NATIONAL & WESTERN CAPE
107 Community House
41 Salt River Rd
Salt River, Cape Town
Tel: 021 447 1000
Admin@r2k.org.za
WesternCape@r2k.org.za

KWA ZULU NATAL
101 Dinvir Centre,
121 Field (Joe Slovo) St
Central, Durban
Tel: 031 301 0914
KZN@r2k.org.za

GAUTENG
5th floor, Heerengracht Building
87 De Korte St
Braamfontein, Johannesburg
Tel: 011 339 1533
Gauteng@r2k.org.za

Supplementary Submission to SABC inquiry
Concerns of Communications Surveillance and State Security Abuses at the Public Broadcaster

16 January 2017

Following Mr Micah Reddy's appearance before the Committee on 14 December 2016, the Committee asked Right2Know to give supplementary information about concerns of the State Security Agency's (SSA) conduct at the South African Broadcasting Corporation (SABC). This brief supplementary submission will outline: (1) Concerns of communications surveillance of SABC employees, either by SABC management or a third party; (2) The SSA's conduct at the SABC; (3) Recommendations for further view and reform.

The clandestine nature of state-security activities, and the extreme lack of transparency of the State Security Agency even in matters of overall policy and non-sensitive operational activities, has undermined public understanding and oversight of this issue. Similarly, the lack of candour from SABC's leadership means that the full picture of exactly what was taking place at the SABC has yet to be fully understood.

However, as this submission will recount, the evidence that is available suggests there are serious causes for concern regarding the conduct of both the SSA and SABC management regarding investigations and scrutiny of SABC employees, which has greatly contributed to a climate of fear and self censorship at the public broadcaster.

It should also be noted that from early 2015 to the end of 2016, there was no Inspector General of Intelligence, meaning that SSA operations have not been subject to basic

independent oversight and individuals prejudiced by their actions have had no recourse.

1. Interception of Employee Communication at SABC

The spectre of communications surveillance ("phone-tapping" and "email-tapping") has become a regular feature of scandals surround the SABC.

The need to protect against communications surveillance at the SABC is at least three-fold. First, it is vital in any context to protect the constitutional right of any person to private communications; any interference with that right can only be justifiable in the narrowest possible contexts. Second, in the context of a media organisation, protecting the integrity and confidentiality of journalists' communications with or about sources must be given the highest possible protection, in keeping with a basic tenet of media freedom and the protection of journalistic sources. In the context of a media organisation that has been subject to internal censorship pressures, protecting journalists' communications is especially important. Third, given the clear pattern of maladministration, mismanagement and abuse of power in the upper echelons of the SABC, the interception of employee communications poses a grave threat to whistleblowers[1].

Despite this, there have been a number of problematic incidents that suggest, at best, employee communications are not adequately protected against interception; at worst, that SABC staff may be subject to unlawful interception of communications. Some of these are outlined below. As the Committee is aware, such interception would have to be governed by the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). Right2Know has raised a range of concerns about the constitutionality of RICA, including its lack of transparency and lack of safeguards[2]. For brevity's sake these will not be detailed in this submission, except to note that even interceptions that occur in terms of RICA may not be properly lawful, justifiable or adequately guarded against abuse.

A few specific incidents have been highlighted, in the main dealing with evidence of communications surveillance either being threatened or actively used against SABC

1 Right2Know could not establish if the SABC has any specific code or policy to promote and protect whistleblowing.

2 R2K memorandum, 26 April 2016, online: http://www.r2k.org.za/2016/04/26/memorandum-demands-to-stand-against-surveillance-and-fix-rica/

employees by those in a leadership role at the public broadcaster.

1.1. SABC chairperson statement in 2014

In January 2014, then SABC chairperson Zandile Ellen Tshabalala reportedly told staff in an editorial meeting that their communications may be intercepted by intelligence services, apparently in relation to perceived information leaks. This incident was made public by representatives of the Broadcasting, Electronics, Media and Allied Workers' Union (Bemawu) at the time, and reported to the Committee in Ms Thandeka Gqubule's submission[3]. According to accounts at the time, Ms Tshabalala incorrectly cited the SABC office's status as a National Key Point to justify possible interception of communications[4].

While the inferred risk of spying on SABC employees is problematic on its own, it is worth noting as an aside that the National Key Points Act gives no special justification for communications interception. In recent years there have been several public examples of SABC management falsely invoking the National Key Points Act to justify lack of transparency, candour and due process in human resources and governance issues, simply because several SABC offices that have National Key Points status.

1.2. Employee contracts on interception of communications

Evidence has come to our attention of changes to the wording of at least some manager-level contracts to broaden the SABC's discretion to intercept and "act on" the electronic communications of employees. Right2Know has studied a manager's contract signed within the past two years which requires the Employee:

> "to consent the SABC to intercept, monitor, read, block or act upon any of the Employee's electronic and other communications which shall include, but not be limited to, telephone conversations, emails and any stored files."

This appears to be an expansion of the SABC management's discretion to intercept employees communications, including personal communications, as the clause did not occur in manager-level contracts from previous years obtained by Right2Know.

1.3 Investigation of SABC Parliament employee, 2014

3 Testimony of Ms Gqubule, Ad Hoc Committee on SABC Board Inquiry hearing, 12 December 2016
4 R2K & SOS statement, 13 April 2014, online: http://www.r2k.org.za/2014/04/13/open-letter-to-sabc-chair-on-the-national-key-points-act/

The Committee has already heard testimony on the matter of a member of SABC's Parliamentary office who was suspected of 'leaking' information to a Member of Parliament in late 2014[5]. Right2Know understands from a person familiar with the investigation that the employee's laptop was confiscated by two individuals identifying themselves as representatives of SABC's IT department and forensics department, and this device was in the possession of SABC forensics for several weeks without explanation. At a later stage, the employee was interrogated by representatives of the SABC's forensics, and eventually cleared of wrongdoing. As to how the employee came under suspicion, it appears to have involved interception and tracing of the employee's communications. Aside from the significant distress caused for the employee, the incident speaks to a climate of extreme paranoia and willingness to violate workers' privacy and other rights to clamp down on perceived dissent.

1.4 Lack of adequate policies to safeguard against unlawful retention and interception of communications

While it is unclear how many contracts contain the above mentioned clause, Right2Know did speak to several SABC workers whose contracts from several years ago did not contain this provision. When R2K sought to assess the provisions of the SABC's email retention policy, we discovered that the SABC does not have an adopted email policy – there is a draft policy on "Electronic Communication" (TE002/02), dated September 1998, which appears never to have been adopted[6] (attached as Appendix 1 to this submission). In any case, this draft policy lacks necessary details, such as whether emails sent through the SABC servers are retained, and if so for how long, and in what circumstances if any they could be searched or used in an investigation, and by whom. This means there are no internal stipulations that guide or restrict how SABC employees' electronic communication may be monitored and intercepted.

However, it does also mean that if employees have not *opted into* an agreement to allow their employee to intercept their communications (however problematic such an agreement may be), any interception of their communication by management may be unlawful in terms of RICA, and may constitute a form of covert intelligence gathering. In terms of the National Strategic Intelligence Act 39 of 1994, no organ of state other than the intelligence agencies may develop a covert intelligence capacity.

5 Testimony of Mr Calata, Ad Hoc Committee on SABC Board Inquiry hearing, 12 December 2016
6 Communication with an SABC spokesperson to seek confirmation of this did not receive a response.

It should also be noted, and which is further discussed below, that the National Strategic Intelligence Act authorises the State Security Agency to intercept communications as part of security clearance investigations – again, only if such interception is undertaken subject to the restrictions in RICA.

2. SSA conduct at the SABC

The State Security Agency's vaguely defined and expansive role in supporting and intervening in security-related matter at public bodies, including but not limited to security vetting, has contributed to a climate of fear at the public broadcaster and created substantial risk of abuse and clampdown. Effectively, in these matters, SABC managers handed over control of governance to the state security structures.

2.1 SSA role in security vetting

It is evident that the State Security Agency's role in vetting SABC employees and directors is a subject of controversy. The Committee has already received testimony from SABC employees raising concerns about the SSA's role in security vetting at the SABC, and SABC employees have raised such concerns in numerous media reports as well[7]. This concern has also been raised in direct engagements between Right2Know and union representatives of SABC employees, and various SABC employees themselves.

The National Strategic Intelligence Act 39 of 1994 mandates the State Security Agency to conduct security vetting investigations for any person employed or applying to be employed to any organ of state. Such an investigation may extend to a startlingly wide range of information about a person, including criminal and financial records, as well as personal information and "any other information that is relevant". The methods for such an investigation may include invasive measures such as a polygraph test or interception of private communication, subject to the provisions of RICA. Vetting procedures, through the Z204 security clearance form, subject candidates to other invasive processes, such as requiring disclosure of candidates' sex life and identity of partners, and requiring candidate's therapists to provide a written report of their mental health (a possible breach of patient confidentiality).

7 For example, City Press 27 November 2016, and Sunday Times 23 November 2016.

The vetting system sets up a one-sided and fundamentally unequal process; the Act gives full discretion to the SSA to determine the scope and methods of such investigations, and make its own findings, and strips the employee and public body itself of any role or say. A person whose security clearance is refused or withdrawn may only appeal to the Minister of State Security, but without necessarily having sight of the case against which they are arguing. Furthermore the Act stipulates that security-vetting regulations should not be published or released via Government Gazette, meaning that vetting teams are following a rulebook that only they can read.

It is a basic principle in international human rights law that invasive measures must be necessary and proportionate, and subject to maximum possible limitations. To say the least the National Strategic Intelligence Act lacks appropriate limitations and safeguards against over-reach in security vetting processes.

2.2 SSA unexplained operation in SABC Durban office in 2015

In August 2015, Bemawu received complaints from members at the SABC Durban office that SSA officials had "instructed employees to leave their offices whereafter operators spent between two and three hours per office for a purpose unknown to the employees."[8] According to the initial complaint, employees were threatened against discussing or reporting the incident. While it has been speculated that this operation may have related to interception of communications, to date there has been no explanation of this incident.

2.3 SSA 'investigation' of leaks in 2015

The Committee has already heard testimony on the SSA's investigation of several senior managers at the SABC at the behest of management. Those identified as the targets are Messrs Itani Tseisi, Henk Lamberts, Angus Summers, and Andries van Dyk. Ms Mandiwe Nkosi's testimony to the Committee supported the view that this investigation was aimed at identifying the source of leaks of financial information at the SABC; in other words, the SSA was enrolled in an operation to identify whistleblowers within the SABC, reportedly at the behest of Mr Hlaudi Motsoeneng[9]. Mr Tseisi has subsequently reported that an SSA official questioned him on his testimony to the Public Protector's inquiry into Mr Motsoeneng's

8 Bemawu head office letter to Frans Matlala, 25 August 2015
9 Ad Hoc Committee on SABC Board Inquiry hearing, 9 December 2016

appointment[10].

The same article reports that another employee under investigationhad his laptop confiscated and wiped of all data. It remains unclear why the SSA had become involved in an internal matter. While the operation has been defended as being in line with the SSA's mandate to provide security-related services to other government departments, in terms of the National Strategic Intelligence Act, as with security-vetting matters, this mandate is at best vaguely defined and not subject to appropriate limitations.

3. Recommendations

3.1 Investigation of SSA activity

We recommend that Parliament requests a full investigation by the Office of the Inspector General of Intelligence, to determine:

* The scope of all operations and activities of the State Security Agency at the SABC
* Who authorised these activities and to whom did they report
* Whether any SABC employees were subject to covert intelligence gathering or other invasive methods, and whether this was lawful.

This investigation should be conducted with maximum speed and maximum transparency, and the findings should be made fully public.

3.2 Steps to protect communication and private data of SABC employees

Given the need for specific protections of SABC employees' communications, both to protect whistleblowers and to protect journalistic freedom at the public broadcaster, the Committee's findings should include recommendations to overhaul SABC's policies on protecting electronic communication, as well as any whistleblower policy of the institution (or the urgent adoption of one).

In addition, we recommend a review of the role, powers, and internal checks of the SABC's internal investigations capacity (referred in Ms Mandiwe Nkosi's testimony to the committee as “internal audit[11]), to curtail any potential for internal investigations to target perceived 'dissenters' within the SABC or clamp down on critics.

10 Quoted in Sunday Times, 23 December 2016.
11 Testimony of Ms Nkosi, Ad Hoc Committee on SABC Board Inquiry hearing, 12 December 2016

3.3 Review of State Security Agency's role and powers in other public bodies

This submission touched briefly on concerns of the SSA's role in security vetting and other security-related matters per the National Strategic Intelligence Act. These roles are poorly defined in the Act and lack transparent and appropriate limitations and safeguards. This needs to be addressed urgently in a review, or the concerning practices which have spooked SABC workers will surely repeat themselves not only at the public broadcaster, but at other public bodies as well.

#Ends

For further information on this submission, please contact:

Murray Hunter
e: murray@r2k.org.za
t: 021 447 1000
m: 072 672 5468

APPENDIX 1 – SABC DRAFT ELECTRONIC MAIL POLICY

Policy No.	**TE002/02**

TITLE:	**ELECTRONIC MAIL**
CUSTODIAN AREA:	**TECHNOLOGY**
PREPARED BY:	SABC Internet Strategy Task Team
DATE APPROVED:	
EFFECTIVE DATE:	16 September 1998
APPROVED BY:	

1. Purpose

This document constitutes the official SABC Electronic Mail policy. The policy governs the conditions for access, usage and management of the SABC's internal and Internet electronic mail systems and services.

This purpose of this Policy is to ensure that:

1.1 Users of SABC electronic mail systems are informed about the applicability of SABC electronic mail policies and how privacy and security apply to electronic mail.

1.2 Electronic mail services are used in compliance with these policies.

1.3 Disruptions to SABC mail systems are minimised.

2. Position

The SABC encourages the responsible use of the *SABC's electronic mail* services to improve business communications and to share ideas within the context of the SABC's business goals and public service responsibilities.

Electronic mail services, including mail addresses and accounts associated with these services are the property of the SABC. These services are provided to authorised users primarily in support of the SABC's business activities.

3. Applicability

This policy governs the conditions for access to, and the usage and management of the SABC's internal and Internet electronic mail systems and services. The policy applies to all holders of *SABC electronic mail accounts*, authorised users, electronic mail administrators and managers.

4. Provisions

4.1 **Access** : Access to the *SABC electronic mail* services is provided as a business tool that may be wholly or partially restricted by the SABC without prior notice and without the consent of the electronic mail user when there is substantiated reason to believe that violations of policy or law have taken place. The SABC reserves the right to withdraw such services at any time.

4.1.1 Access to the SABC *Internet electronic mail services* shall be limited to authorised SABC personnel, contractors and SABC business units who require external electronic mail for business and public communications purposes. In addition, radio and television channels or individual programs may be allocated *SABC electronic mail* services for competition and related programme services.

4.1.2 Access to the SABC *internal electronic mail services* shall be available to all personnel, contractors and business units who require these services for business or workgroup related communications and have access to a suitable electronic mail terminal.

4.2 Responsibility and Accountability

4.2.1 Holders of *SABC electronic mail accounts* will be held responsible and accountable for all messages and attachments which are sent from their e-mail accounts, or received by their e-mail accounts and not deleted.

4.2.2 A non-individual business e-mail account will only be issued to the functional manager responsible for its use. Responsibility and accountability for all aspects of its use will rest with this manager.

4.2.3 All applicants for *SABC electronic mail* services will be expected to sign an agreement to abide by the terms of this policy as a condition of access.

4.2.4 The SABC reserves the right to record and inspect the source and destination addresses of all electronic mail messages originating from, and addressed to recipients on the SABC e-mail systems.

4.3 Acceptable Use

Every user of the *SABC electronic mail* services has the responsibility to maintain and enhance the SABC's public image and to use the services in a responsible and productive manner with normal standards of professional and personal courtesy and conduct.

4.3.1 The primary use of the *SABC electronic mail* service is for business purposes subject to the conditions of this policy.

4.3.2 Attachments must be limited in size to prevent overloading the mail system resources. The SABC reserves the right to limit the sizes of messages and attachments accepted by the service.

4.3.3 While subscriptions to *Mailing Lists* for automatic information updating is accepted electronic mail practice, users are expected to exercise reasonableness in terms of the volumes of information *uploaded* and to ensure that all obsolete subscriptions are cancelled.

4.3.4 All messages communicated on the *SABC electronic mail* systems must contain the name of the sender.

4.4 Unacceptable Use

The SABC electronic mail services may not be used for the following purposes:

4.4.1 Destructive and disruptive practices, which include, but are not limited to (i) the use of electronic mail services to send or forward e-mail chain letters, (ii) exploit *listservers* or similar broadcast systems for purposes beyond their intended scope, (iii) to amplify the widespread distribution of unsolicited e-mail, and (iv) *"Letter bomb",* that is to re-send the same electronic mail repeatedly to one or more recipients so as to interfere with the recipients' use of electronic mail

4.4.2 Transmitting, receiving or storage of any communications of a discriminatory or harassing nature, materials that are obscene, or which contain abusive, profane or offensive language.

4.4.3 Indiscriminate forwarding of mail for which permission has not been obtained from the originator.

4.4.4 The *SABC electronic mail* services are primarily for business purposes and may not be used to solicit or conduct business for personal gain.

4.4.5 The *SABC electronic mail* services may not be used for purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others

4.4.6 No electronic mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else from another organisation.

4.4.7 Users of the *SABC electronic mail* systems who obtain access to materials of other organisations may not copy, modify or forward copyrighted materials, except under the specific copyright terms and conditions.

4.5 Security and Confidentiality :

4.5.1 The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by unintended redistribution, or because of the inadequacy of current technologies to protect against unauthorised access. Users must exercise extreme caution in using electronic mail to communicate confidential or sensitive information.

4.5.2 The SABC has no control over the security of electronic mail that has been downloaded to the user's computer. As a deterrent to potential intruders and the misuse of electronic mail, users must make use of whatever protections, such as passwords, are available to them.

5. Policy Violations

Violations of SABC policies governing the use of electronic mail services may result in restriction to access. In addition disciplinary action may be taken in terms of the conditions of this policy, and/or other SABC policies and codes of conduct.

6. Supplementary Information - Cautions

Users of electronic mail should be aware of the following:

6.1 Both the nature of electronic mail and the public nature of the SABC's business make electronic mail less private than users may think. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. Furthermore, even after a sender or recipient deletes an electronic mail record it may persist on backup facilities.

6.2 All outgoing SABC Internet electronic mail messages contain a reference to the SABC as the originating company. Users must be aware that this may give the impression that the sender is representing, giving opinions, or otherwise making statements on behalf of the SABC, when in fact they are not appropriately authorised to do so. User's should when necessary include a disclaimer on outgoing messages to the effect that the views and opinions expressed are those of the sender and are not necessarily those of the SABC.

6.3 The SABC in general cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the SABC protect users from receiving electronic mail they may find offensive.

6.4 There is no guarantee, unless *authenticated* mail systems are in use, that electronic mail received was in fact sent by the purported sender. Furthermore

electronic mail that is forwarded may also be modified and therefore not represent accurately the contents of the original message. In case of doubt, receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

6.5 *Authentication* and/or *encryption* electronic mail technologies are not currently in use at the SABC.

7. Definitions

These definitions are provided for clarity and consistency in interpreting this policy. Wherever possible the industry standard definitions, or current usage of the terms are used. There may however be minor variations where definitions have been adapted to the specific circumstances of the SABC.

A comprehensive list of terms and definitions used in the SABC Internet policies, standards and supporting documents is contained in the Standards Document : ***SABC Internet Terms and Definitions*** which forms part of the SABC Internet Policy Documentation Structure.

Authentication : Any process that ensures that users are who they say they are. When you type your name and password, you are authenticated and allowed access.

Availability : When used in the policy header it defines the target group which may have access to the policy. Categories are either, *Restricted* or *Unrestricted*.

E-mail : Used interchangeably with electronic mail.

Encryption : The basis of network security. Encryption encodes network packets to prevent anyone except the intended recipient from accessing the data.

Internet Electronic Mail Services : Global electronic mail services on the public Internet.

Internal Electronic Mail Services : Electronic mail services, excluding the Internet mail services where both the source and destination of electronic mail communications are restricted to the SABC.

Letter Bomb : To re-send the same electronic mail repeatedly to one or more recipient's so as to interfere with the recipient's use of electronic mail.

Listserv Lists (or **listservers**) : Electronic discussion of technical and non technical issues conducted by electronic mail over *BITNET* using LISTSERV protocols. Internet users may subscribe to *BITNET* listservers. Participants subscribe via a central service, and lists often have a moderator who manages the information flow and content.

Mailing List : A (usually automated) system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the maillist. When you subscribe to a mailing list, you receive all mail sent to that list (see also Listserv).

SABC Electronic Mail : Proprietary internal, and external Internet electronic mail systems and services operated by the SABC.

SABC Electronic Mail Account : An electronic mailbox address issued by the SABC to an individual or business unit which uniquely identifies the holder as a user of the SABC electronic mail system.

SABC Internet Resources : Includes, but is not limited to all computing and electronic communications system hardware and software, services, publications and any other content directly or indirectly supporting the SABC's Internet services

Upload : The process of transferring information from your computer to another computer through the Internet.