Government Gazette

REPUBLIC OF SOUTH AFRICA

Vol. 472 Pretoria 20 October 2004 No. 26914

AIDS HELPLINE: 0800-0123-22 Prevention is the cure

GENERAL NOTICE

NOTICE 2277 OF 2004

MINISTRY FOR INTELLIGENCE SERVICES

In accordance with the obligations of the Electronic Communications Security (Proprietary) Limited ('Comsec') under sections 17(2) and 17(3) of the Electronic Communications Security (Proprietary) Limited Act, 2002 (Act No. 68 of 2002) ('the Comsec Act') I, Mr R Kasrils, Minister for Intelligence Services hereby make known to the heads of all organs of state the particulars of the procedure to be followed in submitting to Comsec's Board of Directors ('the Board') an analysis of the electronic communications security needs of the organ of state under such head's administration.

1. BACKGROUND

1.1. Section 17(2) of the Comsec Act places an obligation on the head of an organ of state to submit to the Board at its request an analysis of the electronic communications security needs of the organ of state under his or her administration. Failure to do so constitutes a punishable offence in terms of section 23(1)(b) of the Comsec Act.

1.2. In compliance with its obligations under section 17(3) of the Comsec Act, the request referred to in 1.1 must be made by Comsec within 6 (six) months of its incorporation on 20 April 2004, and thereafter, every two years.

1.3. The Board hereby requests all heads of organs of state to submit a response to this request by no later than the date stipulated in the covering letter referred to in 3.1 below ('the submission date') and in the format as prescribed herein.

2. OBJECTIVES OF THE SECURITY AUDIT

2.1. The core objective of Comsec in terms of section 3 of the Comsec Act is to ensure that critical electronic communications infrastructure of organs of state is protected and secure.

2.2. To this end, Comsec shall undertake a security audit to determine the electronic communications security status and needs of all organs of state. Priority will be given to the government security cluster and its entities.

2.3. Comsec may procure the services of external auditing and/or project management professionals to assist it with the needs analysis of electronic communications of organs of state, if such assistance will not jeorpadise national security and national interests of the Republic.

2.4. The first phase of the security audit entails an information-gathering exercise whereby a needs analysis in the form of a request for information contained in a questionnaire shall be distributed to all organs of state. This requires organs of state initially to provide a written response to a series of questions contained in the questionnaire. If necessary, Comsec will complement written responses to the questionnaire through either on-site or off-site interviews.

2.5. Upon receipt of the written responses to the questionnaire and/or on-site or off-site interviews, Comsec will perform a preliminary needs analysis of each organ of state. Should it so determine, Comsec shall conduct a more detailed assessment of the relevant organ of state's individual electronic security level, including but not limited to-

2.5.1. on-site inspections and testing of its current network, server and/or security infrastructure;

2.5.2. interviews with relevant officials within a particular organ of state regarding its security policies, procedures and standards, security management structure, and security custodianship, roles and responsibilities; and

2.5.3. any other methodology required for ascertaining the effectiveness of the network perimeter security,

to determine the electronic communications security systems, products and services and the functionality and interoperability levels of the products currently used by an organ of state

2.6. The second phase of the security audit involves an analysis of the information collected in the first phase. Each organ of state will be individually assessed based on its compliance with certain electronic communications security

requirements, which are to be modelled on international benchmarks. Once the analysis is completed, the project management team will submit its recommendation of the relevant organ of state's security needs to the Board.

2.7. In compliance with section 17(5) of the Comsec Act, the Board must consider the recommendation referred to in 2.6 and if the Board is satisfied that it should attend to the electronic communications security needs of a particular organ of state, it must conclude business level agreements with the relevant organ of state for the provisions of the necessary products and services.

3. NATURE OF THE REQUEST

The request comprises the following documents ('the request documents')-

3.1. a covering letter addressed to all heads of organs of state;

3.2. a questionnaire compiled by Comsec; and

3.3. this regulation, setting out the procedure and format of the response.

4. PROCEDURE FOR THE DISTRIBUTION OF THE REQUEST DOCUMENTS

4.1. The Chief Executive Officer, Comsec will provide each organ of state with the request documents on or before 20 October 2004, and thereafter, every two years.

4.2. The request documents will not be available in electronic format and any distribution thereof within the relevant organ of state will take place under the supervision of the head of the organ of state.

4.3. The request documents will be addressed to the head of the relevant organ of state who shall be responsible for ensuring that all information required for purposes of this security audit is kept strictly confidential.

5. PROCEDURE FOR THE COMPLETION OF THE REQUEST DOCUMENTS

5.1. The head of each organ of state shall upon receipt of the request documents identify the persons (including third party vendors) responsible for providing the relevant organ of state with electronic communication security products and/or maintenance and repair services. Thereafter, the head of an organ of state shall compile a list of such persons which shall be submitted to Comsec for purposes of conducting a security clearance of such persons.

5.2. Should Comsec approve the list of persons responsible for providing the services and/or products (after having obtained a security clearance certificate

issued by the National Intelligence Agency in accordance with the National Strategic Intelligence Act, 1994), it will promptly communicate this to the head of an organ of state, who will in turn instruct the relevant persons to commence answering the section(s) of the questionnaire to which their specialisation pertains.

5.3. Should Comsec decline any or all of the persons contained on the list referred to in 5.1 (after failing to have obtained a security clearance certificate issued by the National Intelligence Agency in accordance with the National Strategic Intelligence Act, 1994) it will communicate this to the relevant head of the organ of state and proceed with arranging a tele-survey or an on-site or off-site interview in the manner set out in paragraph 8.

5.4. The head of the organ of state shall ensure that the request documents shall be made available only to those persons within the relevant organ of state responsible for the provision of electronic communication security products and/or maintenance and repair services forming the subject of this security audit who have a security clearance certificate issued by the National Intelligence Agency.

5.5. Where no person within a particular organ of state is specifically designated to provide services and/or products, the head of the organ of state shall without delay inform the Chief Executive Officer, Comsec of same, and Comsec will proceed to make arrangements with the relevant organ of state to conduct either a tele-survey or an on-site or off-site interview in the manner prescribed in paragraph 8.

5.6. The person(s) responsible for completing the questionnaire (or any part(s) thereof) shall ensure that he or she provides Comsec with such detailed information so as to allow Comsec to adequately assess the security status of the relevant organ of state.

5.7. Comsec may establish a helpdesk to address telephonic queries from organs of state on the questionnaire in case of unclear or ambiguous sections or questions. To the extent that a particular section or question in the questionnaire is unclear or ambiguous, the head of the relevant organ of state or a person duly authorised by him or her, shall either address to the Chief Executive Officer, Comsec in writing (but not via e-mail) and in sufficient detail the particular query raised by the questionnaire or call the helpdesk for

assistance. The Chief Executive Officer, Comsec or a person duly authorised by him or her shall ensure that the relevant query is addressed adequately.

5.8. Should Comsec take longer than a period of 3 (three) days to resolve a particular query, the submission date shall be extended by such period taken by Comsec to resolve the query, commencing the date of receipt of the query by Comsec and terminating the date of communication of a resolution of the query to the relevant organ of state ('the extension period').

6. FORMAT FOR COMPLETING REQUEST DOCUMENTS

6.1. The head of an organ of state shall ensure that he or she submits to Comsec a completed questionnaire ('the response'), not later than six months from 01 November 2004, provided approval for an extended period is granted by Comsec.

6.2. To the extent that an organ of state provides Comsec with a written response to the request documents, such response shall be in type print (Paper: A4; Style: Arial; Font Size: 10), and shall be hand delivered to Comsec. Electronic documents shall be permitted provided they are delivered by hand to Comsec.

6.3. The response must be contained in a new document (not typed on the original questionnaire) and must clearly indicate the specific question number contained in the questionnaire to which it pertains.

6.4. Organs of state are required to complete every question contained in the questionnaire, and must not state in its response that a question contained in the questionnaire is "not applicable". Rather, organs of state must provide an explanation as to why a particular question does not relate to them specifically.

6.5. Organs of state are encouraged to provide with their response any documentation (written or electronic) that might supplement or clarify such response.

7. PROCEDURE FOR THE SUBMISSION OF THE REQUEST DOCUMENTS

7.1. The head of the organ of state must ensure that the response together with any supporting documentation (written or electronic) is returned to Comsec by the submission date and is completed in the prescribed format.

7.2. Organs of state shall be entitled to request in writing from Comsec an extended submission date, provided they motivate in detail the reasons for such extension, and provided further that they request such extended submission date no later than 1 (one) month prior to the initial submission date. Comsec shall ensure that it adjudicates such requests fairly and shall process and communicate its decision to the relevant organ of state timely.

7.3. Subject to any obligations under national legislation, Comsec acknowledges the sensitivity of the information contained in the response and any supporting documentation received from an organ of state and accordingly undertakes to ensure that these documents are kept strictly confidential and shall not be disclosed to any third party, without Comsec having entered into the necessary confidentiality agreements with such party.

7.4. All the responses must be hand delivered or couriered to Comsec and addressed to the attention of the Chief Executive Officer, Electronic Communications Security (Pty) Ltd, at:

138 Witch-Hazel
Cnr Peter & Witchazel,
Technopark, Centurion,
Pretoria.

The respondents will be notified of any changes in the delivery address should this occur.

7.5. Under no circumstances whatsoever must any response be submitted electronically to Comsec, unless the Chief Executive Officer, Comsec permits otherwise.

8. THE PROCEDURE FOR ON-SITE AND OFF-SITE INTERVIEWS

8.1. Where necessary, Comsec shall conduct either an on-site or off-site interview of the organ of state. This shall be arranged with the head of the organ of state at a time convenient to both parties.

8.2. An organ of state shall provide Comsec with reasonable access to their premises as well as all relevant records, data, and other such documents necessary for purposes of the security audit. Similarly, Comsec shall take all reasonable measures not to disturb or unduly interfere with the day-to-day operations of the relevant organ of state in conducting any on-site interview or inspection.

8.3. If after a preliminary needs analysis, Comsec decides to conduct any of the methodologies referred to in 2.5, the provisions of 8.1 and 8.2 shall apply *mutatis mutandis* to such methodology.

9. DEPARTURE

Comsec may as far as it is reasonable and in the interest of national security and national interests, depart or condone any departure from the procedure outlined in this regulation whenever, in its opinion, it is appropriate to do so.

10. INQUIRIES

10.1. Any written queries regarding the request documents or other inquiries must be addressed in writing to-

The Chief Executive Officer
Electronic Communications Security (Pty) Ltd
P O Box 37
Menlyn
Pretoria

11. OFFENCES

11.1 Any person(s) responsible for completing the questionnaire [or any part(s) thereof] who unlawfully disclose (s) or in any way divulges (either in writing or orally) any information required for purposes of this security audit to any third party not authorised by the head of the relevant organ of state, commits an offence and shall if convicted, be liable to the penalties listed in section 22 (2) of the Comsec Act, as determined by the Minister from time to time.

11.2 Any head of an organ of state who is guilty of an offence listed in section 23(1) of the Comsec Act shall if convicted, be liable to the penalties listed in section 23(2) of the Comsec Act.

11.3 Any person who fails to comply with the provisions of these regulations commits an offence and if convicted, shall be liable to a fine or one month imprisonment.

12. DATE OF COMMENCEMENT

These regulations shall be called "The Comsec Security Audit Regulations" and come into operation on 20 October 2004.