recommendations

(a) Any and all provisions and references relating to security competence testing of persons or institutions of national security interests must be removed from the Bill. Vetting investigations and security competence tests should only pertain to prospective or current state employees or contractors who require security clearance due to the fact that their work for the state gives them access to sensitive state information and systems.

(b) As such, the definition of *"person or institution of national security interest"* must be removed in its entirety and the wording *"or is a person or institution of national security interest in terms of Section 4(2)(a)(i) of the Act"* must be removed from the definition of *"security competence test"*.

3. Provisions relating to the National Communications Centre

In February 2021[97], Constitutional Court ruled that *"the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre"* (NCC) were *"unlawful and invalid"*. The Constitutional Court consequently ordered the NCC to cease interception and surveillance operations.

To address this, the Bill makes certain provisions regarding the NCC that are particularly relevant to this submission. They include the following:

97 See AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) Available at https://www.saflii.org/za/cases/ZACC/2021/3.html

"2B(1) The Centre shall, in a prescribed manner, and with regard to

foreign signals, communications and non-communications—
(a) gather, correlate, evaluate and analyse relevant intelligence in order

to identify any threat or potential threat to national security subject to—

(i) submission of bulk interception application in the form and manner, as prescribed for approval by a retired Judge appointed by the President, after consultation with the Chief Justice;

(ii) two advisory interception experts appointed by the Minister based on his or her relevant qualifications and experience in the field; and

(iii) the Centre supplying relevant intelligence to the national intelligence structures.

(2)(b) In a prescribed manner, and with regard to information security and cryptography, the Centre shall—

(i) identify and secure national critical information infrastructures
and protect intelligence from unauthorised access, disclosure, technical and related threats;

(ii) provide verification services for electronic communications security products used by organs of state;

(iii) provide and coordinate research and development with regard to electronic communications, products and any other related services;

(iv) support secure electronic communications solutions to identified Organs of State; and

(v) coordinate cybersecurity activities in order to identify and impede any cyber enabled threats"

Although the Bill, in an apparent attempt to heed the Constitutional Court's order, establishes the NCC and its powers of bulk surveillance in law, it does little to protect the public from potential abuses and extra-legal surveillance.

The Bill's current provisions pertaining to mass signals surveillance and the NCC could allow state intelligence services to monitor, en masse, the communications of every South African, and to do so behind a veil of secrecy in the name of national security.

There are a number of factors contributing to this risk of unfettered mass surveillance of the South African people. These will be set out below.

3.1 Capabilities of National Communications Centre

The first such factor relates to capabilities for the NCC.

The NCC – which is responsible for foreign signals interception – monitors vast volumes of private communication signals without obtaining warrants from a court. Although the NCC is purportedly only meant to target foreign communication signals (in other words, signals that do not originate or terminate within the borders of South Africa) the NCC has the ability to monitor such signals as well as those communications signals that travel outside the borders of the country. Persons

inside South Africa are not spared from being caught in the NCC's surveillance dragnet. This is because the structure and function of the internet and digital, online communications necessitates the transmission of communication signals across borders (even if those communicating are in the same country).

Generally speaking, the aim of bulk surveillance is to enable the state to monitor, collect, retain and analyse vast quantities of communications and signals data. The idea is to allow state intelligence services to locate threats that it would otherwise not have detected, or to investigate a threat or crime retrospectively by examining signals and communications that were intercepted over any number of years. This is possible because advanced algorithms allow keyword searches in order to sift relevant information from masses of stored data. Keywords can also be used to scan communications in real time in order to detect threats, and communications monitoring over the long-term can also be used (in theory, at least) to supposedly predict crime. [98]

Another alarming aspect about the type of bulk surveillance that the NCC conducts, is that it can take place without technical assistance – and therefore without the knowledge – of the service provider (for instance, MTN or Vodacom). In other words, it gives the state secret, direct access to private communications; judges, mobile operators and internet service providers have no way of knowing that bulk interception is occurring. This is due to certain technical aspects relating to how bulk surveillance systems function.

Such 'direct access' surveillance practices are extremely vulnerable to abuse, as was acknowledged by the European Court of Human Rights in its comments[99] on the Russian interception system, Sorm (Systema Operativno-Raziskhikh Meropriatiy – the System of Operative-Search Measures on Communications). Sorm is operated by Russia's Federal Security Service. (In Russian, the Federalnaya Sluzhba Bezopasnosti, or FSB. Its Cold War predecessor was the Komitet Gosudarstvennoy Bezopasnosti, or KGB).

The court stated:[100]

"…the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great."

98 Heidi Swart, "*Say nothing, the spooks are listening*" Mail&Guardian. 17 December 2015. Available at https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening/ See also Heidi Swart "Communications Surveillance by the South African Intelligence Services" Media Policy and Democracy Project. February 2016. Available at https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf

99 See European Court of Human Rights. *"Fact Sheet: Mass Surveillance" Available at* https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng and Presentation by Andrei Soldatov, "R*ussia's communications interception practices (SORM).* 22 January 2014. Available at https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/soldatov_presentation_/soldatov_presentation_en.pdf

100 European Court of Human Rights. *Roman Zakharov v. RUSSIA* Available at https://hudoc.echr.coe.int/eng#%7B%22fulltext%22:[%22zakharov%22],%22documentcollectionid2%22:[%22GRA%20NDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-159324%22]%7D

3.2 Past lack of transparency and independent oversight is not addressed

The second factor underscoring the risk of unfettered mass surveillance through the NCC, is the fact that the Centre has a history of non-transparency and routine non-compliance with interception legislation, and its interception facilities are known to have been abused. The Bill does little to address this.

The management and oversight of interception processes within the NCC have always been kept secret. The public has never been told what factors constitute grounds for mass interception or what the legal authorisation requirements for mass interception are. There is also the issue of refining data until a specific person or group of people can be identified to conduct targeted interception. It is unclear what checks and balances are in place to prevent the misuse of such targeted interception capabilities at the NCC.

This lack of transparency could very well have contributed to the misuse[101] of the NCC's facilities when the voice communications of at least 13 people within the borders of South Africa were intercepted back in the mid-2000s in what came to be known as the "hoax email saga". Those targeted for surveillance included members of the ruling and opposition parties, business persons and public officials. This targeted interception was carried out despite the NCC's official mandate to intercept only communications that occur outside the country's borders.

A lack of transparency and adherence to interception legislation dates back to the early days of the NCC; it was established circa 2002, and in 2008 the Ministerial Review Commission on Intelligence (the Matthews Commission) found that it was operating in contravention of the Regulation of Interception and Provision of Communications-related Information Act of 2002 (RICA).[102]

The Matthews Commission made a number of recommendations[103] to remedy state of affairs it had discovered at the NCC. (These recommendations pertained the National Strategic Intelligence Bill, which at the time was envisioned to make provisions for the NCC and its operations and functions. These provisions never materialised, and the recommendations were never implemented).

The current Bill makes virtually no attempt to implement the Matthews Commission's recommendations, and in certain instances even directly opposes said recommendations. This will be expanded upon below:

Recommendation 1:

> *"The National Strategic Intelligence Amendment Bill, which provides for the functions of the NCC, should state that the NCC is bound by RICA. It should also stipulate that the NCC may not intercept the communication of a targeted person unless it has obtained an interception direction issued by the designated judge as provided for in RICA."*

Not only is the current Bill not bound by Rica – it creates a parallel process whereby state

101 OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE *"EXECUTIVE SUMMARY OF THE FINAL REPORT ON THE FINDINGS OF AN INVESTIGATION INTO THE LEGALITY OF THE SURVEILLANCE OPERATIONS CARRIED OUT BY THE NIA ON MR S MACOZOMA"* MEDIA BRIEFING. 23 MARCH 2006. Available at https://www.gov.za/sites/default/files/gcis_document/201409/igreport0.pdf

102 Final Report of the Ministerial Review Commission on Intelligence, 10 September 2008, available at https://www.r2k.org.za/wp-content/uploads/Matthews-Commission-Report-10-Sept-2008.doc

103 Ibid. pp 202 -203

interception of private communications can occur that falls outside of processes regulated by RICA This is particularly concerning given the February 2021 Constitutional Court ruling[104] that vast sections of RICA were unconstitutional, and had to be rewritten. (Rica was accordingly amended in 2023). The Constitutional Court required the Department of Justice to amend RICA to achieve the following:

> *"(a) provide for safeguards to ensure that a Judge designated in terms of section 1 is sufficiently independent;*
>
> *(b) provide for notifying the subject of surveillance of the fact of her or his surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated;*
>
> *(c) adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte;*
>
> *(d) adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data; and*
>
> *(e) provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist."*

The Bill achieves none of the above. The section of the ConCourt order for which it shows some semblance of acknowledgement, is the oversight aspect. However, the Bill fails to provide independent oversight: To oversee the NCC's work, a judge responsible for issuing interception warrants will be appointed by the president. To aid the NCC judge, two bulk interception experts will be appointed by the minister in charge of intelligence. (The Bill does not define the term "bulk interception expert".) In essence then, the president and the minister will control who oversees interception via the NCC, thus making no provision for judicial independence.

While the memorandum to the Bill does state that the retired judge shall be recommended by the Judicial Services Commission/Minister of Justice and appointed by the President, it is not at all clear that these recommendations are binding. Notably, the NCC judge will be appointed in addition to and separately from the judge appointed to issue interception directions in terms of RICA. Thus, a separate, parallel process to seek interception directions will be available exclusively to the intelligence services.

Recommendation 2:

> *"The Bill should indicate which intelligence, security and law enforcement bodies are entitled to apply to the NCC for assistance with the interception of communication; it should specify the grounds that can be invoked by each of these bodies; and it should*

104 See AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) Available at https://www.saflii.org/za/cases/ZACC/2021/3.html

describe the information that must be contained in an application for signals monitoring."

The Bill does provide for the NCC to *"supplying relevant intelligence to the national intelligence structures"*. The Bill lists five national intelligence structures: NICOC, Defense Intelligence, the South African Police Services' crime intelligence division, the South African Intelligence Agency and the South African Intelligence Services. However, apart from this aspect, this recommendation is largely ignored.

Recommendation 3:

"The Bill should not allow for the interception of communication on the grounds of protecting and advancing international relations and the economic well-being of the Republic or on the grounds of supporting the prevention and detection of regional and global hazards and disasters. As proposed in Chapter 7, intrusive measures such as interception of communication should be limited to situations where there are reasonable grounds to believe that a serious criminal offence has been, is being or is likely to be committed."

This recommendation is not implemented; on the contrary, the Bill simply states that the NCC shall "*gather, correlate, evaluate and analyse relevant intelligence in order to identify any threat or potential threat to national security subject". From t*he use of the words *"identify"* and "threat or potential threat" , it is apparent that a reasonable suspicion of criminal activity is not a prerequisite for a bulk interception application.

Recommendation 4:

"The Bill should indicate whether the NCC can, on its own initiative, identify targets for signals monitoring or whether it can only monitor the targets identified by another intelligence service or a law enforcement body."

As the Bill stands, there is no indication whether or not the NCC is limited in its actions to intelligence applications from other intelligence structures.

Recommendation 5:

"The Bill should provide that interception of communication is a method of last resort that can only take place if non-intrusive methods are inadequate or inappropriate."

This recommendation is not implemented.

Recommendation 6:

"The Bill should provide for the discarding of personal information that is acquired in the course of intercepting communication where the information is unrelated to the commission of a serious criminal offence."

AND

Recommendation 7:

> *"The legislation should also cover the NCC's 'environmental scanning', which entails random monitoring of signals. It is not possible to obtain prior judicial authorisation for this kind of monitoring since there are no known targets. Where random monitoring identifies the need to focus on a specific person or organisation, however, then the requirements of ministerial approval and judicial authorisation should apply."*

Recommendations six and seven are related in the sense that they pertain to the regulation of different stages of bulk interception. Neither of these recommendations are adequately implemented by the Bill, and the Bill is largely silent on the management of information and how data is collected, stored and analysed by the NCC.

This is concerning, since the processes involved in bulk surveillance are complex and require regulating at the various phases of interception. For instance[105], first, communications and call record data are intercepted (collected); second, this information is filtered; third, the information identified through the filtering is investigated further. Analysis through artificial intelligence (AI) is usually needed, given the massive amounts of data.

These processes give rise to several issues in terms of personal privacy: What keywords are utilised to search through collected data and how are keyword searches authorised, if at all? Is it really necessary to collect so much data? What role does artificial intelligence and algorithms play in analysing mass data sets, and how are these regulated to prevent errors and bias? The Bill does nothing to address these issues.

Recommendation 8:

> *"The intelligence organisations should take immediate steps to ensure that their policies and procedures on the interception of communication provide for ministerial approval and judicial authorisation and are in alignment with the Constitution and legislation. The Minister should set a deadline by which this is to be done and should request the Inspector-General of Intelligence to certify the revised policies and procedures in terms of their alignment with the Constitution and the law."*

This recommendation, as well as the Protection of Information Act, and the ConCourt's orders pertaining to RICA are ignored by the Bill.

3.3 Other issues:

3.3.1 The meaning of signals intelligence today

Today, communications signals includes much more than simply verbal or written conversations that are transmitted via the internet in the form of electronic signals. We live in an era in which the metadata – data about communications and online activities (such as web browsing, subscribing to

105 SEE Privacy International, *"How Bulk Interception Works".* September 2016. Available at https://medium.com/privacy-international/how-bulk-interception-works-d645440ff6bd

online services, social media activities, banking, completing online surveys, etc.) – is generated in vast amounts on a scale unprecedented in history. Just as location and call data records reveal much about a persons whereabouts, associations and activities, so does data generated by what is known as Internet-of-things devices (IoTs). These so-called 'smart devices' usually can be linked to and monitored or controlled with smart phones or computers, and they generate data that can intimately track a person's daily life, beliefs, sexual orientation, whereabouts (on a micro-scale), purchases, and preferences (to name a few). The data thus generated is increasingly being used by law enforcement in the United States during criminal investigations. The collection and analysis of such data through bulk interception is a gross violation of privacy, yet the Bill's provisions are silent on this aspect. [106]

This is again an illustration of the failure to implement the Matthews Commission's recommendations that the NCC's operations should adhere to RICA.

3.3.2 The housing of the NCC within the domestic branch of the Intelligence Services

In locating the NCC within the domestic branch of the Intelligence Services, the Bill completely ignores the HLRP's recommended that the NCC be located within the foreign intelligence branch. [107] The latter makes sense, since the NCC should only be concerned with foreign signals interception, which does not fall within the mandate of domestic intelligence.

3.3.3 Listed equipment

The Bill currently states that one of the functions of the NCC is to "*provide and coordinate research and development with regard to electronic communications, products and any other related services"*.

This provision could potentially relate to what is defined in RICA as 'listed equipment' [108] (such as the so called grabber – a device that can be used in field operations to capture mobile phone conversations and track phone users).

There is no indication in the Bill that the intelligence services will be legally compelled to adhere to RICA in this regard.

3.3.4 Cybersecurity coordination

The Bill provides for the NCC to coordinate national cybersecurity matters. It states that one of the NCC's functions is to *"coordinate cybersecurity activities in order to identify and impede any cyber enabled threats".*

The NCC has a history of operating in secret, and of not publishing known cyber threats and incidents related to government organisations and infrastructure. For instance, during 2021 cyber attack on Transnet, there was a major stoppage of services in the Durban harbour.[109] The State

106 Heidi Swart *"5G opens the Gates for Surveillance on Steroids"* The Daily Maverick. Available at https://www.dailymaverick.co.za/article/2021-04-06-5g-opens-the-gates-for-surveillance-on-steroids/

107 HLRP report, p 31 and para 5.5(b) p32

108 Heidi Swart *"State surveillance in SA just got a legal boost, but it's not an unrestricted licence to intercept"* 30 May 2023. The Daily Maverick. Available at https://www.dailymaverick.co.za/article/2023-05-30-state-surveillance-in-sa-just-got-a-legal-boost-but-its-not-an-unrestricted-licence-to-intercept/

109 Toby Shapshak. *"Note to Transnet: Cyberattacks only work when there are vulnerabilities to exploit"* The Daily Maverick. 4 August 2021. Available at https://www.dailymaverick.co.za/opinionista/2021-08-04-transnet-ports-closed-and-were-in-the-dark/

Security Agency did not make public any investigation (if there was one) of this incident. This is out of step with international best practice.

For instance, in December 2020[110]Christopher Krebbs, then head of the United States Cybersecurity and Infrastructure Security Agency, took responsibility for a massive security breach of US government systems. Details about the attack were made public, and widely published in the media. It is also customary, across the world, for both government (at least democratic ones) and corporate entities to reveal cyber vulnerabilities and security breaches within their systems and products, in order to allow the public and various affected sectors to secure their systems as a matter of urgency.[111]

As the Bill now stands, there is no obligation on the intelligence services to fulfill this role.

3.4 Recommendations

(a) The Matthews Commission's recommendations must be implemented through the Bill. The Bill must also set limitations on the use, management, collection, storage and analysis of signals, communications, and metadata in all its forms.

(b) It is preferable that the designated RICA judge also oversees interception applications to the NCC. If this is not possible, the judge overseeing the NCC should be housed in the DOJ. This will further the independence of NCC oversight, and shield it from interference from the intelligence services and the executive.

(c) The HLRP recommended that the NCC we located within the foreign intelligence branch. This recommendation should be implemented with urgency.

(d) Listed equipment development by the intelligence services must be subject to RICA regulations on listed equipment.

(e) Cyber coordination cannot occur in secret. The Bill must provide for an obligation on the NCC to make information on security threats and breaches public as soon as it becomes available to them, including breaches of government systems and the results of investigations on breaches of these systems.

3.5 Additional Recommendations and information

For Intelwatch's additional recommendations concerning bulk surveillance, please see: ANNEXURE 1: 'The Future of Bulk Interception and digital communication: Issues and policy options' (2024)

110 Inyoung Choi *"Former US cybersecurity chief Chris Krebs says officials are still tracking 'scope' of the SolarWinds hack"*. Business Insider. 20 December 2020. Available at https://www.businessinsider.com/krebs-solarwinds-cybersecurity-hack-more-broad-2020-12

111 See for instance https://www.cvedetails.com

4. Oversight: The Inspector General of Intelligence (IGI), the Joint Standing Committee on Intelligence (JSCI), the Auditor-General (AG), investigative bodies external to the intelligence community, and the courts

The role of intelligence oversight cannot be discussed without examining the inextricable links between the three main oversight bodies, namely the IGI, the JSCI and the AG. The role of investigative bodies external to the intelligence community, such as the South African Police Service (SAPS) and the National Prosecuting Authority (NPA) must also be taken into account.

Our analysis and recommendations will therefore be based on a view that takes into account how the legal limitations placed upon the JSCI, IG, and AG impact the dynamics between them in such as way as to render oversight ineffective. We will also look at the problems plaguing each individual entity, and make recommendations to remedy the issues. While doing this, we will take into account the crucial roles of investigative bodies external to the intelligence community as well as the courts in bringing members of the intelligence community to book when they break the law.

The Bill does not provide sufficiently for the independence and powers of the IG, JSCI and AG. This is despite the findings of the 2018 HLRP and the State Capture Commission that both the JSCI and the IGI, for various reasons, failed to provide sufficient oversight, and despite years of qualified audits from the AG.

Currently, the legislation is such that the IG in particular lacks the independence required to truly bring intelligence community members to book when they commit transgressions. The JSCI and AG's shortcomings have greatly exacerbated this situation.

Factors that contribute to the malfunctioning of and malfeasance in South Africa's intelligence community *must* be addressed by the Bill. These factors are dealt with below, with accompanying recommendations.

4.1 The risks of a partisan JSCI

The State Capture Commission found that the Joint Standing Committee on Intelligence (JSCI) was largely ineffective during the state capture years, and that their lack of efficacy could even directly have contributed to state capture.[112] In fact, it was apparent from the testimony before the Commission of the former IG, Setlhomamaru Dintwe, that the JSCI was the place where the IG's recommendations went to die. Other major issues with the JSCI have included repeatedly publishing late reports, and leaving the seat of the IGI vacant for protracted periods.

Just what went wrong with the committee during this time is difficult to ascertain, since little is known about its functioning and decision-making. Much of this is due to restrictions placed on it in terms of secrecy and classification of information by the intelligence services and entities: the committee has never met in public, and is restricted in which of its findings it can make public.[113]

112 See HLRP Report para 13.3.3 pp 95-96 AND para 13.4.3 at p. 97; Judicial Commission of Inquiry into State Capture Report Part 5 Vol 1 para 913 - 916 at pp. 345-346.

113 Sandy Africa "*Financial Oversight of the Civilian Intelligence Services in South Africa",* Strategic Review for Southern Africa, Vol 41, No 2, *December 2019, pp* 8 – 9 , available at

However, what is known to the public, is that the High Level Review Panel of 2018 found that the JSCI was not immune to political interference; as early as 2005, after the IG had found concrete evidence of wrong-doing during the so-called email hoax saga (where technology at the NCC was abused), the JSCI, along with the ANC, questioned the IG's report.[114]

The impact of the ANC's parliamentary representatives voting along party lines was illustrated in 2016 when parliament held a vote to impeach then-president Jacob Zuma over the Nkandla matter. The ANC quashed the motion (which was brought by the opposition)[115]. Evidence and testimonies in the State Capture Commission have since revealed Mr Zuma to be a primary machinator and benefactor of state capture. Coincidentally, during much of Mr Zuma's tenure, Mr Cecil Burgess – a staunch supporter of Mr Zuma and dubbed in the media as the 'champion' of the highly controversial and draconian Protection of State Information Bill – chaired the JSCI.[116] Later, the ANC's preferred candidate for IG was Mr Burgess, which outraged the opposition. Mr Burgess' appointment ultimately failed due to parliamentary opposition.[117]

As it currently stands, the JSCI consists of a majority of representatives of the ruling ANC party (this includes the chair of the JSCI). According to parliament's website[118], eight out of 13 JSCI members are from the ANC, three are from the Democratic Alliance, one is from the Economic Freedom Fighters, and one from Al Jama-ah. Of these members, three are members of the National Council of Provinces (NCOP), and the remainder are in the National Assembly (NA). Two of the three NCOP members are ANC representatives.

This means that the ANC holds the majority in terms of both houses of parliament – the NCOP and the NA – within the JSCI. As a result, members of the ANC can ultimately determine the outcomes of committee decisions and which recommendations to make regarding the services and entities, and can decide whether or not to support and ultimately pursue the recommendations of the IG.[119]

There is little reason to trust that ANC members of the JSCI will not heed party lines when it comes time for the committee to vote on intelligence matters that may have, from the ANC's perspective, adverse consequences for that party, or that may result in less favourable political conditions for the party. In fact, the very state of the current Bill to which this submission pertains, does nothing to inspire further trust in the ANC and its members on the JSCI.

Our criticism here of the JSCI is not of the type unique to South Africa or the ANC. For instance, the United Kingdom also uses a parliamentary oversight model[120]; oversight of intelligence services (including signals interception) are conducted by the Intelligence and Security Committee (ISC).

---

https://upjournals.up.ac.za/index.php/strategic_review/article/download/305/252/1268

114 See HLRP Report para 9.3.1 p63.

115 BBC *"South Africa's Jacob Zuma survives Nkandla impeachment vote"* 5 April 2016, available at https://www.bbc.com/news/world-africa-35966916

116 News 24 "Secrecy Bill 'champion' Cecil Burgess cracks nod for top spy job" 15 June 2015, available at https://www.polity.org.za/article/secrecy-bill-champion-cecil-burgess-cracks-nod-for-top-spy-job-2015-06-19

117 Marianne Merten "*The ANC abandons Cecil Burgess as candidate for Inspector-General of Intelligence"* 16 March 2016 available at https://www.dailymaverick.co.za/article/2016-03-16-the-anc-abandons-cecil-burgess-as-candidate-for-inspector-general-of-intelligence/

118 See Parliament of the Republic of South Africa, Joint Standing Committee on Intelligence, as at 5 February 2024 at https://www.parliament.gov.za/committee-details/169

119 See Joint Rules of Parliament 24 (a) and (b) pp 16 – 17 available at https://www.parliament.gov.za/storage/app/media/JointRules/joint-rules-a51.pdf

120 Government of the United Kingdom *"The National Intelligence Machinery"* 2010, available at https://assets.publishing.service.gov.uk/media/5a78ee84ed915d07d35b38e9/nim-november2010.pdf

The ISC was established in 1994 through the Intelligence Services Act. Concerns arose as to the ISC's independence: Although its nine members consisted of representatives from different political parties, these representatives were appointed by the Prime Minister (PM), as was the chair of the ISC. The ISC also reported directly to the PM, and what the ISC ultimately reported in the public domain was determined by the PM.[121]

With the ANC majority in the JSCI, and with the location of the State Security Agency in the Presidency (currently also occupied by an ANC member), it is not difficult to see how the president could directly influence the work of the JSCI by instructing ANC members on the committee on how to vote. (The dangers of having South Africa's intelligence services and entities located in a president's office have been clearly elucidated upon by astute analysts.[122]) Thus, even if the model upon which the UK ISC's functioning was originally based technically differs to South Africa's current parliamentary oversight model, the potential results are the same: in both models, the leader of the country could potentially serve the purposes of their political party by quashing the findings and recommendations of the intelligence oversight committees.

An attempt to remedy the lack of independence of the ISC was made through the 2013 Justice and Security Act. For instance, one of the safeguards introduced by the Act provides for the PM to nominate ISC members, but the list of names from each house of parliament has to be approved by the relevant house. The PM also cannot simply remove a committee member – only a resolution from the relevant House can achieve that.

These and other potential solutions to promote the ISC's independence are not failsafe, nor are they necessarily relevant to the JSCI's circumstances. There has also been controversy surrounding the ISC's effectiveness since the introduction of the 2013 act. In other words, carbon-copying another country's legislative practices are not necessarily the answer to South Africa's oversight issues.

However, the introduction of such legislative safeguards as seen in the United Kingdom does illustrate that it is not beyond the capacity of lawmakers to introduce mechanisms to promote an oversight committee's non-partisan nature and independence from the president's office (and by extension insulating the committee from interference by the ruling party).[123]

Currently, the composition[124] of the JSCI is prescribed by section 2(2)(a) of the Intelligence Service Oversight Act 40 of 1994. It reads as follows:

> (2) *(a)* The Committee shall consist of 15 members of Parliament appointed on the basis of proportional representation determined according to the formula in paragraph *(c)*: Provided that –

121 Dominic Grieve *"The Intelligence and Security Committee and its role in democratic accountability"* The Constitution Unit 24 July 2020, available at https://constitution-unit.com/2020/07/24/the-intelligence-and-security-committee-and-democratic-accountability/

122 See for instance Marianne Merten "South Africa a step closer to a super Presidency after Ramaphosa's master class in consolidating power" The Daily Maverick 9 August 2021, available at https://www.dailymaverick.co.za/article/2021-08-09-south-africa-a-step-closer-to-a-super-presidency-after-ramaphosas-master-class-in-consolidating-power/

123 Dominic Grieve *"The Intelligence and Security Committee and its role in democratic accountability"* The Constitution Unit. 24 July 2020. Available at https://constitution-unit.com/2020/07/24/the-intelligence-and-security-committee-and-democratic-accountability/

124 Intelligence Services Oversight Act 40 of 1994, Section 2.

(i) if the total number of seats on the Committee allocated to the political parties in terms of paragraph *(c)* is less than 15, the unfilled seats shall not be allocated to any political party, but the Committee shall nevertheless be deemed to be properly constituted; and

(ii) if one political party has been allocated more than eight seats in terms of paragraph *(c)* and more than five political parties are represented in Parliament, the five minority parties with the largest representation in Parliament are entitled to at least one member each on the Committee, and the Committee so constituted shall be deemed to be properly constituted regardless of whether the total number of seats so allocated on the Committee is more or less than 15; and

(iii) if any political party is unwilling to serve or to continue to serve on the Committee, the seats of such political party on the Committee shall not be allocated to any other political party but the Committee shall nevertheless be deemed to be properly constituted.

It is clear that the current law significantly lessens the probability that the majority party's members on the JSCI could be challenged by a unified opposition. It also increases the likelihood that the majority party will hold the majority within the JSCI, thus securing decision-making powers. If this situation persists, the public cannot be guaranteed that the JSCI will not act in the interest of the ruling majority party before it acts in the interest of the nation and its people. Crucially, the same holds true ***for any other party*** that may hold the majority.

Recommendation

Possible solutions to ensure non-partisanship in the JSCI can be borrowed from elsewhere. For instance, the Dutch oversight model calls for six parliamentarians, to serve on the parliamentary intelligence oversight committee, and none of these parties hold a majority on that committee.[125]

This would require the Bill to explicitly amend section 2 of the Intelligence Oversight Act, as well as to make adjustments to the Joint Rules of Parliament (specifically in terms of sections 19; 20 and 27) to provide for special circumstances pertaining to the JSCI. New rules could stipulate that no party may hold the voting majority on the JSCI, that the JSCI may only continue with business if the committee is quorate, and that the members of the JSCI must be approved by greater parliament, as is the case with the IG. The new Bill should be amended to compel the establishment of these mechanisms.

125 See annexure 2: Vicky Heideman *"Secret Funding and the State Security Agency: Holding Intelligence Services Accountable (Recommended changes to funding and accountability mechanisms for South Africa's state intelligence services based on international trends)"* par 77 p17 Intelwatch and the Media Policy and Democracy Project. June 2023. Available at https://intelwatch.org.za/wp-content/uploads/2023/07/Report-Secret-Funding-SSA-accountability-2023.pdf

4.2 Powers and capacity of the JSCI

The Joint Standing Committee on Intelligence ("JSCI") currently provides oversight in that the budgets and financial reports for the intelligence services and entities are reviewed by them. However, as pointed out by the Matthews Commission, the documents themselves are confidential and are not presented to parliament. Therefore, "according to the National Treasury, the intelligence services are not directly accountable to Parliament for their budgets and spending".[126]

Furthermore, the JSCI receives annual reports from the IGI as well as the designated RICA judge, and certificates from the IGI. The committee then makes recommendations to parliament based on this information.

As was found by the HLRP as well as the State Capture Commission, the JSCI was ineffective in the state capture era, for various reasons. The JSCI was found to have failed in its role by not acting on the Inspector General's reports nor on the briefing given to them by Mzuvukile Jeff Maqetuka. In doing so, the Chief Justice found that parliament contributed to state capture.[127]

The JSCI is governed by the Intelligence Services Oversight Act 40 of 1994, which provides that the Committee shall have access to the AG's report on the SSA and the report of the Evaluation Committee[128], among others. The JSCI is also to consider and report on the appropriation of revenue or monies for the functions of the SSA. However, one can immediately see that the JSCI may be hampered by restrictions on access to the intelligence services and entities documents contained in s4(2) of the Act. Section 4(1) of the Act also limits the Committee's access to documents to only those that are "necessary" for the performance of its functions. In the context, the party who determines which documents are "necessary" could only be the SSA itself. Therefore, the existing legislation provides that crucial information may be withheld from the JSCI simply because the DG of the SSA deems it to be unnecessary.[129]

The new Bill does nothing to address this shortcoming.

Ultimately, because the JSCI lacks a full view of the intelligence community's activities and therefore how expenditures relate to those activities and operations, it cannot make informed decisions and recommendations on the intelligence budget. This is exacerbated by the fact that the AG cannot conduct an unqualified audit, because the intelligence services and entities can, through classification, block access to any information the AG needs to carry out a full and proper audit. The result, is that the JSCI (and parliament by extension) effectively provides nothing more than a rubber stamp in approving the intelligence budget.

A remedy for this is not without precedent; we can again see an implementable solution in the oversight model used in the Netherlands, where a non-partisan[130] parliamentary oversight committee has access to classified information relating to the past activities of the security services, as well as to its future plans at the time that the budget is approved. Certain members of the legislature therefore have the power to block the approval of funds to the security services

126 See Annexure 2: Heideman, paras 23-26, p 7-8 AND paras 130 – 132, p24
127 Ibid.
128 For and examination of recommendations pertaining to the Evaluation Committee, see 4.7 below
129 Annexure 2, Heideman, para 23 p7
130 Annexure 2, Heideman, para77 p17

were they to be of the opinion that the funds may be used/may have been used for illegitimate or nefarious purposes.[131]

Similar circumstances prevail in the United Kingdom. The British equivalent of the JSCI, the Intelligence and Security Committee (ISC), was established under the Intelligence Services Act of 1994. Its powers were extended under the Justice and Security Act of 2013, in terms of which the ISC now has access to primary material held by the security services.[132] (However, the British system is inadequate in that the ISC is not protected from interference from the Prime Minister, who still has the power to redact any sections of the ISC's annual reports to the public should he, she or they feel that releasing such information could prejudice the intelligence services.)

Recommendations:

a) In order to make informed recommendations upon which to base the budget allocations for the intelligence community, we recommend that the Bill provides for the JSCI to have full access to all the documents, information, persons, and systems that they require to approve the annual budget for the intelligence services and entities. What is required must be determined by the JSCI, and *not* the services and entities. To protect the information that is justifiably classified, the JSCI need not disclose information to broader parliament when they make their final budget recommendations. (For recommendations regarding criminal penalties for failing to disclose or unduly classifying information, see 4.5 below)

b) The JSCI should have the power to block approval of funds where they are of the opinion that expenditure is unjustified, or in funding areas where any of the past year's expenditures were underutilised, irregular, unlawful, wasteful, and/or used on illegitimate activities or activities that were not budgeted for in the financial year. In other words, as is the case with treasury, the JSCI should apply a *'use it or lose'/'use it well and legally or lose it'* approach.

c) In order to assist them in their work and decision-making on matters pertaining to the budget, the JSCI must ensure that it has the necessary support (which should be funded from parliament's budget to ensure that sufficient funds are not withheld by the intelligence community or the executive). Such support should include expert forensic accountants, specialists in intelligence operations and strategies, and legal council. These persons must be appointed by the JSCI, either on a permanent or on a consultative basis, and should obviously require security clearance. While the JSCI may consult with the Minister and the members of the intelligence community as to what type of expertise would best serve them, the final decision on who to appoint and consult should lie with the JSCI.[133]

d) In addition to end-of-year reviews, the JSCI must be empowered to, of their own accord and at any time, launch ad hoc investigations into any part or aspect of the intelligence community. The JSCI must be empowered to make legally binding recommendations following such ad hoc investigations. The JSCI must also be empowered to open a criminal or civil cases based on the outcomes of an ad hoc investigation, and to turn to the courts in their efforts to have their decisions and recommendations upheld. Finally, the JSCI must have the power to remove the directors-general or heads of services and entities from their posts (should the outcome of an

131 Ibid

132 Annexure 2, Heideman, paras 94 – 96 p19

133 HLRP Report para 13.5 p97 (e) *"The panel's recommendation states: Given the demands of intelligence oversight, he idea of a dedicated capacity for the JSCI needs to be explored further."*

investigation justify this).

e) Alternatively (or simultaneously) the JSCI must be given the power to, at any time, compel the Evaluation Committee or the IG to investigate any part or aspect of the intelligence community. Should it be warranted by the outcome of the ad hoc investigation, the IG must be compelled to open a criminal or civil case based on the outcomes of an ad hoc investigation, and to turn to the courts in their efforts to have their decisions and recommendations upheld.

f) In order for the JSCI to do its job, the Auditor-General must have unfettered access to the all documents, classified and unclassified, required to audit the intelligence community's finances. Which information and documents are required must be determined by the AG, not the services or entities.

4.3 The Office of the Inspector General of Intelligence

4.3.1 Agreement on and endorsement of certain recommendations by the IG, Mr Imtiaz Fazel

We support the following recommendations made by the current IG, Mr Imtiaz Fazel, during the his briefing to the Ad Hoc Committee on GILAB, which took place on 7 December 2023:

a) “Significant Intelligence Failure” must be clearly defined. We, however, also recommend that this definition be reached following consultation with not only the intelligence services and the entities, but also with the IG, and external experts on intelligence matters and related legislation. The definition should be benchmarked against existing international policy and practice. The details of such benchmarking must be included in the memorandum to the Bill.

b)“Unlawful Intelligence Activity” must be clearly defined to prevent a subjective interpretation of the term by the intelligence services and entities. We contend that such a vague definition leaves room for abuse by the intelligence community.

c) In issuing certificates, the IG must express an opinion on the fair presentation of the intelligence services and entities' operational report before them. The term “fair presentation” must also be defined. (It is not sufficient to simply require that the IG be 'satisfied' as this lacks clarity.)

d) Definition of intelligence as contained in the National Strategic Intelligence Act and the Intelligence Oversight Act must be made uniform and standardised.

e) The IG's mandate must extend to both the intelligence services and the entities. That is, oversight of the domestic and foreign intelligence services, the NCC, the OIC and the Academy must all be a part of the IG's oversight mandate and functions.

f) Reports of the IG should contain findings and recommendations for *all* functions served by the IG, and recommendations should be binding.

g) Explicit provision must be made for the JSCI to order the IG to conduct investigations at the behest of the JSCI.

(h) We agree with the IG that the Bill currently further limits the autonomy of the IG's office, and that an appropriate institutional form is required to ensure the autonomy and independence of the IG's office.

Specifically problematic, is the the following amendment:

The Minister—

> *(a)* must, after consultation with the Inspector-General, appoint such number of persons to the office of the Inspector-General as may be necessary for the performance of the functions of that office, on such conditions of employment and security requirements as are applicable to members of the intelligence services; and
>
> *(b)* may determine the organisational structure and grading of the posts for the functioning of the Office of the Inspector-General in terms of the Intelligence Services Act, 2002 (Act No. 65 of 2002''.

This amendment creates ample opportunity for ministerial over-reach. The OIGI must have complete autonomy over its own budget, organisational structure, and who it chooses to hire in terms of normal staff contingent (excluding the IG and the Deputy-IG – see our recommendation below).

j) Section 7(7)(c) of the existing Intelligence Oversight Act provides for the following:

> *"The functions of the Inspector-General are, in relation to the Services-*
>
> *…*
>
> *to perform all functions designated to him or her by the President or any Minister responsible for a Service."*

The new Bill provides that

> *"the Minister, acting with the concurrence of the Committee, must make regulations regarding the performance of [his or her] the functions designated to the Inspector-General under section 7(7)(c)".*

We agree with the IG that this amendment, which refers solely to section 7(7)(c), is a "fundamental error" which limits of power of the Minister and the JSCI to only issue regulations to those IG functions designated by the President or Minister responsible for a Service. Such regulations must be issued on *all* functions of the IG, and in fact the law must provide for the Minister, in concurrence with the JSCI, to regulate any matter that has to do with the Intelligence Oversight Act.

k) The definition of intelligence gathering conflates intelligence gathering with intelligence analysis. The definition must either be limited to that of intelligence gathering, or a better definition must

be provided for covert intelligence collection. In addition, we recommend strongly recommend that intelligence analysis be provided with its own specific, operationalised definition. This is in addition to our recommendations on definitions in section 1 of this submission.

l)The IG argued that the Bill allows for members of the intelligence services to "impede and apprehend members suspected of contravention of this Act and related regulations and hand them to the relevant law enforcement agencies". He further stated it was unclear whether intelligence service members had now been given the powers of arrest, and that, in the absence of offences stipulated in the Bill, it is not clear how a contravention will take place. He further argued that the power to apprehend resides with the police, and that to confer powers of arrest on members of the intelligence services undermines the intention of the Constitution and White Paper on Intelligence, and runs contrary to the segregation of functions between the intelligence services and the police.

While we agree with the IG on these technical points, we find it exceedingly alarming that the Bill would allow for the apprehension of person, based on the vague criteria of what constitutes national security and the absence of any clearly stipulated offences. The idea that civilian intelligence services can apprehend a person raises questions as to how this will play out in practical terms: How long will an apprehended person be detained? Where will they be detained? Will they have access to a lawyer? What role, if any, will the police play?

The most alarming aspect of this provision for apprehension, however, that it mimics the illegal practice of forced renditions and illegal detention.[134] It does this by creating an opportunity for the intelligence services (under the guise of secrecy justified by a non-sensical definition of 'national security') to apprehend persons and detain them in secret, without any of the normal legal protections that accompany apprehension and arrest by the police. This sets the stage for gross human rights violations by the services, and its results – illegal detention and torture by both democratic and authoritarian regimes – have been clearly documented.

South Africa cannot be allowed to go down this path, but there are already strong indications that the country's intelligence services are more than capable of moving in that direction.

Two examples come to mind:

Testimony was heard before the State Capture Commission that Mrs Matuli Zuma was detained, against her will, by the SSA at their various safe houses on suspicion of having poisoned then president Mr Jacob Zuma. She was said to have been detained during the investigations into the allegations against her, and was only released once she made contact with her legal counsel.[135]

A second example is that of Khalid Rashid, a Pakistani national who was reportedly apprehended

134 See for instance *"Guantánamo Bay: over 20 years of injustice"* Amnesty International. 9 August 2023. Available at https://www.amnesty.org.uk/guantanamo-bay-human-rights and Jeff Li, *"China's History of Extraordinary Rendition"*. 16 June 2019. Available at https://www.bbc.com/news/world-asia-china-48634136

135 See Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector Including Organs of State Report: Part V Vol. 1: State Security Agency, and Crime Intelligence, para 592 p234; para 745 to 746, pp285-286.

by state intelligence services at his family's home in KwaZulu-Natal, and taken out of the country in a clandestine manner, devoid of any application of South Africa' s criminal or civil legislation.[136]At the time, his lawyer told the Mail&Guardian newspaper that 'Rashid was taken from South Africa to an unknown port of entry in Kenya', stating:

"From Kenya, we aren't certain; at that stage investigations suggested he may have been taken to the Channel Islands. Others suggested Guantánamo," she said, adding that Mr Rashid told her that during this time he had been tortured: "He was waterboarded, he was incarcerated, they put on a light continuously so that he wouldn't fall asleep."

To this day, no official explanation has been issued by the South African government as to what actually happened to Mr Rashid.

South Africa's intelligence services cannot be granted the right to apprehend persons. We strongly recommend that this power should reside with the South African Police Services only.

m) Gilab provides that the new South African Intelligence Agency should "provide periodic national security briefing to the Joint Standing Committee on Intelligence, members of Cabinet, Premiers, Parliamentary Presiding Officers and the Chief Justice". While we do not take issue with providing briefings to the Chief Justice (since these are only briefings, and not review matters), we agree with the IG that the Inspector General of Intelligence and the National Security Advisor should we also briefed. In addition, we recommend that the Evaluation Committee (see 4.4 below) also be briefed.

However, we disagree that the Agency should provide such a briefing to the Cabinet. This must be done by National Intelligence Coordinating Committee (NICOC), which consolidates and then presents all of the intelligence services' information. In fact, it is preferable that NICOC conduct such briefings to all relevant entities, in order to provide a clear, comprehensive view of the intelligence landscape that is free of contradictions and potential sources of confusion.

n) In addition to the term "civilian intelligence structures (which the Bill defines), the Bill refers to the term 'civilian intelligence services', but does not define it. This term needs to be defined, or otherwise removed.

o) The Bill amends the Intelligence Services Act, 2002, to stipulate that the "Minister must in the prescribed manner make provision for internal rules to deal with complaints, grievances and consultation on conditions of service and human resources within the **[Agency]** Civilian Intelligence Service.''

The IG recommended that the Minister should also make provisions for an alternative dispute resolution mechanisms that is independent from and falls outside of the management hierarchy of the intelligence services and entities. His motivation was that the inclusion of such a mechanism could compromise for the fact that the CCMA is not available to members of the intelligence services and entities; he added that the absence of such recourse had led to the dereliction of duty by management, and that this fundamentally impacts on moral within the services.

We agree with the IG that such an alternative mechanism should be implemented, and are of the opinion that this will also provide an additional layer of protection for those who wish to report malfeasance within the services and entities to management (particularly where persons in

136 See Heidi Swart, *"How cops and crooks and grab your cell phone – and you."* The Mail&Guardian. 29 November 2015. Available at https://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you/

management are the ones who are subject to a complaint by any of their subordinates).

4.3.2 Further aspects regarding non-binding nature of recommendations of the IG

Currently, the IG cannot make legally binding recommendations.[137] Accordingly, there appears to be no significant consequences (legal or otherwise) for the intelligence services and entities should they ignore the recommendations of the IG. The result is that the IG's recommendations are simply not implemented.[138] In fact, during his testimony[139] before the State Capture Commission, Dr Setlhomamaru Dintwe explained that, after he submitted reports to the intelligence services and the JSCI, but they were ignored.

For the sake of convenience, we list[140] the unaddressed issues stemming from various IG certifications which were ignored over the years. This can also be found in the HLRP report:

These include the following:

- The involvement of the Minister of State Security in operational work and administrative decision-making of the SSA;
- Certain forms of intrusion such as surveillance and targeting are not regulated through legislation or ministerial regulation, in spite of the fact that there is a constitutional requirement to legislate such objects and powers;
- Intermittent restructuring within the SSA had created restructuring fatigue;
- Continued politicisation of the SSA remained a problem;
- The blurring of the lines between covert and overt operations, where covert resources are being used for overt purposes;
- Poor or inadequate training on SSA Operational Directives;
- The SSA approved framework for the Cover Support Unit may not be in compliance with the Constitution and applicable laws;
- The appointments of senior managers of SSA are often made outside the prescribed recruitment processes;
- There is a culture of non-accountability in the SSA;

137 Marianne Merten *"Vague Intelligence law amendments open door for ongoing abuse by State Security Agency"* The Daily Maverick. 7 December 2023. "Available at https://www.dailymaverick.co.za/article/2023-12-07-vague-intelligence-law-amendments-open-door-to-ongoing-abuse-by-state-security-agency/

138 Vicky Heideman *"How to unmuzzle the state security watchdogs"* Intelwatch. 5 July 2023. https://intelwatch.org.za/2023/07/05/oped-zondo-how-to-unmuzzle-state-security-watchdogs/

139 Judicial Commission of Inquiry into State Capture Report Part 5 Vol 1 para 366 - 367 at p 148-149

140 See for instance the HLRP report section 13.3.2 p95 for a list of legal issues identified by the IG that were not addressed.

- There are a large number of acting capacity appointments;
- The SSA does not have an internal collective bargaining mechanism;
- The SSA does not maintain adequate integrated electronic audit trails and logs on the use of intrusive measures;
- The administration of applications for intercept of communication is inadequate;
- There is inadequate access to the OIC's real-time intercepts by the SSA's Domestic Operations;
- There are numerous barriers to effective foreign intelligence collection and liaison;
- Intelligence and counter-intelligence activities at provincial level have been seriously compromised by the lack of dedicated human capacity in strategic areas.

While we support the current IG in his recommendation to the Ad Hoc committee on GILAB that the IG's recommendations must be binding, we note with great concern the suggestion that these recommendations only be finalised and made binding once the heads of intelligence services and relevant ministers have agreed to accept them.

We strongly recommend against this practice, as it creates an opportunity for executive overreach, since a minister can use these negotiations to exert undue pressure on the IG. This is particularly true given the status quo that the IG is not independent from the Minister responsible for intelligence in terms of resource allocation, budget expenditures and staff appointments. Even if the IG were fully independent, negotiating over recommendations on and requiring agreement from parties to whom the recommendations pertain, creates an opportunity for those recommendations to be watered down. This opportunity will not exist if the final binding recommendations are left to the IG to determine.

During his testimony before the State Capture Commission, Dr Dintwe explained that part of the IGI's task was to oversee whether or not the services were able to develop internal controls and implement them, similar to how an Auditor General functions. He described a situation whereby the IG identifies problems within the services, brought these to the services' attention, and afforded the services an opportunity to apply internal disciplinary procedures. Significantly, Dr Dintwe consulted with the relevant minister before finalising recommendations in what appears to have been an attempt facilitate their practical implementation.

We do not find fault with the practice of consulting with the relevant minister, intelligence services, and entities to gather information to inform recommendations, nor to we find fault with the practice of giving the services and entities a reasonable opportunity to implement the recommendation internally. However, the Bill must stipulate that the IG should have the final say

over what is contained in the recommendations. It must also stipulate the time frame within which these recommendations should be implemented internally, and that the IG does not require concurrence from the executive or heads of services to establish the time allotted to implement the recommendations.

If either the intelligence services, intelligence entities, or member/s of the executive responsible for intelligence do not adhere to recommendations within the time frame determined by the IG (and only the IG), the IG must approach the public courts to seek remedy.

The Bill must make explicit that any form of suspected or confirmed ministerial/executive interference and overreach in the operations and budget of OIGI constitutes an offence, and must be investigated by the IGI.

The Bill must also make explicit that any form of suspected or confirmed ministerial/executive interference and overreach in relation to the intelligence services or entities constitutes a criminal offence, and must be investigated by the IGI.

Once the IGI investigates any suspected or confirmed incident of executive overreach, their recommendations in this regard must be legally binding. If recommendations are not adhered to, the IGI must approach the court for relief.

Should the IGI conduct an investigation and conclude that there was criminal misconduct involved, they must report the matter directly to the police, and pursue the matter through the courts.

4.3.3 Independence of the OIGI as it relates to funding and budget

The IG is currently funded from the budget of the State Security Agency[141]. Thus, when conducting investigations into the Agency, the IG must bite the hand that feeds it. This is obviously not desirable, and the IG risks being chronically underfunded[142] . Already in 2008, the Matthews Commission concluded that the IG could not be independent if it relied on the intelligence services for funding[143] This shortcoming has since been underscored by the HLRP[144] and in the State Capture Commission report on the SSA.[145]

During his testimony before the State Capture Commission, former IG Dr Dintwe made the following recommendations that:

- the OIGI be established in terms of the Public Service Act as a national department, distinct from the SSA;

141 Intelligence Services Oversight Act 40 of 1994. Section 7(13). Available at https://static.pmg.org.za/docs/120224oversight_0.PDF

142 See for instance Steve Kretzmann. "Meddling ministers and dodgy spooks: Inspector-General of Intelligence lays bare his woes to Zondo" The Daily Maverick. 21 April 2021. Available at https://www.dailymaverick.co.za/article/2021-04-21-meddling-ministers-and-dodgy-spooks-inspector-general-of-intelligence-lays-bare-his-woes-to-zondo/

143 Final Report of the Ministerial Review Commission on Intelligence. 10 September 2008. Available at https://www.r2k.org.za/wp-content/uploads/Matthews-Commission-Report-10-Sept-2008.doc

144 HLRP para13.3.2 pp92-93

145 State Caputre Commission report on SSA, para 365.1 and 365.2 p147

- the OIGI should have its own funding from a source not aligned to the SSA

The HLRP report states the following with regard to the findings of the IGI by both the 2008 Matthews Commission and the 2006 Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies:

> *"Over a decade has passed since these two sets of findings on the OIGI were made by ministerial-appointed entities. It appears to the Panel that, with the change in administration in 2009, there was no follow-up on these recommendations. The Panel understands, however, that there has been an attempt to draft and promulgate the regulations governing the OIGI. These were drafted in 2010 and submitted to the then Minister and the JSCI, but it was decided to put these on hold until the promulgation of the GILAA – the Act which amended all related intelligence legislation to provide for the establishment of the SSA. After GILAA was promulgated in July 2013, the regulations were redrafted and provided to the then Minister in 2014 who did not respond. The regulations were provided to the then Chair of the JSCI in November 2014, but the OIGI has heard nothing since."*

From the above, it is clear that the need for reform to the office of the IG to ensure independence have long been known and understood. There is therefore no reason why GILAB should not be utilised to rectify the lack of independence and autonomy of the OIGI.

Recommendations

We support Dr Dintwe's recommendations to the State Capture Commission that the OIGI be established in terms of the Public Service Act as a national department, distinct from the SSA, and that the OIGI should have its own funding from a source not aligned to the intelligence services. The Bill must therefore ensure that the OIGI is not dependent cost centres controlled by intelligence services at the Musanda Complex.

The Ad Hoc Committee on GILAB should also consider other structures, such as that of the Financial Intelligence Centre.

An alternative, although far less desirable, is that the Bill be used to amend section 3 of the Intelligence Services Act in order to establish the OIGI as a department in the same manner that the former National Intelligence Agency (NIA) and the South African Secret Services (SASS) was established (or the envisioned South African Intelligence Agency and the South African Intelligence Service, for that matter).

Regardless of which institutional form is ultimately adopted, the Bill must, at the very least, achieve the following:

- The IGI must be insulated from interference by the executive and the services, and the Bill should make this, as well as mechanisms to achieve it, explicit.

- This can be done by ensuring that the Bill stipulates that the OIGI must have complete autonomy over its own budget, organisational structure, and who it chooses to hire and fire in terms of staff contingent. The IG, and not a director-general of the intelligence services, should be the responsible accounting officer for the OIGI.

- The budget for the OIGI must also be sufficient in order for the office to function effectively in its oversight role. At the very least, if the OIGI is funded through the intelligence services' cost centres (although this is not recommended), the Bill could provide that the budget must be ring-fenced within the larger intelligence budget. (The practice of ring-fencing is similar to that suggested to the Ad Hoc Committee on Gilab by NICOC[146] during its parliamentary submission on the Bill. It has also been applied to the OIGI in the past.[147]) To do this, in turn, the Bill must provide for the JSCI to have control over the final budget allocation recommendations to parliament, which means the Committee needs to know *exactly* how the intelligence services and entities are spending taxpayers' money. This will allow the JSCI to decide how money should be allocated not only to actual intelligence work, but also to public oversight. Thus, the JSCI will need full access to classified information not only to conduct oversight properly, but also to approve and recommend an adequate budget allocation for the IG. The portion of the intelligence budget to be allocated to the OIGI should also be informed by the budget plan presented to the JSCI by the IG. The final allocation must be balanced against the scope of the budget allocated to the intelligence services and entities for the same financial year.

- In addition to taking into account the IG's budget projection, the JSCI must also consult directly with the OIGI before settling on an amount to allocate.

- As an additional safeguard, the Bill must stipulate a fixed minimum percentage of the total intelligence budget to be ring-fenced and allocated to the OIGI during each budget year.

4.3.4 The lack of provision for deputy Inspector General

During the State Capture era, following the end of Faith Radebe's term as IG in 2015, the position of IG remained vacant[148] for a number or years until Dr Setlhomamaru Dintwe was appointed IG in 2017. Without an actively appointed IG, the office was effectively hamstrung. Since the IG is appointed by the president, it was possible to leave the position open for such a period of time, and today the public is still largely dependent on the president's discretion as to whether or not an IG will be appointed in good time. The Bill does nothing to remedy this state of affairs.

As a solution to this, we recommend that a deputy IG be appointed. Their terms cannot coincide precisely, since that would mean that both would vacate their offices simultaneously, again leaving the OIGI hamstrung.

In the event of an IG leaving office while the seat of the deputy IG remains unfilled, an alternative safeguard needs to be introduced to ensure continuity in leadership and the OIGI's continued functioning. Such a safeguard could include a stipulation in the Bill compelling the IG, prior to vacating office, to appoint from within the existing staff contingent a suitably ranked and experienced staff member as acting-IG in the interim period.

---

146 *Briefing by the National Intelligence Coordinating Committee on its input into the General Intelligence Laws Amendment Bill*. 5 December 2023. Available at https://www.youtube.com/live/NZLnCYt4nuc?si=HYyM9IqGLM5SHiw1

147 ANNUAL REPORT OF THE JOINT STANDING COMMITTEE ON INTELLIGENCE FOR THE FINANCIAL YEAR ENDING 31 MARCH 2020 INCLUDING THE PERIOD UP TO DECEMBER 2020. p19 Available at https://www.parliament.gov.za/storage/app/media/Docs/atc/21a7768b-9b45-4985-95e9-2bf98d576b2f.pdf

148 Jenny Evans "Fill Inspector General of Intelligence post urgently – R2K" News24. 22 April 20216.Available at https://www.r2k.org.za/2016/04/23/fill-inspector-general-of-intelligence-post-urgently-r2k/

4.3.5 Whistleblower protection for persons approaching the IGI with complaints

President Cyril Ramaphosa has acknowledged the importance of whistleblowers in combatting corruption. This was in response to the report from the State Capture Commission. He stated:

"Whistleblowing is an essential weapon in the fight against corruption. The actions of whistleblowers have played a vital role in exposing many of the activities that were part of state capture. Whistleblowers need to be encouraged to report instances of fraud and corruption and need to be protected from victimisation, prejudice, or harm."[149]

We recommend that the Bill must ensure the following:

a) A person lodging a complaint with the IG should be considered a whistleblower eligible for witness protection should the IGI find that

i. the complaint warrants further investigation; and

ii. the complaint is of such a nature that the disclosure of the whistleblower's identity could potentially lead to harm coming to the whistleblower because of retaliatory measures taken by actors within the intelligence community.

b) Such a whistleblower must be afforded the protections provided in existing legislation (such as the Witness Protection Act 112 of 1998).

c) The IG should be empowered with adequate budget, or access to budget mechanisms, to facilitate protection for whistleblowers.

d) The IG should have the right to contract private security services to ensure witness protection for whistleblowers.

e) The IG should establish an anonymous, secure whistleblower hotline to facilitate reporting of complaints, not only from the public, but also from members within the intelligence community.

4.4 The resurrection and reimagining of the Evaluation Committee

While the JSCI receives various reports from the intelligence community after-the-fact, it seems that at present South Africa has no functioning mechanism to continually review the day-to-day activities and intelligence priorities of South Africa's intelligence services and entities. This role would have been served by the now-defunct Evaluation Committee (provided for in section four of the Secret Services Account Amendment Act 142 of 1992). The committee's purpose was to "evaluate all intended secret services in order to determine whether the object thereof and the *modus operandi* to achieve it are in the *national interest*; and review all secret services annually with the said object in order to determine whether they may be continued...".[150] (Further amendments were made by the Secret Services Account Amendment Act 5 of 1993.)

As it stands, without a functioning Evaluation Committee to adjudicate on the question of 'national interest', this nebulous term was (and still is) left open to the sole interpretation of the SSA's

149 South African Human Rights Commission *"Frequently asked questions on whistleblowers"* 2022. p1, Available at https://www.sahrc.org.za/home/21/files/Human%20Rights%20FAQ%20Whistle%20Blowers%20Booklet.pdf

150 Annexure 3, Heideman, para 29 p8

Director-General, with no oversight mechanisms in place.[151]

However, to revive the Evaluation Committee in such a manner that the executive cannot ride roughshod over the oversight entities' decisions, the current Bill would have to amend the prescripts of Act 142 of 1992 and Act 5 of 1993 significantly; as the law now stands, the Evaluation Committee is not independent of the executive.

Act 42 provides for the Evaluation Committee to consists of three to five members – all to be appointed by the president. The president also has the power to dismiss these committee members. Furthermore, the president could decide to pay committee members for their service, and how much. While the committee can make recommendations, the responsible minister or the president can override recommendations. Act 5 provides some improvement, but not significantly so. It allows for the appointment to the Evaluation Committee of one member that is appointed in consultation (not in concurrence) with the political opposition. However, the final decision still resides with the president.

Recommendations

It is evident that the above two amendment acts did nothing to bolster the independence of the Evaluation Committee. They contain no provisions to shield the Committee from executive interference.

a) We therefore strongly recommend that the Bill amends legislation so that the Evaluation Committee must pass the test of adequate independence laid down by the majority in the case of Hugh Glenister vs President of the Republic of South Africa And Others 2011(3) SA 347 (CC). As such, this could be an independent Chapter 9 institution (or similar body) consisting of three members appointed by the Chief Justice, at least two of which must have previously served as judges of the High Court.[152]

b) An alternative solution, would be for the JSCI to designate members to a sub-committee, with equal representation from members of each party. In other words, no party should outnumber other parties to the extent that they could control the vote unilaterally.

c) Regardless of which of the above models are chosen, the committee must have expert assistance in the form of members who serve in a non-executive capacity (in other words, without voting capacity) as advisers. These persons must be a suitably qualified. They should include, at the very least:

- a member from the Office of the Inspector General (this can be the IG, or a suitable staff member appointed by the IG);
- at least one legal expert (with adequate security clearance) to assist in matters of local and international intelligence-related laws; and
- at least one expert (with adequate security clearance) in strategic intelligence matters at a local and global level, with a particular knowledge of the South African and African context.

d) As is the case with the JSCI, the additional experts on the panel should address the HLRP's

151 Annexure 3, Heideman, para 30 p8
152 See annexure 3, Heideman, para 125 p23

concerns that committee members lack the expertise and knowledge to adequately fulfill their functions.[153] It also mimics the model of the HLRP to some extent (which had members with "senior level experience and expertise in law, security studies, civil society, academia, the intelligence and security community and other arms of government"). [154]

e) The Evaluation Committee must consult with the directors-generals/heads of the various intelligence services, the heads of the intelligence academy, as well as the heads of the OIC, the NCC and the Intelligence Coordinator for NICOC. The Bill should provide that the Evaluation Committee may consult with any other members of the intelligence services and intelligence entities as the need arises. The committee must also be empowered to call before it any witnesses it deems relevant, and such witnesses must be legally compelled to cooperate and to provide classified documents and information as deemed necessary by the Evaluation Committee. Verbal testimony must be provided under a sworn oath. (For recommendations regarding criminal penalties for failing to disclose information or unduly classifying information, see 4.5 below.)

f) The Evaluation Committee's recommendations should be legally binding. In addition, they must be reflected in the final budget allocation (as recommended by the JSCI) of the intelligence services and intelligence entities.

g) While intelligence services and entities as well as NICOC must be consulted, their concurrence should not be required by law in order for the Evaluation Committee to make final recommendations.

h) The Evaluation Committee must report their findings and recommendations to parliament, and make their findings public and publicly accessible. Such findings should be as detailed as possible, without revealing aspects that could pose a risk to national security (whatever that may be). The final decision of what should appear in the publicly accessible report will be left to the Evaluation Committee.

i) The president, the minister responsible for intelligence, the directors-general, and the heads of the intelligence entities must be furnished with a full, unredacted report. None of these parties may unilaterally redact any aspects of the report.

j) As is the case with the JSCI, members of the Evaluation Committee (and those non-executive members appointed or coopted to assist them with expertise) must have full access to classified documentation, information, premises and systems that they may require to carry out their reviews and make decisions and recommendations. The law must state clearly that it is not the prerogative of the executive nor of the intelligence services and entities to determine what information the Evaluation Committee should have access to; such determinations should lie solely with the Evaluation Committee.

k) Lying to or withholding information, classified or otherwise, from the Evaluation Committee, where the committee deems such information necessary to conduct its work, should be penalised as a criminal offence (see 4.3 (g) below).

---

153 HLRP Report para 13.5 p97 (e) *The panel's recommendation states: "Given the demands of intelligence oversight, the idea of a dedicated capacity for the JSCI needs to be explored further."*

154 HLRP Report p 1

l) The Evaluation Committee should produce quarterly review reports, and submit those to the JSCI on a continual basis. They should also be made publicly accessible as soon as they are presented to parliament. The Evaluation Committee must further have the power to initiate legal proceedings based on its review findings.[155]

m) For the Evaluation Committee to have parameters placed upon its work, clear definitions and criteria for the following concepts must be supplied in the bill, and these must be defined in a manner that operationalises them within the confines of the Constitution and White Paper on Intelligence:

x. National Interest

xi. National Security

xii. Threat

n) In addition to quarterly reviews, the Evaluation Committee must be empowered to, of their own accord and at any time, launch an ad hoc investigation into any part or aspect of the intelligence community. The Evaluation Committee must be empowered to make legally binding recommendations following such ad hoc investigations. The Committee must also be empowered to open a criminal or civil case based on the outcomes of an ad hoc investigation, and to turn to the courts in their efforts to have their decisions and recommendations upheld.

o) Alternatively (or simultaneously) the Evaluation Committee must be given the power to, at any time, compel the IG to investigate any part or aspect of the intelligence community. In needed, the IG must be able to pursue matters in court following the outcome of such an ad hoc investigation, and recommendations of such an investigation must be legally binding (as should be all recommendations from the IG).

4.5 Preventing access to classified material or failing to provide access to information required for investigations into the intelligence community

While currently the IG is legally entitled to have access to any classified documents they deem necessary for their investigations, the same is not true for the JSCI and the AG. The JSCI is restricted by what the intelligence services and entities deem necessary for the JSCI and AG to perform their oversight.[156]

During his testimony before the State Capture Commission, Dr Setlhomamaru Dintwe explained that one way in which the SSA could stifle investigations into their activities, was to classify documents and block access to information required by investigators external to the SSA (like the NPA). Thus, the Agency could shield themselves against criminal investigations.[157] Perhaps the clearest illustration of this, is when the SSA prevented the members of the Investigating Directorate of the NPA and the IG from entering SSA headquarters to access materials necessary to investigate the Agency (following the evidence heard at the State Capture Commission).[158]

---

155 Lotte Houwing *"Dutch watchdog orders bulk datasets held by intelligence services to be deleted"* About Intel. 22 June 2022. Available at https://aboutintel.eu/ctivd-bulk-datasets-held-by-intel-need-to-be-deleted/

156 See Annexure 2: Heideman paras 23-26, p 7-8 AND paras 130 – 132, p24

157 Judicial Commission of Inquiry into State Capture Report Part 5 Vol 1

158 Qaanitah Hunter, Kyle Cowan, Pieter du Toit and Jeff Wicks "Top spies block anti-corruption unit from seizing secret documents on 'farm'" News24. 11 March 2021. available at

It is entirely possible – without compromising national security (whatever that may mean) – to devise a process to ensure secure access to classified material for external entities tasked with conducting lawful criminal investigations into any aspect of the intelligence services or entities. In fact, a clear procedure for this was established in 2021 during the process of launching and NPA ID investigation into the SSA (an investigation based on testimony at the State Capture Commission).

In summary, this entailed securely housing all information deemed relevant to the period under investigation with the IG (while the investigation was ongoing). The NPA or SSA could have copies of the documents to prepare their cases, but not the originals. Should any original documents be required as evidence in court, the SSA would be allowed to redact information that could harm national security if revealed, or to declassify the document. This agreement, however, was never honoured, no doubt contributing to the fact that the findings of the State Capture Commission are gathering dust.

In addition, if members of the intelligence community have the audacity to withhold access to information required for investigations by oversight entities, there is no reason to believe that the same practice does not occur during investigations that are internal to the intelligence community (i.e. when the members of the services or entities are investigated by other members). The Bill also does nothing to address this aspect.

Recommendations:

a) The bill must introduce provisions to ensure that the JSCI, the Auditor-General, and any investigative and prosecutorial authorities external to the intelligence community who are conducting lawful and legitimate investigations into the services (such as the NPA) are granted full access by the intelligence community to any and all classified and unclassified materials, information, systems, locations and persons they deem necessary to fulfill their functions. Similarly, the Bill must ensure that information is not withheld or classified unduly during internal investigations in the intelligence community.

b) When external investigations by entities such as SAPS or the NPA's ID are taking place, the IG should act as the interface between the intelligence community and the external investigative authority by securing and facilitating access to classified and sensitive information required for the investigation

c) The Bill must provide for it to be a criminal offence for any member of the intelligence community to withhold information (by undue classification or through any other means) requested by

viii. the JSCI;

ix. the Evaluation Committee

x. the AG;

xi. the IG ;

xii. investigators external to the intelligence community; and

https://www.news24.com/news24/southafrica/news/breaking-top-spies-block-anti-corruption-unit-from-seizing-secret-documents-on-farm-20210311-2

xiii. internal investigators (who are themselves members of the intelligence community)

when any of these bodies are conducting an investigation into or a review of the intelligence services or entities and deem it necessary to have access to said information in order to carry out the investigation or review successfully.

d) The determination of the necessity of such full access to information must be made by the parties conducting the investigations or reviews, and not by those being investigated or reviewed.

e) If there is reasonable suspicion with any of the investigating/reviewing entities that crucial information has been withheld or unduly classified, this must be reported directly the relevant director-general/heads of the intelligence services or head of the intelligence entities, as the case may be. If the relevant director-general or head fails to grant the required access within a reasonable period of time (the reasonability of which should be left to the determination of the investigating party), the investigating party must report the matter to the IG (unless the IG is a part of the investigating party). The IG must lodge a criminal complaint with the South Africa Police Service.

f) The bill must stipulate penalties should the court find a member of the intelligence community guilty of withholding access to or unduly classifying information required in an investigation or review into any of the intelligence services or entities.

g) Any director-general or head failing to ensure the release of classified information, or access to any other information deemed necessary to conduct an investigation, must be deemed complicit in the offence and face similar penalties.

4.6 The weaponisation of vetting

The IGI and the JSCI are vetted by the State Security Agency in order to determine security competence. They must be granted security clearance to commence with their work. Thus, it is within the power of the intelligence services to revoke security clearance of those who investigate them, thus hamstringing said investigations.

The current bill does nothing to safeguard against such a malpractice, which is not theoretical: In 2018, then SSA director-general Arthur Fraser[159] revoked the security clearance of then IG Setlhomamaru Dintwe, at a time when Dr Dintwe was investigating him. Dr Dintwe turned to the court to have his security clearance reinstated, and maintained that his clearance was revoked to stymie the investigation into Mr Fraser. Dr Dintwe's view that Mr Fraser was deliberately withdrawing his clearance in order to stop the investigation was later supported by the State Capture Commission's report on the SSA.[160]

While testifying before the State Capture Commission, Dr Dintwe set out the legal framework for security vetting and the issuance of security clearance certificate, and testified that while

159 Marianne Merten "When guardians refuse to be guarded, or, the curious case of one Arthur Fraser" The Daily Maverick. 16 Aril 2018. Available at https://www.dailymaverick.co.za/article/2018-04-16-when-guardians-refuse-to-be-guarded-or-the-curious-case-of-one-arthur-fraser/

160 Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector Including Organs of State Report: Part V Vol. 1: State Security Agency, and Crime Intelligence, par 374 pp 151-152.

regulations governing security clearance for the IG and the staff of their office had been drafted, they were not promulgated. Thus, the same regulations pertaining to the security clearance of the members of the SSA were applied to the IG and OIGI staff. As a result, the latter regulations empowered the Director-General of the SSA to unilaterally revoke the security clearance of the IGI or OIGI staff.[161]

During his testimony before the State Capture Commission, Dr Dintwe also detailed how vetting was weaponised by the SSA for the benefit of its own members. This weaponisation extended beyond his own office to the Independent Police Investigative Directorate, as well as the National Director of Public Prosecutions. Thus, vetting can be weaponised by the intelligence services to insulate themselves from criminal investigations, further rendering the IGI and the JSCI toothless.[162]

The issue of vetting and security clearance also potentially extends to the JSCI. Like the IG, members of the JSCI depend on the State Security Agency for their security clearance, meaning that members' admission to the JSCI could be delayed as a result of not being granted a security clearance.[163]

The power of intelligence services to vet the elected public representatives that oversee them, can have devastating consequences on intelligence services, as was illustrated in the United States in the post-9/11 era.

John Kiriakou was employed by the United State's Central Intelligence Agency (CIA) from 1990 to 2004, initially as an intelligence analyst and then as a foreign counterterrorism operations officer. Kiriakou turned whistleblower against the intelligence community, but was sentenced to two and a half years in prison after he was indicted under the Espionage Act. In a 2022 interview[164] with veteran investigative journalist Chris Hedges, Kiriakou discussed the impact of the CIA's global secret operations in the post-9/11 era. He explains how, following the September 2001 bombings of the Twin Towers in New York City, legislation and practices pertaining to security and intelligence services changed drastically, thus allowing for the CIA to turn into the president's personal international assassination squad.

Kiriakou further explained that, post 9/11, congressional oversight (the US's equivalent of South Africa's parliamentary oversight) of the CIA degraded to such an extent as to become completely ineffective. Said Kiriakou:

> *"Now, we've got these oversight committees that really act as little more than cheerleaders for the CIA. It's up to these members of Congress to tell the CIA: 'No, you can't do that. No, you can't have a torture programme, or an illegal rendition programme, or an archipelago of secret prisons around the world. You can't transform yourself without Congressional approval into a paramilitary*

161 Ibid. par 377 p153

162 Ibid paras 376 -390 pp 152-168

163 Mayibongwe Maqhina *"Intelligence standing committee gets one member, but still short of another to quorate"* Independent Online. 4 May 2023. Available at https://www.iol.co.za/capetimes/news/intelligence-standing-committee-gets-one-member-but-still-short-of-another-to-quorate-7e63e5a1-f980-4fc9-9cda-56ab7a05d729

164 Interview with John Kiriakou *"We don't need the CIA"* The Chris Hedges Report. 12 August 2022. Available at https://youtu.be/vhyQRc1vzkg?s

organisation, you can't set up an assassination squad that travels around the world to just carry out hits on people whose politics you don't like.'

"The consequences of removing real oversight – true oversight – is that you end up with a rogue organisation. The nature of the CIA is to push the envelope. The nature is to see what it is that they can get away with, on the one hand. On the other hand, the nature is to try and recruit these members of the oversight committees, to make them feel like they are one of the guys: they're part of this secret team, they're insiders, everybody's working together. And that way you can get away with things that you otherwise wouldn't get away with or wouldn't attempt. That's not what the role of the oversight committee is supposed to be. The role of the oversight committee is to say: 'You can't do that because it's ***illegal****.'" (Kiriakou's emphasis)*

Underpinning this weakened role of the congressional oversight committees, Kiarkou explained, is the fear of committee members of having their security clearance revoked by the very services they are supposed to oversee. On one occasion, Kiriakous said, he confronted a member for the Senate Intelligence Committee for not supporting him once he became a whistleblower. According to Kiriakou, the member became agitated and responded to him as follows: "*Look, it takes all my energy just to not lose my security clearance.*"

The weaponisition of vetting within the SSA is not the only vetting-related issue in the Agency. One cannot discuss the weaponisation of vetting without taking into consideration the broader context of a vetting system that has a history of irregularities and failures and backlogs[165]. Testimony emerged before the State Capture Commission that parallel, irregular vetting procedures had been established during the state capture years, ostensibly to fast track security clearance for certain persons who would facilitate state capture.[166] The HLRP also identified several shortcomings in the vetting system, including an overly broad vetting mandate and a lack of an electronic vetting application system (which could aid the reduction of the perpetual vetting backlog). The Panel recommended that the Agency undertake an urgent security vetting policy review. [167]

The result of these shortcomings in the vetting system, is that the right people do not get vetted at the right time, thus creating a risk to the country's security and safety.

Recommendations

a) The Bill must be amended so that recommendations for intelligence vetting processes as set out by the HLRP of 2018 are implemented. For the sake of convenience, we will reiterate them here:

"An urgent policy review of the Agency's security vetting mandate be undertaken to consider the scope and reach of that mandate and to clearly identify the division between the normal probity checks of existing and prospective state employees to be undertaken by the employing

165 Parliamentary Monitoring Group. Update by State Security Agency on the vetting of Eskom officials; with Minister and Deputy Minister 30 November 2022. Available at https://pmg.org.za/committee-meeting/36193/

166 Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector Including Organs of State Report: Part V Vol. 1: State Security Agency, and Crime Intelligence, p304

167 HLRP Report para 7.3.6 pp 43-44 and para 7.5 (e)(f) p46

departments and the more focused security competency vetting to be undertaken by the SSA. The SSA should, as a matter of extreme urgency, resource and give priority to the further development and upgrading of the electronic vetting system to its full intended functionality."[168]

b) Furthermore, in order to ensure that vetting is not weaponised, the Bill must provide for clear safeguards against weaponisation of the vetting procedures. These safeguards must be made clear in the legislation; waiting for the Minister to issue regulations has not served the intelligence community well in the past. This was made evident by Dr Dintwe's testimony that dedicated vetting regulations for the IG and their office staff were never promulgated.

c) We strongly recommend that the Bill make provisions to ensure that the director-general (or any other member of the services with sufficient authority) is prevented from unilaterally revoking the security clearance of the IG (or of a member of the JSCI , Auditor General, IPID, the NPA, or any other investigative authority, for that matter). The HLRP panel learned during its inquest that the erstwhile South African Secret Service (SASS) was responsible for the vetting of its own members, and in fact had established a vetting panel which reviewed vetting outcomes. This practice was eliminated by the SSA, "leaving decisions up to individuals and their chain of command". [169] This was cemented by the promulgation of the Intelligence Services Regulations of 2014, which placed the decision making-power over final vetting outcomes firmly in the hands of the SSA's director-general.[170]

d) The Bill should provide for the establishment of a separate vetting agency within the intelligence community, with its own director general or head, on par with the directors-general and heads of the intelligence services and entities. In other words, the vetting agency needs to be an automonous agency within the intelligence community, with its own budget, staff, financial systems, mandate, and operating procedures (in the same manner as any other service or entity).

e) Within the vetting agency, there should be a vetting appeals department or unit to oversee the vetting processes (including investigations, decision-making, and outcomes) conducted by intelligence services.

e) As the name clearly states, this oversight conducted by the vetting appeals department should occur primarily through the establishment of an appeals process; the appeals department should be responsible for considering appeals in cases where people object to their security clearances being revoked, degraded or withheld. Under no circumstances should the final decision of the outcome of any appeals rest with the Minister responsible for the intelligence services or the members of the intelligence services/vetting agency that originally conducted the security competence test. Those facilitating the appeals process *cannot* be the same persons who conducted the initial vetting investigations and made recommendations pertaining to the appellant's security clearance status.

f) The Bill must make provisions to ensure that the vetting agency and its appeals department's decisions should be immune from interference by the executive and high ranking members of the services.

---

168 Ibid.

169 Ibid.

170 "Intelligence Services Regulations, 2014" Government Gazette. 29 January 2014. Available at https://www.gov.za/sites/default/files/gcis_document/201409/37280rg10103gon63.pdf

g) Anyone who is of the view that their security clearance has been revoked, degraded, withheld or unreasonably delayed, must be allowed to lodge an appeal with the appeals department. This also pertains to those who believe that the status of their security clearance has been altered in order to retaliate against them (for instance, in order to sabotage whistleblowers, or stifle investigations into the intelligence services or entities, or because an individual is perceived as a threat to whatever actions – illegal or otherwise – a certain member or members of the services plan to carry out).

h) If security clearance is denied, reasons[171] for such clearance must be provided by the vetting agency, in writing, with all supporting documentation, within a reasonable period of the official issuance of the denial, revocation or degradation of such clearance. These should form part of the appellant's appeal to the appeals department,[172] along with additional information and documentation supporting the appellant's case as to why security clearance should not be denied, revoked or degraded.

i) Should the appeals department deny the appeal, reasons should again be furnished to the appellant in writing, with all supporting documentation. The appellant should then be allowed to respond to these reasons in writing, within a reasonable time frame, should they wish for the appeals department's decision to be reviewed. Such a review could then be undertaken by legal council and a designated, standing appeals review committee or panel, and that committee or panel's final decision should be taken in consultation and concurrence with said legal council. [173]

j) The Bill should stipulate the maximum time period for providing the applicant with the outcome of:

xii. the initial vetting investigation;

xiii. the appeals departments' decision; and

xiv. the appeals department review committee/panel's final review outcome.

k) If the application is rejected by the appeals department review committee, that applicant should then be allowed to apply to the court[174] to have the revision overturned.

l) An applicant who suspects that their security clearance has been revoked, degraded or denied in retaliation against them for whatever reason, must retain the right to lodge a complaint with the Inspector General of Intelligence. A complaint with the IG and an appeal with the appeals department may be initiated simultaneously.

---

171 See for instance the case of Romania in "Thematic Brief: Vetting Members of Parliament" Geneva Sector for Security Sector Governance. 2021. Available at https://www.dcaf.ch/sites/default/files/publications/documents/VettingMembersParliamentsMar2021.pdf

172 See for instance National Security Law Firm. "*Overview of the Security Clearance Appeals Process for Military, Civilian, and Government Contractors"* as at 6 February 2024. Available at https://www.nationalsecuritylawfirm.com/security-clearance/security-clearance-denial-appeals/ See also Dunlap, Bennett and Ludwig *"Resolving a Security Clearance Revocation".* n.d. Available at https://www.dbllawyers.com/resolving-a-security-clearance-revocation/

173 Ibid.

174 See for instance General Intelligence and Security Service of the Netherlands (Ministry of the Interior and Kingdom relations) "The security screening". n.d. Available at https://english.aivd.nl/topics/security-screening/the-security-screening

m) The Evaluation Committee must ensure that all aspects of vetting, the vetting agency, and the appeals department are included in their quarterly reviews of the intelligence community. Similarly, the JSCI must include in their end-of-year review all aspects of vetting, the vetting agency, and the appeals department.

n) JSCI, the Evaluation Committee and the IG must be empowered to, of their own accord and at any time, launch ad hoc investigations into vetting, the vetting agency, and the appeals department, and must be empowered to make legally binding recommendations following such ad hoc investigations. All three bodies must also be empowered to open a criminal or civil case based on the outcomes of an ad hoc investigation, and to turn to the courts in their efforts to have their decisions and recommendations upheld.

m) Finally, for the above to be realistically implementable, it is necessary to develop clear, publicly available legal requirements for what constitutes sufficient grounds for the denial, revocation, or downgrading of one's security clearance status. To this end, the Bill fails miserably.

Currently, the some criteria for vetting are stipulated in Minimum Information Security Standards (MISS). Revoking, degrading, or withholding security clearance are determined by a *"person's ability to act in such a manner that he does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the security or interests of the State. Security competence is normally measured against the following criteria: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behaviour, and loyalty to the state / institution".*

These 'criteria' are further expanded upon by the Intelligence Services Regulations of 2014. They include[175]:

- Criminal offences and misconduct
- Use of dependency coming substances
- Financial considerations
- Behavioural disorders
- Citizenship and/or foreign influence and
- Loyalty to the constitution

These criteria are overly broad and vague, and as matters stand their meaning, in practical terms, is determined by a single, extremely powerful official: the Director-General of the SSA. The Bill in its current state does not remedy this situation sufficiently. We therefore recommend that these criteria be clarified and operationalised in such a manner that a panel, legal council and court can discern whether or not said criteria were in fact justifiably applied to revoke, degrade, delay or withhold security clearance.

n) Finally, vetting procedures need not be immune to external scrutiny, and the Ad Hoc committee should consider introducing such a mechanism to oversee the way in which the intelligence

175 *"Intelligence Services Regulations, 2014"* 3(1) Government Gazette p 77. 29 January 2014. Available at https://www.gov.za/sites/default/files/gcis_document/201409/37280rg10103gon63.pdf

services conduct vetting. In the United States, for instance, the Federal Bureau of Investigation has a vetting programme to establish the legitimacy and trustworthiness of its 'confidential human sources'. In 2019, the US Department of Justice issued a public report in which it detailed the outcome of its investigation into the FBI's vetting programme of its sources, and identified numerous issues with that programme (including backlogs, lack of controls for validation of information, and lack of safeguarding source communications).[176]

176 *"DOJ OIG Releases Report on the FBI's Management of its Confidential Human Source Validation Processes"* U.S. Department of Justice, Office of the Inspector General. 19 November 2019. Available at https://oig.justice.gov/news/doj-oig-releases-report-fbis-management-its-confidential-human-source-validation-processes

5. NICOC

Regarding NICOC, the HLRP found that "urgent measures should be put in place to ensure compliance by the intelligence services with the White Paper and legislative prescripts on intelligence coordination with consequences for non-compliance". The Panel also found that the SSA's Strategic Development Plan of 2017 ignored crucial functions of NICOC, which is to provide National Intelligence Estimates. The panel stated in its report[177]:

> *"One aspect of the SDP that arouses concern is that it appears to completely ignore the role of NICOC in providing intelligence estimates and assessments to government by collating the information from all the intelligence services as well as other government departments and external experts. The implication of the SDP is that the SSA seems to abrogate this role largely to itself. There is no mention of NICOC in its thinking."*

Based on the issues [178]identified by the HLRP, as well as the briefing delivered to the Ad Hoc Committee on GILAB by the Intelligence Coordinator of NICOC[179] we make the following recommendations for the Bill's provisions.

a) In the State Capture era, NICOC was moved to the Ministry of State Security, despite the fact that the Crime Intelligence Division of the SAPS and Defence Intelligence (and thus their respective ministries) stand on equal footing with the SSA in terms of NICOC. This is not tenable. The Bill must ensure that NICOC and the Office of the Intelligence Coordinator is located outside of these ministries.

b) The Bill must provide for an Office of the Intelligence Coordinator of NICOC, for such an office to be established as a fully fledged organisation, and for powers of the Intelligence Coordinator. This is to ensure that NICOC can carry out its work as per existing legislation, without having to manage it, as the HLRP put it, "through some sort of consensual decision-making". In this regard, as is the case with the OIGI (see section 4.3.3 above) , alternative institutional form must be provided for in the Bill to ensure for the independence and autonomy of NICOC.

Regardless of the institutional form adopted, the bill must, at the very least, ensure the following:

c) The Intelligence Coordinator must be made the Accounting Officer of NICOC

d) The Office of the Intelligence Coordinator must be empowered by the Bill to allocate funding resources as it sees fit, without permission or interference from the intelligence services (including persons currently operating the spending centres of the SSA)

e) In line with this, Office of the Intelligence Coordinator must be given full authority to determine its organisational structure, staff gradings, and whom it appoints and promotes

177 HLRP section 6.3.2 p37

178 HLRP pp84-88

179 *Briefing by the National Intelligence Coordinating Committee on its input into the General Intelligence Laws Amendment Bill*. 5 December 2023. Available at https://www.youtube.com/live/NZLnCYt4nuc?si=HYyM9IqGLM5SHiw1

(and in which positions) without interference from the intelligence service structures or the executive.

f) The Bill must ensure that analysts of the Office of the Intelligence Coordinator are empowered to fully access and consult all government departments, academics, think tanks, research bodies and civil society organisations (governmental or non-governmental) *of its choice*, should it require additional knowledge to fulfill its functions. This must be adequately budgeted for.

g) The Office of the Intelligence Coordinator must have full access to any classified information it requires to carry out its work. The Office of the Intelligence Coordinator must be responsible for identifying what classified information is requires in this regard.

h) Under no circumstance should any person (including members of the executive or of the services and entities) be allowed to withhold information, classified or otherwise from Office of the Intelligence Coordinator. A failure in this regard should result in criminal penalties for perpetrators.

i) As is the case with the OIGI, the budget for the Office of the Intelligence Coordinator must be adequate. At the very least, if the Office of the Intelligence Coordinator is funded through the intelligence services' cost centres (although this is not recommended), the budget of Office must be ring-fenced as part of the larger budget allocation to the services and entities by parliament. Again, as with the OIGI, the Bill should stipulate a minimum fixed percentage of the entire budget to be allocated to the Office of the Intelligence Coordinator.

j) Upon reviewing the budgets of the intelligence community, considering the budget proposal of the Office of the Intelligence Coordinator, and through direct and face-to-face consultations with the Office of the Intelligence Coordinator, the JSCI must decide to allocate funding over and above that of the said fixed minimum percentage. This decision must be determined by the relative workload of NICOC and the Office of the Intelligence Coordinator, when considered against the scale of the intelligence services and entities' operations and functions.

k) The Bill provides that the new South African Intelligence Agency should "provide periodic national security briefing to the Joint Standing Committee on Intelligence, members of Cabinet, Premiers, Parliamentary Presiding Officers and the Chief Justice".

We disagree with tasking the Agency with such a briefing to Cabinet. This provision blatantly disregards the crucial role that NICOC and the Intelligence Coordinator plays in synthesising the intelligence products of all intelligence services, and then acting as the link between the intelligence community and the parties it is tasked to keep informed on national security matters. In fact, it would be preferable for briefings to all of the relevant entities to be provided by NICOC in order to ensure an clear, coherent and comprehensive overview of intelligence that is informed by all the intelligence services bound to the various ministries. We therefore recommend that the Bill be changed to provide for NICOC to provide such briefings.

l) The Bill must allow NICOC to co-opt (through unanimous agreement) any role player required to fulfill their functions. Such a role player must have adequate security clearance.

6. The prevention of interference with oversight processes

Recommendations

The Bill Must provide for the prevention of interference with the work of the JSCI, OIGI, the Evaluation Committee, NICOC, and entities and persons conducting extern or internal criminal or civil investigations into the intelligence services and entities.

To this effect, the bill must provide for criminal penalties for any attempt to interfere with the functions of the OIGI. It must provide adequate definitions of what constitutes such interference, and the law should apply to any person guilty of interference, including members of the executive, the services and entities.

7. Secret Accounts

The Bill does not address the issue of the secret accounts from which intelligence agencies are currently funded. This needs to be rectified, given the role the looting of the accounts played during the State Capture years, as became evident during the Zondo Commission hearings.

For our recommendations pertaining to the secret accounts, see Annexure 2 'Secret funding and the State Security Agency: holding intelligence services accountable' (2023)

ANNEXURE 1: The Future of Bulk Interception and digital communication: Issues and policy options

Available at: https://intelwatch.org.za/2024/01/31/policy-brief-the-future-of-bulk-interception/

ANNEXURE 2: Secret funding and the State Security Agency: holding intelligence services accountable'

Available at: https://intelwatch.org.za/wp-content/uploads/2023/07/Report-Secret-Funding-SSA-accountability-2023.pdf