SCHEDULE C

DIRECTIVE FOR INTERNET SERVICE PROVIDERS IN TERMS OF SECTION 30(7)(a) READ WITH SECTION 30(2) OF THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, 2002 (ACT NO. 70 OF 2002)
(This Directive must be complied with within a period of six months from the date of publication hereof)

ARRANGEMENT OF CONTENT

PART 1: INTRODUCTORY PROVISIONS

1. Definitions

In this directive, unless the context otherwise indicates, a word or expression to which a meaning has been assigned in the Act has the meaning so assigned, and:

"Act" means the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002);

"applicant" means an appticant as defined in the Act;

"buffer" means the temporary storing of communication-related information in case the necessary telecommunication connection to route information to the IC is temporarily unavailable, and "buffered" has a similar meaning;

"client" means the ISP customer whose indirect communications are to. be intercepted, or whose real-time communication-related information is to be routed by the ISP to the IC, pursuant to a direction or request (synonymous to "interception target" or "interception subject").

"handover interface" means a pre-defined physical or logical interface across which the results of a direction or request are delivered between the ISP and the IC, as specified by the OIC;

"identity" means a technical label which may represent the origin or destination of any communications traffic, as a rule clearly identified by a physical: telecommunications identity number (such as a caller line identity number) or the logical communications identity number (such as an Internet Protocol address and/or Internet Protocol port number);

"Interception Centre" means an interception centre established in terms of section 32 of the Act and is herein referred to as the "IC";

"interception measure" means a technical measure which facilitates the interception of communications traffic pursuant to the Act;

"interception target" means the customer whose indirect communications are to be intercepted is to be routed by an ISP to the IC or provided to an interception applicant, pursuant to a direction or request;

"internet service" means connectivity or access to a public TCP/IP network and/or services layered over TCP/IP such as web, e-mail, file transfer, web mail, online chat and voice-over-IP (VoIP) telephony.

"internet service provider" means any telecommunication service provider providing internet services regardless of whether it has been issued with a licence under Chapter 5 of the Telecommunications Act, 1996 (Act No. 103 of 1996) or not, and is herein referred to as an "ISP";

"IPSec" means IP Secure, an industry-standard security protocol utilising modern data cryptographic techniques for the establishment of a secure tunnel;

"quality of service" means the quality specification of a communications channel, system, virtual channel, computer communications session, etc. "quality of service" may be measured in the case of an ISP, for example, in terms of latency or packet loss;

"result of interception" means the content of an indirect communication which is routed by an ISP to the IC pursuant to an interception directive or request;

"request" means a request in terms of section 7 of the Act;

"secure tunnel" means an encrypted and authenticated IP communication channel established using the most recently published versions of the IP Secure (IPSec), Transport Layer Security (TLS), or Secure Socket Layer (SSL) protocols;

"target identity" means the identity associated with an interception subject;

"target service" means a communications service provided by an ISP and utilised by an interception target and usually specified in a direction or request; for example, this refers to web (HTTP), e-mail

(SMTP, POP and/or IMAP); chat (JRC), news (NNTP), web-mail (Hotmail, Yahoo etc.) and others.

2. Application

This directive applies to and is binding on all telecommunication service providers providing internet services.

3. Statement Of General Duties

3.1 An ISP must provide a telecommunications service that has the capability to be intercepted in accordance with the provisions of the Act and this directive.

3.2 When a direction or request is presented to an ISP that ISP shall comply fully with the provisions of that direction or request for the period specified in such direction or request.

PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS

4. General requirements in respect of interception

4.1 An ISP must:

(a) provide a telecommunications service in respect of which the packets of all indirect communications can be duplicated and routed to the IC;

(b) apply software and/or hardware equipment on its telecommunication system to duplicate and route to the IC all indirect communications; and

(c) ensure that the applied software and/or hardware equipment is capable of identifying the targeted communication on the basis of:

- IP address;
- access login user name (e.g. RADIUS login);
- e-mail address (if hosted by the ISP); and/or
- telephone number or SIP URI (in case of VoIP).

4.2 In accordance with a direction or request an ISP shall ensure that:

(a) the entire content of an indirect communication associated with a target identity can be intercepted during the period specified within the direction or request; and

(b) checksum information on the results of interception is recorded, during the period specified within the direction or request.

4.3 The ability to intercept telecommunications shall be provided by an ISP in respect of all interception targets utilising its telecommunications system and in respect of all target services.

4.4 In so far as is technically and practically feasible, the results of interception relating to an interception target shall be provided by the ISP in such a way that any indirect communication that does not fall within the scope of the direction or request shall be excluded by the ISP.

4.5 All results of an interception of an indirect communication provided at the handover interface shall be given a unique identification relating to the direction or request,

4.6 After a direction or a request has been presented, interception of the indirect communications shall proceed in accordance with the Act, this directive and the direction or request.

4.7 The ISP shall, in relation to each interception target duplicate and route the packets of each successful establishment of an indirect communication to the IC.

4.8 In so far as is technically and practically feasible, the provisions of paragraph 4.7 shall also apply to multi-party or multi-way communications (eg. multicast), if and as long as the target identity participates in the multi-party or multi-way communications.

5. Unchanged state of service

5.1 In so far as is technically and practically possible, interception shall be implemented and operated in such manner that an interception target can not technically detect that he/she is being intercepted.

5.2 In so far as is technically and practically possible, interception shall be implemented and operated in such manner that no telecommunicating parties can technically detect that an interception target is being intercepted nor can they discern the targeting information used to implement the interception measure for that interception target.

5.3 In so far as is technically and practically possible, the aperation of the target service shall not be discernibly altered as a result of any interception measure and the operation of any other service shall not be altered as a result of any interception measure.

5.4 In so far as is technically and practically possible, the quality of service for the target's service shalt not be discernibly altered or degraded as a result of any interception measure. The quality of service of any telecommunications service other than the target's

service shall not be altered or degraded as a result of any interception measure.

6. Security requirements for interception

6.1 Information on the manner in which interception measures are implemented in a given telecommunication installation shall not be made available to unauthorised persons.

6.2 Information relating to target identities and target services to which interception is being applied shall not be made available to unauthorised persons.

6.3 To the extent that the ISP is obligated to consult on the manner in which interception measures are implemented in a given telecommunications or other technical installation with the designer, manufacturer, distributor, installer and/or other supplier of such telecommunications or other technical installations for the implementation of interception measures, such consultation shall be subject to appropriate confidentiality undertakings by the relevant designer, manufacturer, distributor, installer and/or other supplier.

6.4 The technical arrangements required within a telecommunication system to allow implementation of the interception measures shall be realised with due care exercised in operating telecommunication installations, particularly with respect to:

(a) the need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active;

(b) the restricting to a minimum, the number of staff engaged in implementation and operation of the interception measure;

(c) ensuring the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, by ensuring that interception provisioning is carried out only by authorised personnel;

(d) ensuring that the results of interception are delivered through a handover interface to the IC;

(e) preventing any form of unauthorised access to the handover interface shall be granted to unauthorised persons;

(f) appropriate measures to protect the handover interface against misuse;

(g) ensuring that the results of interception shall only be routed to the IC as indicated in the direction or request and ascertaining that proof of the authority to receive has been received from the IC, and ensuring that proof of the authority to send to the handover interface, has been furnished; authority to send will be in the form of a signature by the designated judge on the warrant or direction; authority to receive will be in the form of a Lawful tnterception ID (LIID) configured by the IC and indicated in the warrant or direction.

(h) authentication of each call set-up where switched lines to the IC are used;

(i) the use of encryption as specified in section 9 of this directive, and the use of additional encryption or other confidentiality measures to protect the routing of the results of such interception, at the cost of the IC, where this is specified in the directive or request;

(j) ensuring that handover interfaces support the use of encryption, authentication, integrity checking or other confidentiality measures specified in this directive and shall co-operate with applicants or the IC, or a person authorised by the IC, to implement such measures if required at the cost of the IC;

(k) preventing or tracing misuse of the technical functions integrated in the telecommunication installation enabling interception. In particular, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorised input, and the records shall cover:

(i) the target identities of the target service or target services concerned;

(ii) the beginning and end of the activation or application of the interception measure;

(iii) the IC to which the result of interception is routed;

(iv) an authenticator suitable to identify the operating staff (including date and time of input);

(v) a reference to the direction or request.

6.5 The ISPs shall take reasonable steps to ensure that the records referred to in paragraph 6.4(k) are secure and only accessible to specific nominated staff within their organisations.

7. Technical and functional requirements in respect of interception

7.1 The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure dictated within the direction or request.

7.2 The configuration of the handover interface shall ensure that it provides the results of interception.

7.3 The configuration of the handover interface shall be such that the routing to the IC of the result *of* interception provided at the interface can be implemented with industry standard transmission paths, protocols and coding principles.

7.4 Each interception target shall be uniquely associated with a single instance of the handover interface. (This could be achieved by the use of separate channels or unique interception identifiers).

7.5 The correlation between the indirect communication and communication-related information shall be unique.

7.6 The format for routing the intercepted indirect communications to the IC shall be an industry standard format.

7.7 ISPs must be able to route the intercepted indirect communications to the IC via a secure tunnel over circuit or packet switched connections.

7.8 The content of an indirect communication routed to the IC must include both incoming and outgoing content.

7.9 The IC will, within a reasonable period after the event, be informed by the ISP *of:*

(a) the activation of an intercept measure;
(b) the deactivation *of* the intercept measure;
(c) any change of the intercept measure;

(d) the temporary unavailability of the intercept measure due to link failure or faults on the ISP's side of the link;

(e) the temporary unavailability of the intercept measure due to software and/or hardware failure within ISP equipment supporting the intercept measure; and

(9 the temporary unavailability of the intercept measure due infrastructure failure resulting from a virus or denial of service attack on an ISP.

7.10 An ISP shall ensure that the configuration of the telecommunication system is such that it can implement and operate each interception measure with no or the minimum involvement of third parties.

7.11 Where an ISP makes use of any other telecommunication service provider's telecommunication system, both that ISP and that other telecommunication service provider must co-operate in the provision of interception, to the extent provided for in the interception direction.

7.12 To the extent provided for in the interception direction, an ISP must ensure that:

(a) any telecommunication service provider involved in the provision of interception Facilities is given no more information relating to operational activities than is strictly necessary to allow authorised target services to be intercepted;

(b) any telecommunication service provider involved in the co-operative provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorised target services to be intercepted.

7.13 When duplication and routing to the IC of the packets of an indirect communication is, in exceptional cases, not possible the remainder of the results of the interception shall nevertheless be duplicated and routed to the IC.

7.14 Where the special properties of a given telecommunication service, and the justified requirements of the applicant, necessitate the use of various identifying characteristics for determination of the telecommunications traffic to be intercepted, the ISP shall

ensure that the telecommunications traffic can be intercepted on the basis of the following characteristics:

(a) address information (physical and/or postal address);
(b) user name;
(c) subscriber name (in certain instances the subscriber is billed for the service and he/she may not necessarily use the service);
(d) e-mail address; and
(e) IP address and time stamp (time stamp indicating when the IP address was assigned) to the extent that an ISP has records of IP address assignment at that time.

7.15 In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear identification of the interception target.

7.16 The ISP shall ensure that more than one interception measure can be operated concurrently for one and the same interception target and service. Multiple interceptions may be required for a single interception target to allow monitoring by more than one applicant.

7.17 If multiple interceptions are active, an ISP shall take reasonable precautions to safeguard the identities of the applicants and ensure the confidentiality of the investigations.

7.18 The multiple interception measures, requested by different applicants, may require information according to different lawful directions or requests.

7.19 Each ISP must ensure that the indirect communications of multiple customers can be intercepted simultaneously at any given time in its telecommunications system, and all the results of interception routed to the IC. An ISP must be able to intercept a number of simultaneous individual targets equal to at least 2 in 25,000 individual customers, and a number of simultaneous corporate/organisational targets equal to at least 1 in 500 of such customers.

7.20 The arrangements made in a telecommunication system for the technical implementation of interception measures shall be set

up and configured so as to enable the identification and elimination, without undue delay, of bottlenecks and potential bottlenecks in a regional or functional part of that system when several interception measures are operated concurrently.

PART 3: DETAILED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS OF THE FACILITIES AND DEVICES FOR LAWFUL INTERCEPTION

ISPs are expected to abide by the following in terms of the functionality and security of the facilities and devices implemented to make their networks compliant to lawful interception (LI) requirements.

8. Facilities and Devices

8.1 The ISP is expected to install and maintain LI interception software, probes and any associated tapping devices. The interception devices must be positioned in the ISP network to ensure that:

- all network traffic to and from servers hosted by the ISP can be intercepted;
- all network traffic to and from access authentication servers hosted by the ISP can be intercepted; and
- all network traffic originating from or destined for an intercept target which is carried across the ISP's network links can be intercepted.

8.2 The ISP is expected to implement an# manage one or more interception provisioning terminal for lawful interception (LI) compliance purposes. These terminals must be sufficiently closely located on the network to the probes or devices being managed by them so as to ensure that the delay in provisioning an interception based on access login information is minimised.

8.3 Where necessary, the ISP must implement mediation device(s) for the collection from these probes and devices, normalisatian and delivery to an interception centre {IC) of intercept related information (IRI) tickets in the format specified within the technicat requirement section of this document.

9. Security Requirements

9.1 Interception provisioning terminals must be housed in areas with access controls implemented to limit access by authorised staff only. Provisioning terminals may be accessible remotely across a network, in which case an encrypted communication channel is to be used.

9.2 Logical access control must be implemented on the provisioning terminals; at minimum, a password that is changed monthly is required.

9.3 The provisioning terminal must be configured to provide detailed togs of both successful and failed access attempts to the terminal.

9.4 The provisioning terminal and mediation device must be secured through means of a network firewall. The rule set on the firewall must explicitly deny all externally originated communication sessions unless it is from the interception centre (IC).

9.5 The provisioning terminals should have appropriate virus protection, and the virus protection chosen should be updated as often as is reasonably possible.

9.6 The communication link between the mediation device and the IC for the delivery of intercept related information (i.e. H12) and intercepted content (i.e. H13) must be encrypted using an IPSEC based link encryption software or device working in ESP mode. The encryption atgorithm to be used is either 168-bit EDE mode Triple DES or 192-bit CBC mode AES.

10. Functional Requirements

10.1 The following minimum functions must be implemented within the ISP for LI purposes; the processes used to support these functions must be well documented and auditable at all times:

- Support of OIC in feasibility study phase i.e. provision on request of customer-related targeting information required for inclusion in the warrant or direction.
- Receipt of LI warrants and directions from the Office of Interception Centers (OIC) by means of either:
  - hand delivery; or
  - an electronically signed and encrypted form delivered by electronic mail or another messaging means to be determined in conjunction with the IC.
- Verification of the validity of the warrant or direction;
- Provision of the warrant or direction into the provisioning terminal as per the targeting and timing information provided in the warrant or direction; the electronic confirmation of the

activation of the warrant or direction to the IC through the mediation device;
- Administration of the physical and logical security and access control mechanisms implemented for this purpose;
- Any systems administration of the provisioning terminal, databases and mediation devices implemented at the ISP, which is requested by the IC;
- Reporting to the IC on security breach attempts and failed access attempts relating to the interception provisioning terminals; and
- Regular internal audit of security and operations implemented for LI purposes.

11. Technical Requirements

11.1 The result of interception must be transmitted from the ISP mediation device to the interception centre through a shared or dedicated IP connection over the Internet or via a direct circuit to the IC. The hardware, software and bandwidth costs incurred to support this connectivity from the mediation device will be borne by the ISP.

11.2 It is recommended that the ISP adopt specifications relevant to its network from the following documents; any deviations and option choices from specifications provided in these documents must be communicated to and agreed upon by the IC prior to implementation:

ETSI Technical Specification	Title	Description
TS 102 232	Telecommunications security; Lawful Interception (LI); Handover Specification for IP Delivery	Technical interface for mediation and handing over of intercepted IP traffic to an IC, including Voice-over-IP (VoIP)
TS 102 233	Telecommunications security; Lawful Interception (LI); Handover Specification for Email Delivery	Technical interface for the mediation and handing over of intercepted e-mails to an IC
TS 102 234	Telecommunications security; Lawful Interception (LI); Service Specification Details for Internet Access Services	Specification of LI requirements for ISPs providing an Internet Access service directly to end-users

11.3 Alternative specifications that the ISP may adopt are the latest versions of CALEA J-STD-025 and TIIT. Any deviations and option choices from these specifications must be communicated to and agreed upon by the IC prior to implementation.