GENERAL NOTICE

NOTICE 1325 OF *2005*

DEPARTMENT OF COMMUNICATIONS

DIRECTIVES IN RESPECT OF DIFFERENT CATEGORIES OF TELECOMMUNICATIONS SERVICE PROVIDERS MADE IN TERMS OF THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT, *2002* (ACT NO. *70* OF 2002)

I, Or. Ivy Matsepe-Casaburri, Minister *of* Communications, hereby make the Directives in Schedules A to C 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 (Aet No. *70* of 2002), and determine, in terms of section 30(7)(b) *of* the said Act, a period of six months from the date of publication hereof for compliance with the Directives.

Dr. Ivy Matsepe-Casaburri
MINISTER

SCHEDULE A

DIRECTIVE FOR FIXED LINE OPERATORS 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
2. Application
3. Statement of general duties

PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS

4. General requirements in respect of interception
5. Unchanged state of service
6. Security requirements for interception
7. Technical and functional requirements in respect of interception

PART 3: ROUTING, PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION

8. General requirements in respect of real-time communication-related information
9. Routing and content of additional real-time communication-related information during active intercept or in respect of future information
10. Routing, recording, storing and content *of* real-time communication-related information already available
11. security requirements in respect of real-time communication-related information

12. Technical and functional requirements in respect of real-time communication-related information

PART 4: ROUTING, PROVISION AND STORING OF ARCHIVED COMMUNICATCON-RELATED INFORMATION

13. General requirements in respect of archived communication-related information
14. Content of archived communication-related information
15. Security requirements in respect of archived communication-related information
16. Technical and functional requirements in respect of archived communication-related information

PART 5: STORAGE PERIOD FOR COMMUNICATION-RELATED INFORMATION

17. Period for which communication-related information must be stored

PART 6: DETAILED SECUIRTY, FUNCTIONAL AND TECHNICAL REQUIREMENTS OF THE FACILITIES AND DEVICES FOR LAWFUL INTERCEPTION

18. Facilities and Devices
19. Security Requirements
20. Functional Requirements
21. Technical Requirements

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);

"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;

"fixed line operator" means a fixed line operator as defined in section 1 of the Telecommunications Act, 1996 (Act No. 103 of 1996), including any telecommunications service provider who has fixed line technology deployed in its telecommunications system, and is herein referred to as a "FLO";

"handover interface" means a physical and logical interface across which the results of a direction or request are delivered from a FLO to the IC;

"identity" means a technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a logical or virtual telecommunications identity number (such as a personal telephone number or subscriber number) assigned to a physical access;

"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 telecommunications traffic pursuant to the Act;

"interception target" means the customer whose indirect communications are to be intercepted, or whose real-time communication-related information or archived communication-

related information is to be routed by a FLO to an IC or provided to a law enforcement agency, pursuant to a direction or request;

"quality of service" means the quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call btocking probability.

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

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

"target identity" means the identity associated with a target service (see below) used by the interception target; and

"target service" means a telecommunications service associated with an interception target and usually specified in a direction or request.

2. Application

This directive applies to and is binding on all FLOs that have been issued with a licence under Chapter 5 of the Telecommunications Act, 1996 (Act No. 103 of 1996).

3. Statement of General Duties

3.1 A FLO must –

(a) provide a telecommunications service which has the capability to be intercepted; and
(b) store communication-related information,
in accordance with the provisions of the Act and this directive.

3.2 When a direction or request is presented to a FLO, that FLO shall comply with the provisions of that direction or request.

PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS

4. General requirements in respect of interception

4.1 A FLO must-

(a) provide a telecommunication service in respect of which the in-band signals of all indirect communications can be duplicated and routed to the IC; and

(b) apply software and/or equipment on its telecommunication system to duplicate and route to the IC all indirect communications in accordance with a phased implementation plan to be agreed upon in consultation with the IC.

4.2 In accordance with a direction or request a FLO shall ensure that-

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

(b) any content of an indirect communication associated with a target identity, which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire period; service-specific sotutions must be presented by the FLO to the IC for consideration prior to implementation;

4.3 The ability to intercept indirect communications shall be provided by a FLO in respect of all interception targets utitising its telecommunications system and in respect of all target services.

4.4 All results of an interception of an indirect communication provided at the handover interface shall be uniquely identifiable in relation to the direction or request through the use of separate channels or unique identifiers.

4.5 After a direction or a request has been presented, interception of the indirect communications shall proceed in accordance with that direction or request.

4.6 The FLO shall, in relation to each interception target duplicate and route the signals of each indirect communication.

5. Unchanged state of service

5.1 Interception shall be implemented and operated in such manner that no unauthorized person can detect any change from the unintercepted state.

5.2 Interception shall be implemented and operated in such manner that no telecommunicating parties can detect any change from the unintercepted state.

5.3 The operating facilities of the target service shall not be altered as a result of any interception measure and the operating facilities of any other service shall not be altered as a result 'of any interception measure.

5.4 The quality of service of the target service shall not be altered as a result of any interception measure. The quality of service of any telecommunications service other than the target service shall not be altered 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 unauthorized persons.

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

6.3 The FLO shall agree to confidentiality on the manner in which interception measures are implemented in a given telecommunication installation with the manufacturers of its technical installations for the impternentation of interception measures.

6.4 The technical arrangements required within a telecommunication system to allow implementation of the

interception measures shall be realized with due care exercised in operating telecommunication installations, particularly with respect to the following:

(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 restriction to a minimum of staff engaged in implementation and operation of the interception measure.

(c) To ensure the ctear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception shall be carried out in operating rooms accessible only by authorized personnel.

(d) The results of interception shall be delivered through a handover interface to the IC.

(e) No access of any form to the handover interface shall be granted to unauthorized persons.

(f) FLOs shall take all necessary measures to protect the handover interface against misuse.

(g) The resutts of interception shall only be routed *to* the IC as indicated in the direction or request when proof of the authority to receive, was received from the IC, and proof of the authority to send from the handover interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations and as agreed upon by the IC and FLO.

(i) Where switched lines to the IC are used, call set-up shall be restricted through the use of the Closed User Group (CUG) facility.

(j) In certain interception cases applicants may require, at the cost of the IC, the use of encryption or other confidentiality measures to protect the routing of the results of such interception,

(k) FLOs shall co-operate with the IC, or *a* person authorised by the IC, to implement encryption or other-confidentiality measures if required for the purposes of paragraph (j), above.

(l) in order to prevent or trace misuse of the technical functions integrated in the telecommunication

installation enabling interception, 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 unauthorized input, and the records shall cover all or some of-

(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); and
(v) a reference to the direction or request,

6.5 The **FLOs** shall take reasonable steps to ensure that the records referred to in paragraph 6.4(l) are secure and only accessible to authorised staff.

6.6 Refer to paragraphs 18 and 19 for further compliance requirements with respect to security.

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.

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 ensure that the quality of service of the telecommunications traffic provided at the handover interface is not inferior to that offered to the target service for each particular calt.

7.4 The configuration of the handover interface shalt 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, protocots and coding principles,

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

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

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

7.8 FLOs must be able to route the intercepted indirect communications to the IC via fixed or switched connections.

7.9 The content of an indirect communication must be provided across the handover interface in one of the formats outlined below-

(a) the content of communication relating to two or more communicating parties is placed in a single telecommunications channet;
(b) the content of communications relating to two communicating parties is placed in two separate telecommunications channels;
(c) other configurations appropriate to the target service concerned.

7.10 The IC will be informed of-

(a) the activation of an intercept measure;
(b) the deactivation of the intercept measure;
(c) any change of the intercept measure; and
(d) the temporary unavailability of the intercept measure due to fault on the FLO's side of the link.

7.11 A FLO 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.

7.12 Where a FLO makes use *of* any other telecommunication **service** provider's telecommunication system, both that FLO and that other telecommunication service provider must co-operate in the provision of interception, if required. In this case, a

warrant/directive is to be served upon each of the involved service providers.

7.13 A FLO 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 authorized target services to be intercepted; and

(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 authorized target services to be intercepted.

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

7.15 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 indirect communications to be intercepted, the FLO shall ensure that the indirect communications can be intercepted on the basis of these characteristics. Identifying characteristics include, but are not limited to, the telephone number and subscriber number.

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

7.17 A FLO shall ensure that interception on the basis of more than one direction or request can be effected in respect of one and the same interception target. Multiple directions or requests may be applicable to a single interception target to allow monitoring by more than one appticant.

7.18 if multiple directions or requests are applicable, a FLO shall take reasonable precautions to safeguard the identities of the law

enforcement agencies concerned and to ensure the confidentiality of the investigations.

7.19 Multiple directions or requests may require different information in respect of the same interception target,

7.20 A FLO must ensure that the indirect communications of initially one in every 10 000 (ten thousand) customers can be intercepted simultaneously at any given time in its telecommunications system and all the results of interception routed to the IC.

7.21 Interception within a telecommunication system shall be implemented with reasonable measures to cater for the concurrent operation of several interceptions.

7.22 Supplementary to the provisions of paragraph 7.21, above, FLOs shall monitor their capacity in respect of simultaneous interceptions and shall be able to upgrade any regional or functional part of their telecommunication system within a reasonable period of time.

7.23. Refer to paragraphs 18, 20 and 21 for further compliance requirements with respect to technology and functionality.

PART 3: ROUTING, PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION

8. General requirements in respect of real-time communication-related information

8.1 A FLO must provide a telecommunication service in respect of which all real-time communication-related information can be –

(a) routed to the IC; or
(b) provided to a law enforcement agency.

8.2 A FLO must ensure that real-time communication-related information can immediately, on receipt of a direction, be-

(a) duplicated and routed to the IC; or
(b) provided to the law enforcement agency.

8.3 After a direction has been presented, the routing or provision of the real-time communication-related information shall proceed in accordance with that direction.

8.4 When real-time communication-related information cannot immediately be routed to the IC due to a fault on the telecommunications system of the FLO, it shall be buffered until it can be routed.

9. Routing and content of additional real-time communication-related information during active intercept or in respect of future information

9.1 When-

(a) both a real-time communication-related direction as well as an interception direction or request, in respect of the same target identity, are received; or
(b) a real-time communication-related direction, that requires information in respect of a future period of time, is received, a FLO shall be able to route or provide the real-time communication-related information in accordance with the direction concerned:

(i) when a call setup is attempted and a call control session has been established with the controlling network element;
(ii) when a call is estabtished (call is answered);
(iii) when no successful call *is* established (call is not answered).

9.2 In the circumstances set out in paragraph 9.1, above, a FLO shall be able to route the following real-time communication-related information to the IC for calls originating from, and originating in the FLO telecommunication network and terminating to the target identity:

(a) Called number (destination of an outgoing communication by the target identity).
(b) Calling number (telephone number of originating party of a terminating communication to the target identity).
(c) Date, time and duration of the communication.
(d) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.).
(e) Intermediate numbers where target identity establishes conference calls or calls to link through services.
(f) Telephone and subscriber number of target identity.
(g) Forwarding call number.

10. Routing, recording, storing and content *of* real-time communication-related information already available

10.1 A FLO shall record and store the real-time communication-related information set out in paragraph 10.3 whenever a call is established.

10.2 When a real-time communication-related direction, that requires information that is already available in the records of a FLO is received, that FLO shall be able to immediately route or provide the real-time communication-related information set out in paragraph 10.3 in accordance with the direction concerned.

10.3 For the purposes of paragraphs 10.1 and 10.2, above, a FLO shall be able to route or provide the following real-time communication-related information for calls originating from, and

originating in the FLO telecommunication network and terminating to the target identity:

(a) Called number (destination of an outgoing communication by the target identity).
(b) Calling number (telephone number of originating party of a terminating communication to the target identity).
(c) Date, time and duration of the communication.
(d) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.), if available-
(e) Intermediate numbers where target identity establishes conference calls or calls to link through services.
(f) Telephone and subscriber number of target identity.
(g) Nature of the telecommunication (e.g. fax, voice or data).
(h) Forwarding call number.

10.4 A FLO must provide a telecommunication service in respect of which all real-time communication-related information set out in paragraph 10.3 can be securely stored, retrieved and duplicated for-

(a) routing to the IC; or
(b) provision to a law enforcement agency.

10.5 Real-time communication-related information set out in paragraph 10.3 must be immediately available in the records of the FLO for a period of at least 90 days from the date of the indirect communication to which the real-time communication-related information relates.

10.6 The real-time communication-related information set out in paragraph 10.3 must immediatety be retrievable from the records of the FLO.

10.7 A FLO must ensure that real-time communication-related information set out in paragraph 10.3 can immediately, on receipt of a direction, be-

(a) duplicated and routed to the IC; or
(b) provided to the law enforcement agency.

10.8 The real-time communication-related information set out in paragraph 10.3 must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction.

10.9 When the real-time communication-related information set out in paragraph 10.3 is transferred to an archived storage facility, the FLO must ensure that-

(a) all the information is transferred;
(b) the information is not deleted before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
(c) the integrity of the information is not compromised.

11. Security requirements in respect of real-time communication-related information

11.1 Information on the manner in which storage measures in respect of real-time communication-related information are implemented by a FLO shall not be made available to unauthorized persons.

11.2 Real-time communication-related information shall not be made available to unauthorized persons.

11.3 The FLO shall agree to confidentiality on the manner in which storage measures in respect of real-time communication-related information are implemented with the manufacturers of its technical installations for the implementation of storage measures.

11.4 The technical arrangements required within a FLO, to allow-implementation of the storage measures in respect of real-time communication-related information, shall be realized with due care exercised in operating telecommunication installations, particularly with respect to the following:

(a) The need to protect information on which and how many target identities are or were subject to a real-time communication-related direction and the periods in respect of which the directions were applicable.

(b) The restriction to a minimum of staff engaged in implementation and operation of storing measures in respect of real-time communication-related information.

(c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, storing facilities in respect of reat-time communication-related information shalt be accessible only by authorized personnel.

(d) Real-time communication-refated information shall be delivered through a handover interface to the IC or provided to a law enforcement agency.

(e) No access of any form to the handover interface shall be granted to unauthorized persons.

(f) A FLO shall take all necessary measures to protect the handover interface against misuse.

(g) Real-time communication-related information shall only be routed to the IC as indicated in the direction when proof of the authority to receive of the IC, and proof of the authority to send of the interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations and as agreed upon by the IC and FLO.

(i) Where switched lines to the IC are used, call set-up shall be restricted through the use of the Closed User Group (CUG) facility.

(j) In certain interception cases applicants may require, at the cost of the IC, €he use of encryption or other confidentiality measures to protect the routing of real-time communication-related information.

(k) FLOs shall ensure that their handover interfaces support the use of encryption, authentication, integrity checking or other confidentiality measures and shall co-operate with applicants or the IC, or a person authorised by them, to implement such measures if required in terms of subparagraph (j), above.

(l) In order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling the storing, routing and provision of real-time communication-related information, 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

unauthorized input, and the records shalt cover all or some of-

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

(ii) the beginning and end of the activation or application of the real-time communication-related direction;

(iii) the IC to which the real-time communication-related information is routed or law enforcement agency to which it is provided;

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

(v) a reference to the direction.

11.5 The FLO shalt take reasonable steps to ensure that the records referred to in paragraph 11.4(l) are secure and only accessible to specific nominated staff.

11.6 The FLO shall take reasonable steps to ensure the integrity of real-time communication-related information when it is recorded and stored.

11.7 A FLO shall take reasonable steps to ensure the physical, environmental and logical security of all stored real-time communication-related information.

11.8 A FLO shall employ reasonable measures to ensure the availability of real-time communication-related information.

12. Technical and functional requirements in respect of real-time communication-related information

12.1 The technical handover interfaces shall provide all the relevant requested real-time communication-related information only, in a readable, intelligible and understandable format, and in accordance with the direction.

12.2 The configuration of the handover interface shall be such that the routing to the IC of the requested real-time communication-related information provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

12.3 Each instance of requested real-time communication-related information shall be uniquely associated with a single instance of the handover interface. Separate channels or the use of identifiers could achieve this.

12.4 The format for routing the requested real-time communication-related information to the IC must be an industry standard format.

12.5 FLOs must be able to route or provide the requested real-time communication-related information to the **IC.**

12.6 The IC will be informed of-

(a) any change of the storage system, measures and functionality that may impact on the routing, provision or configuration of real-time communication-related information; and
(b) the temporary unavailability of stored real-time communication-related information.

12.7 A FLO shall ensure that the configuration of the storage system is such that it can store; maintain, extract, process, transmit or provide real-time communication-related information with no or the minimum involvement of third parties.

12.8 Where a **FLO** makes use of any telecommunication service provider's telecommunication system or storage provider's service, that FLO and other telecommunication service provider or storage provider must co-operate in the storing, routing or provision of real-time communication-related information, if required. In this case, a warrant/directive is to be served upon each of the involved service providers.

12.9 A FLO must ensure that-

(a) any telecommunication service provider **or** storage provider involved in the storing, provision or routing of real-time communication-related information is given no more information relating to operational activities than is strictly necessary to store, provide or route real-time communication-related information; and

(b) any telecommunication service provider or storage provider involved in the co-operative storing, provision or routing of real-time communication-retated information is given no more information relating to operational activities than is strictly necessary to allow the storing, provision or routing of real-time communication-related information.

12.10 When the provision or routing of all the requested reat-time communication-related information is, in exceptional cases, not possible the remainder of the real-time communication-related information shall nevertheless be provided to the law enforcement agency or routed to the IC.

12.11 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested real-time communication information without unreasonable effort or delay.

12.12 The FLO shall ensure that more than one direction for real-time communication-related information can be operated concurrently for one and the same storage device or media.

12.13 If one or more direction for real-time communication-related information is processed, FLOs shall take reasonable precautions to safeguard the identities of the law enforcement agencies and ensure the confidentiatity of the investigations and information.

PART 4: ROUTING, PROVISION AND STORING OF ARCHIVED COMMUNICATION-RELATED INFORMATION

13. General requirements in respect of archived communication-related information

13.1 A FLO must provide a telecommunication service in respect of which all archived communication-related information can be securely stored, retrieved and duplicated for-

(a) routing to the IC; or
(b) provision to a law enforcement agency.

13.2 Archived communication-related information must be available in the storage facility of the FLO for the period specified in paragraph 17.

13.3 Archived communication-related information must be retrievable from the storage facility of the FLO.

13.4 A FLO must ensure that archived communication-related information can within the period specified in the direction, be-

(a) dupficated and routed to the IC; or
(b) provided to the law enforcement agency.

13.5 Archived communication-related information must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction.

13.6 When real-time communication-related information is transferred to an archived storage facility, the FLO must ensure that-

(a) all the information is transferred;
(b) the information is not deleted before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
(c) the integrity of the information is not compromised.

13.7 After a direction has been presented, the routing or provision of the archived communication-related information shall proceed in accordance with that direction.

14. Content of archived communication-related information

FLOs shall be able to provide the following archived communication-related information:

(a) Called telephone number or address (destination of outgoing communication by the target identity).
(b) Date, time and duration of the communication.
(c) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.), if available.
(d) Telephone number of target identity.
(e) Forwarding call number.

15. Security requirements in respect of archived communication-related information

15.1 Information on the manner in which storage measures in respect of archived communication-related information are implemented by a FLO shalt not be made available to unauthorized persons.

15.2 Archived communication-related information shall not be made available to unauthorized persons.

15.3 The FLO shall agree confidentiality on the manner in which storage measures in respect of archived communication-related information are implemented with the manufacturers of his technical installations for the implementation of storage measures.

15.4 The technical arrangements required within a FLO, to allow implementation of the storage measures in respect of archived communication-related information, shall be realized with due care exercised in operating telecommunication installations, particularly with respect to the following:

(a) The need to protect information on which and how many target identities are or were subject to an

archived communication-related direction and the periods in respect of which the directions were applicable.

(b) The restriction to a minimum of staff engaged in implementation and operation of storing measures in respect of archived communication-related information.

(c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, storing facilities in respect of archived communication-related information shall be accessible only by authorized personnel.

(d) Archived communication-related information shall be delivered through a handover interface to the IC or provided to a law enforcement agency.

(e) No access of any form to the handover interface shall be granted to unauthorized persons.

(f) A **FLO** shall take all necessary measures to protect the handover interface against misuse.

(g) Archived communication-related information shall only be routed to the IC as indicated in the. direction when proof of the authority to receive of the IC, and proof of the authority to send of the interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations and as agreed upon by the IC and FLO.

(i) Where switched lines to the IC are used, call set-up shall be restricted through the use of the Closed User Group (CUG) facility.

(j) In certain interception cases applicants may require, at the cost of the IC, the use of encryption or other confidentiality measures to protect the routing of archived communication-related information.

(k) FLOs shall ensure that their handover interfaces support the use of encryption, authentication, integrity checking or other confidentiality measures and shall co-operate with applicants or the IC, or a person authorised by them, to implement such measures if required in terms of subparagraph (j).

(l) In order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling the storing, routing and provision of archived communication-related information, 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 unauthorized input, and the records shall cover all or some of-

(i) €hetarget identities of the target service or target services concerned;
(ii) the beginning and end of the activation or application of the archived communication-related direction;
(iii) the IC to which the archived communication-related information is routed or taw enforcement agency to which it is provided;
(iv) an authenticator suitable to identify the operating staff (including date and time of input); and
(v) a reference to the direction.

15.5 The **FLOs** shall take reasonable steps to ensure that the records referred to in paragraph 15.4(l) are secure and only accessible to specific nominated staff.

15.6 The **FLO** shall take reasonable steps to ensure the integrity of archived communication-related information when it is stored, during transfer thereof to any storage device or media and for the entire storage period set out in paragraph 17.

15.7 A FLO shall take reasonable steps to ensure the physical, environmental and logical security of all stored archived communication-related information.

15.8 A FLO shall employ reasonable measures to ensure the availability of archived communication-related information.

16. Technical and functional requirements in respect **of** archived communication-related information

16.1 The technical handover interfaces shall provide all the relevant requested archived communication-related information only, in a readable, intelligible and understandable format, and in accordance with the direction.

16.2 The configuration of the handover interface shall, be such that the routing to the IC of the requested archived communication-related information provided at the interface can be implemented with industry standard, generally available transmission paths, protocols and coding principles.

16.3 Each instance of requested archived communication-related information shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

16.4 The format for routing the requested archived communication-related information to the IC must be an industry standard format.

16.5 **FLOs** must be able to route or provide the requested archived communication-related information to the **IC.**

16.6 The IC will be informed of-

(a) any change of the storage system, measures and functionality that may impact on the routing, provision or configuration of archived communication-related information ; and

(b) the temporary unavailability of stored archived communication-related information.

16.7 A FLO shall ensure that the configuration of the storage system is such that it can store, maintain, extract, process, transmit or provide archived communication-related informatiin with no or the minimum involvement of third parties.

16.8 Where a FLO makes use of any telecommunication service provider's telecommunication system or storage provider's service, that FLO and other telecommunication service provider or storage provider must co-operate in the storing, routing or provision of archived communication-related information, if required. In this case, a warrant/directive is to be served upon each **of** the involved service providers.

16.9 A FLO must ensure that-

(a) any telecommunication service provider or storage provider involved in the storing, provision or routing of archived communication-related information is given no more information relating to operational activities than is strictly necessary to store, provide or route archived communication-related information; and

(b) any telecommunication service provider or storage provider involved in the co-operative storing, provision or routing of archived communication-related information is given no more information relating to operational activities than is strictly necessary to allow the storing, provision or routing of archived communication-related information.

16.10 When the provision or routing of all the requested archived communication-related information is, in exceptional cases, not possible the remainder of the archived communication-reiated information shall nevertheless be provided to the law enforcement agency or routed to the IC.

16.11 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested archived communication-related information without unreasonable effort or delay.

16.12 The FLO shall ensure that more than one direction for archived communication-related information can be operated concurrently for one and the same storage device or media.

16.13 If one or more direction for archived communication-related information are processed, FLOs shall take reasonable precautions to safeguard the identities of the law enforcement agencies and ensure the confidentiality of the investigations and information.

PART 5: STORAGE PERIOD FOR COMMUNICATION-RELATED INFORMATION

17. Period for which communication-related information must be stored

Communication-related information, whether real-time or archived communication-related information, must be stored for a cumulative period of three (3) years from the date on which the indirect communication to which the communication-related information relates, is recorded.

PART 6: DETAILED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS OF THE FACILITIES AND DEVICES FOR LAWFUL INTERCEPTION

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

18. Facilities and Devices

18.1 The operator is expected to implement a marking facility for lawful interception (LI) compliance purposes. This facility must comply with the physical and access control security measures specified in the security requirement section of this document.

18.2 Within this marking facility, the operator must implement an Interception Management System (IMS), composed of one or more LI servers and one or more administration workstations, for the marking and management of targets and interceptions. The IMS must be protected from the rest of the operator's network by means of one or more network firewalls.

18.3 Where necessary, the operator must implement mediation device(s) for the collection from network elements, normatisation and delivery to an interception centre **(IC)** of intercept related information (I RI) tickets in the format specified within the technical requirement section of this document.

18.4 The internal interception function (IIF) of network elements (when provided by the vendor) must **be** used in preference to physical wiretap and external interception equipment.

18.5 When external interception equipment is necessary (i.e. no IIF is provided by the equipment vendor), the interception function must be implemented in dedicated hardware or firmware and must **he** connected in a manner as to:

- not disrupt normal operation of the telecommunication network when the equipment fails.

19. Security Requirements

19.1 The marking facility implementation for lawful interception purposes at the fixed line operator must comply with the following security guidelines:

-
- the Minimum Information Security Standards (MISS) national information security policy as approved by Cabinet on 4th December **1996.**

19.2 This dedicated area of the marking facility must conform to the physical security requirements stipulated within MISS.

19.3 Physical access control to the marking facility must be implemented using an electronic access control device such as a RFID token.

19.4 The access control system to the marking facility must provide detailed logs of both successful and failed access attempts to the facility.

19.5 The mechanical key mechanism should only be used in the event of the electronic access control device or the access control system failing. This key must be kept safely with strict control over its access.

19.6 Logical access control to the marking facility must be implemented using a token-based authentication mechanism such as a one-time password token.

19.7 Insofar as is possible, the logical access control system on the provisioning and mediation platforms at the marking facility must provide detailed logs of both successful and failed access attempts to these platforms.

19.8 Network access to the marking facility must be secured through means of a network firewall.

19.9 The rule set on the firewall must explicitly deny all externally originated communication sessions.

19.10 The firewall security must be augmented with intrusion detection systems capable of identifying and blocking network hacking attempts on the marking facility. The IDS pattern files must be updated regularly from the vendor of the IDS solution.

19.11 Both network and server based anti-virus solutions must be implemented for the marking facility. The anti-virus definition files must be updated regularly from the vendor of the anti-virus software.

19.12 Insofar as is possible, the communication link between the marking facility and the IC for the delivery of intercept related information (i.e. HI2) must be encrypted using an IPSEC based link encryption device working in ESP mode. The encryption algorithm to be used is either 168-bit EDE mode Triple DES or 192-bit CBC mode **AES.**

20. Functional Requirements

20.1 The following minimum functions must be implemented by the operator; 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:
  - o a secure telefax; or
  - o 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 as per the targeting and timing information stipulated in the warrant or direction; the confirmation of the activation of the warrant or direction to the IC;
- Administration of the physical, logical and LI application security and access control mechanisms;
- Systems administration (including configuration management, change management, backup and disaster

recovery) of the LI servers, databases, mediation devices and workstations implemented in the marking facility;

- Provision of available reports on performance, availability, capacity, utilisation and other measures (to be determined in conjunction with the OIC) to the IC;
- Reporting on security breach attempts and failed access attempts to the OIC; and
- Internal and external audit of security and operations within the marking facility.

21. Technical Requirements

21.1 As far as is possible, the fixed line operator must adopt specifications relevant to its network from the foilowing 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 101 331 Version 1.1.1 2001-08	Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies	LI requirements from an Law Enforcement Agency (LEA) point of view
ES 201 158 Version 1.2.1 2002-04	Telecommunications security; Lawful Interception (LI); Requirements for network functions	Derived network functions and the general architecture (or functionat model) for LI
TS 101 671 Version 2.5.1 2003-01	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	Generic flow of information, the procedures, the information elements and the network/service specific protocols relating to the provision of lawful interception at the handover interface

SCHEDULE B

DIRECTIVE FOR MOBILE CELLULAR OPERATORS ON 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 pubtication hereof)

ARRANGEMENT OF CONTENT

PART 1 : INTRODUCTORY PROVISIONS

1. Definitions
2. Application
3. Statement of general duties

PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS

4. General requirements in respect of interception
5. Unchanged state of service
6. Security requirements for interception
7. Technical and functional requirements in respect of interception

PART 3: ROUTING, PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION

8. General requirements in respect of real-time communication-related information
9. Routing and content of additional real-time communication-related information during active-intercept or in respect of future information
10. Routing, recording, storing and content of real-time communication-related information already available
11. Security requirements in respect of real-time communication-related information

12. Technical and functional requirements in respect of real-time communication-related information

PART 4: ROUTING, PROVISION AND STORING OF ARCHIVED COMMUNICATION-RELATED INFORMATION

13. General requirements in respect of archived communication-related information
14. Content of archived communication-related information
15. Security requirements in respect of archived communication-related information
16. Technical and functional requirements in respect of archived communication-related information

PART 5: STORAGE PERIOD FOR COMMUNICATION-RELATED INFORMATION

17. Period for which communication-related information must be stored

PART 6: DETAILED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS OF THE FACILITIES AND DEVICES FOR LAWFUL INTERCEPTION

18. Facilities and Devices
18. Security Requirements
20. Functional Requirements
21. Technical Requirements

PART 1 : INTRODUCTORY PROVISIONS

1. Definitions

In this directive, unless the context othetwise 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-retated Information Act, 2002 (Act No. 70 of 2002);

"buffer" means the temporary storing of real-time communication-related information and "buffered" has a similar meaning;

"direction" means a written or oral interception direction, real-time communication-related direction or archived communication - related direction, as the case may-be "handover interface" means a physical and logical interface across which the results of a direction or request are delivered from a MCO to the IC;

"identity" means a technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone handset number, IMEI or SIM-card number, IMSI) or the logical or virtual telecommunications identity number (such as a personal number, MSISDN) assigned to a physical access;

"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 telecommunications traffic pursuant to the Act;

"interception target" means the customer whose indirect communications are to be intercepted and routed to the IC, or whose real-time communication-related information or archived communication-related information is to be routed by a MCO to an IC or provided to a law enforcement agency, pursuant to a direction or request;

"mobile cellular operator*' means a mobile cellular operator as defined in section I of the Telecommunications Act, 1996 (Act No. 103 of 1996), including any telecommunications service provider who is licensed to use mobile cellular or fixed mobile technology in its telecommunications system, and is herein referred to as a "**MCO**";

"quality of service" means the quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

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

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

"successful call" means the successful establishment of communication channel with the generation of one or more call data records (CDRs) associated with the communication channel.

"target identity" means the identity associated with a target service used by the interception target; and

"target service" means a telecommunications service used by an interception target and specified in a direction or request.

2. Application

This directive applies to and is binding on all MCOs that have been issued with a licence under Chapter 5 of the Telecommunications Act, 1996 (Act No. 103 of 1996).

3. Statement of general duties

31 A MCO must-

(a) provide a telecommunications service which has the capability to be intercepted; and
(b) store communication-related information,

in accordance with the provisions of the Act and this directive.

3.2 When a direction or request is presented to a MCO, that MCO shall comply with the provisions of that direction or request.

PART 2: INTERCEPTION OF INDIRECT COMMUNICATCONS

4. General requirements in respect of interception

4.1 A MCO must-

(a) provide a telecommunication service in respect *of* which the signals **of** specified indirect communications can be duplicated and routed to the IC; and

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

4.2 In accordance with **a** direction or request **a** MCO shall ensure that-

(a) the entire content of an indirect communication associated with a target identity can be intercepted during the entire interception period; and

(b) any content of an indirect communication associated with a target identity which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire interception period.

4.3 The ability to intercept indirect communications shall be provided by a MCO in respect of all interception targets utilising its telecommunications system and in respect of all target services.

4.4 The results of interception relating to an interception target shall be provided by the MCO 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 MCO.

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 that direction or request.

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

5. Unchanged state of service

5.1 interception shall be implemented and operated in such manner that no unauthorised person can detect any change from the unintercepted state.

5.2 Interception shall be implemented and operated in such manner that communicating parties cannot detect any change from the unintercepted state.

5.3 The operating facilities of the target service shall not be altered as a result of any interception measure and the operating facilities of any other service shall not be altered as a result of any interception measure.

5.4 The quality of service of *the* target service shall not be altered as a result of any interception measure. The quality of service of any telecommunications service other than the target service shall not be altered 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 system 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 The MCO shall agree confidentiality on the manner in which interception measures are implemented in a given telecommunication system with the manufacturers of its technical installations for the implementation of interception measures.

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 systems, particularly with respect to the following:

(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 restriction to a minimum number of staff engaged in implementation and operation of the interception measure.

(c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception shalt be carried out in operating rooms accessible onty by authorised personnel.

(d) The results of interception shall be delivered through a handover interface to the IC.

(e) No access *of* any form to the handover interface shall be granted to unauthorised persons.

(f) MCOs shall take all necessary measures to protect the handover interface against misuse.

(g) The results of interception shall only be routed to the IC as indicated in the direction or request when proof of the authority to receive, was received from the IC, and proof of the authority to send of the handover interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations.

(i) Where switched lines to the IC are used, proof of authentication shall be furnished for each call set-up.

(j) In certain interception cases applicants may require, at the cost of the IC, the use of encryption or other confidentiality measures to protect the routing of the results of such interception.

(k) **MCOs** shall co-operate with the IC, or a person authorised by the IC, to implement encryption or other confidentiality measures if required for the purposes of subparagraph (j) above.

(l) In order to prevent or trace misuse of the technical functions integrated in the telecommunication system enabling interception, any activation or application of these functions in relation to a given target identity shatl be fully recorded, including any activation or application caused by faulty or unauthorised input, and the records shall cover all or some of-

(i) the target identities of the target service or target services concerned;
(ii) the beginning and end of the activation or implementation 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); and
(v) a reference to the direction or request.

6.5 The MCOs shall take reasonable steps to ensure that the records referred to in paragraph 6.4(l) are secure and only accessible to specific nominated staff.

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.

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

7.3 The configuration of the handover interface shall enable that the quality of service of the telecommunications traffic provided at the handover interface is not inferior to that offered to the target service for each particular call.

7.4 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.

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

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

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

7.8 MCOs must be able to route the intercepted indirect communications to the **IC** via fixed or switched connections.

7.9 The content of an indirect communication must (unless expressly specified in the direction or request) be provided across the handover interface in one of the formats outlined below -

(a) the content of communication relating to two or more communicating parties **is** placed in a single telecommunications channel;
(b) the content of communications relating to two communicating parties **is** placed in two separate telecommunications channels;
(c) other configurations appropriate to the target service concerned.

7.10 The **IC** will be informed of-

(a) the activation of an intercept measure;
(b) the deactivation of the intercept measure;
(c) any change of the intercept measure; and
(d) the temporary unavailability of the intercept measure due to **a** fault on the telecommunication system of the **MCO.**

7.11 Each **MCO** shall reasonably 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.

7.12 Where a MCO makes use of any other telecommunication service provider's telecommunication system, both that MCO and that other telecommunication service provider must co-operate in the provision of interception, if required.

7.13 A MCO must reasonably 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; and

(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.

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

7.15 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 indirect communications of the target services to be intercepted, the MCO shall ensure that the indirect communications can be intercepted on the basis of these characteristics, Identifying characteristics include, but are not limited to, the MSJSDN, IMEI and IMSI numbers.

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

7.17 The **MCO** shall ensure that more than one interception measure can be operated simultaneously for one and the same interception target. Multiple interceptions may be required for a single interception target to allow monitoring by more than one applicant.

7.18 tf multiple interceptions are active, a MCO shall take reasonabte precautions to safeguard the identities of the Jaw enforcement agencies and ensure the confidentiality of the investigations.

7.19 The multiple interception measures may require different information according to different lawful directions or requests.

7.20 The MCO mentioned in Column ▮ of Table 1 must ensure that it can initially simultaneously intercept €he indirect communications of the number of customers mentioned opposite to that MCO in Column 2 of Table 1 at any given time in its telecommunications system and all the results of interception routed to the IC.

Table ▮

Column 1	**Column 2**
Cell C (Pty.) Ltd.	**60**
Mobile Telephone Networks (Pty.) Ltd.	120
Vodacom (Pty.) Ltd.	**240**
Any other MCO	1 for every 25 000 customers

7.21 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 severat interception measures are operated simultaneously.

7.22 Supplementary to the provisions of paragraph 7.21, above, MCOs shall monitor their capacity in respect of simultaneous interceptions and shall be able to upgrade any regional or functional part of their telecommunication system within a reasonable period of time.

PART 3: ROUTING, PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION

8. General requirements in respect of real-time communication-related information

8.1 A MCO must provide a telecommunication service in respect of which all real-time communication-related information of the target service can be-

(a) routed to the IC; or
(b) provided to a law enforcement agency.

8.2 A MCO must ensure that real-time communication-related information can immediately, on receipt of a direction, be-

(a) duplicated and routed to the IC; or
(b) provided to the law enforcement agency.

8.3 After a direction has been presented, the routing or provision of the real-time communication-related information shall proceed in accordance with that direction.

8.4 When real-time communication-related information cannot immediately be routed to the IC due to a fault on the telecommunications system of the MCO, it shall be buffered until it can be routed.

9. Routing and content of additional real-time communication-related information during active intercept or in respect *of* future information

9.1 When-

(a) both a real-time communication-related direction as well as an interception direction or request, in respect of the same target identity, are received; or
(b) a real-time communication-related direction, that requires information in respect of a future period of time, is received,

a MCO shall be able to route or provide the real-time communication-related information in accordance with the direction concerned-

(i) when a call setup is attempted and a link has been established with the controlling network element, such as a Mobile Switching Centre (MSC};
(ii) when a successful call is established;
(iii) when no successful call is established but a tink has been established with the controlling network element, such as a Mobile Switching Centre (MSC);
(iv) on change of service or service parameter (e.g. activation of call forwarding and includes so-called supplementary services);
(v) on change of location during an established call.

9.2 In the circumstances set aut in paragraph 9.1, above, a MCO shall he able to route the following real-time communication-related information to the IC:

(a) Global System for Mobile Communication (GSM), including telephony, fax, Circuit Switched Data (CSD), as well as Wireless Application Protocol (WAP) over CSD and Multimedia Message Service (MMS) over CSD:

(i) Called number - (destination of an outgoing-communication by the target identity).
(ii) Calling number (MSISDN of originating party of a terminating communication to the target identity).
(iii) Date and time of the start and duration of the communication, when available.
(iv) Type of communication (incoming, outgoing, link through, conference).
(v) Intermediate numbers where target identity establishes conference calls or calls to link through services.
(vi) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(vii) Identification of the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.
(viii) Nature of the indirect communication (etc fax, voice, or data).
(ix) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (a)(i) to (viii), above, when available on the date to be determined by the Minister
(x) Forwarding call number.

(b) General Packet Radio Service (GPRS), including Wireless Application Protocol (WAP) over GPRS and Multimedia Message Service (MMS) over GPRS:

(i) Called address, Access Point Name or APN (destination of an outgoing communication by the target identity).
(ii) Date and time of the start and duration of the communication, when available.
(iii) Data volume, if available.
(iv) Type of communication (incoming, outgoing).
(v) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(vi) Identification of the base–station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.
(vii) Nature of the indirect communication (etc fax, voice, or data).
(viii) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (b)(i) to (vii), above, when available and on the date to be determined by the Minister

(c) Short Messaging Service (SMS), including outgoing and terminating short messages:

(i) Called number (destination of an outgoing communication by the target identity where receipt of the message has been confirmed by the controlling network element, SMSC).
(ii) Date and time of the communication, when applicable.
(iii) Type of communication (incoming, outgoing).
(iv) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(v) Identification of the base–station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.
(vi) Nature of the indirect communication (etc fax, voice, or data).
(vii) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (c)(i) to (vi), above, when available.

(d) Unstructured Supplementary Service Data **(USSD):** The information available in the records of the MCO on the same basis as set out in subparagraph (c), above.

(e) Universal Mobile Tetephone Service (UMTS): The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

(f) Any other data service not mentioned in subparagraphs (a) to *(e),* above: The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

10. Routing, recording, storing and content of real-time communication-related information already available

10.1 A MCO shall record and store the real-time communication-related information set out in paragraph 10.3 when a successful call is established.

10.2 When a real-time communication-related direction, that requires information that is already available in the records of a MCO is received, that MCO shall be able to immediately route or provide the real-time communication-related information set out in paragraph 10.3 in accordance with the direction concerned.

10.3 For the purposes of paragraphs 10.1 and 10.2, above, a MCO shall be able to route or provide the following real-time communication-related information:

(a) Global System for Mobile Communication (GSM), including telephony, fax, circuit switched data (CSD), as well as Wireless Application Protocol (WAP) over CSD and Multimedia Message Service (MMS) over **CSD:**

(i) Called number (destination of an outgoing communication by the target identity).

(ii) Calling number (MSISDN of originating party of a terminating communication to the target identity).

(iii) Date and time of the start and duration of the communication, when applicable.

(iv) Type of communication (incoming, outgoing, link through, conference).

(v) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(vi) Identification of the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.
(vii) Nature of the indirect communication (etc fax, voice, or data).
(viii) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (a)(i) to (viii), above, when available.
(ix) Forwarding call number.

(b) General Packet Radio Service (GPRS), including Wireless Application Protocol (WAP) over GPRS and Multimedia Message Service (MMS) over GPRS:
(i) Called address, Access Point name or APN (destination of an outgoing communication by the target identity).
(ii) Date and time of the start and duration of the communication, when applicable.
(iii) Data volume.
(iv) Type of communication (incoming, outgoing).
(v) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(vi) Identification of the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.
(vii) Nature of the indirect communication (etc fax, voice, or data),
(viii) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (b)(i) to (vii), above, when available.

(c) Short Messaging Service (SMS), including outgoing and terminating short messages:
(i) Called number (destination of an outgoing communication by the target identity where receipt of the message has been confirmed by the controlling network element, SMSC).
(ii) Date and time of the communication, when applicable.
(iii) Type of communication (incoming, outgoing).
(iv) IMSI number, IMEI number (where available) and MSISDN number of target identity.

(v) Identification of the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.

(vi) Nature of the indirect communication (etc fax, voice, or data).

(vii) For outbound roaming where the target identity roams on a foreign network, the information set out in subparagraph (c)(i) to (vi), above, when available, and on a date to be determined by the Minister.

(d) Unstructured Supplementary Service Data (USSD): The information available in the records of the MCO on the same basis as set out in subparagraph (c), above.

(e) Universal Mobile Telephone Service (UMTS): The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

(f) Any other data service not mentioned in subparagraphs (a) to (e), above: The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

10.4 A MCO must provide a telecommunication service in respect of which the real-time communication-related information set out in paragraph 10.3 can be securely stored, retrieved and duplicated for-

(a) routing to the IC; or
(b) provision to a taw enforcement agency.

10.5 The real-time communication-related information set out in paragraph 10.3 must be immediately available in the records of the MCO for a period of at least 90 days from the date of the indirect communication to which the real-time communication-related information relates.

10.6 The reat-time communication-related information set out in paragraph 10.3 must immediately be retrievable from the records of the MCO.

10.7 A MCO must ensure that real-time communication-related information set out in paragraph 10.3 can immediately, on receipt of a direction or request, be –

(a) duplicated and routed to the IC; or
(b) provided to the law enforcement agency.

10.8 The real-time communication-related information set out in paragraph 10.3 must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction or request.

10.9 When the real-time communication-related information set out in paragraph 10.3 is transferred to an archived storage facility, the MCO must ensure that-

(a) all the information is transferred;
(b) the information is not transferred before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
(c) the integrity of the information is not compromised.

11. Security requirements in respect of real-time communication-related information

11.1 Information on the manner in which storage measures in respect of real-time communication-related information are implemented by a MCO shall not be made available to unauthorised persons.

11.2 Real-time communication-related information shall not be made available to unauthorised persons.

11.3 The MCO shall agree to confidentiality on the manner in which storage measures in respect of real-time communication-related information are implemented with the manufacturers of its technicat systems for the implementation of storage measures.

114 The technical arrangements required within a MCO, to allow implementation of the storage measures in respect of real-time communication-related information, shall be realised with due care exercised in operating telecommunication systems, particularly with respect to the following:

(a) The need to protect information on which and how many target identities are or were subject to a real-time communication-related direction and the periods in respect of which the directions were applicable.

(b) The restriction to a minimum number of staff engaged in implementation and operation of storing measures in respect of real-time communication-related information.

(c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, storing facilities in respect of real-time communication-related information shall be accessibte only by authorised personnel.

(d) Real-time communication-related information shall be delivered through a handover interface to the IC or provided to a law enforcement agency.

(e) No access of any form to the handover interface shall be granted to unauthorised persons.

(f) A MCO shall take alt necessary measures to protect the handover interface against misuse.

(g) Real-time communication-related information shall only be routed to the IC as indicated in the direction when proof of the authority to receive of the IC, and proof of the authority to send of the interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations.

(i) Where switched lines to the IC are used, such proof shall be furnished for each routing of information.

(j) In certain interception cases applicants may stipulate, at the cost of the IC, the use of additional security devices to protect the routing of real-time communication-related information.

(k) MCOs shall ensure that their HI2 (CRI) handover interfaces support the use of encryption, authentication, integrity checking or other confidentiality measures and shall co-operate with applicants or the IC, or a person authorised by them, to

implement such measures if required for the purposes of subparagraph (j) above.

(l) In order to prevent or trace misuse of the technical functions integrated in the telecommunication system enabling the storing, routing and provision of real-time communication-related information, any activation or application of these functions in relation to a given target identity shall be fully recorded, including any activation or application caused by faulty or unauthorised input, and the records shall cover all or some of-

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

(ii) the beginning and end of the activation or application of the real-time communication-related direction;

(iii) the IC to which the real-time communication-related information is routed or law enforcement agency to which it is provided;

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

(v) a reference to the direction.

11.5 The MCO shall take reasonable steps to ensure that the records referred to in paragraph 11.4(l) are secure and only accessible to specific nominated staff.

11.6 The MCO shall take reasonable steps to ensure the integrity of real-time communication-related information when it is recorded and stored.

11.7 A MCO shall reasonable steps to ensure the physical, environmental and logical security of all stored real-time communication-related information.

11.8 A MCO shall employ all reasonable measures to ensure the availability of real-time communication-related information.

12. Technical and functional requirements in respect of real-time communication-related information

12.1 The technical handover interfaces shall provide all the relevant requested real-time communication-related information

only, in a readable, infelligible and understandable format, and in accordance with the direction.

32.2 The configuration of the handover interface shall be such that the routing to the IC of the requested real-time communication-related information provided at the interface can be implemented with industry standard, generally available transmission paths, protocats and coding principles.

12.3 Each instance of requested real-time communication-related information shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

12.4 The format for routing the requested real-time communication-related information to the IC must be an industry standard format.

12.5 MCOs must be able to route the requested real-time communication-related information to the IC via fixed or switched connections.

12.6 The IC will be informed of-

(a) any change of the storage system, measures and functionality that may impact on the routing, provision or configuration of real-time communication-related information; and

(b) the temporary unavailability of stored real-time communication-related information.

12.7 A MCO shall ensure that the configuration of the storage system is such that it can store, maintain, extract, process, transmit or provide real-time communication-related information with no or the minimum involvement of third parties.

12.8 Where a MCO makes use of any telecommunication service provider's telecommunication system or storage provider's service, that MCO and other telecommunication service provider-or storage provider must co-operate in the storing, routing or provisioning of real-time communication-related information, if required.

12.9 A MCO must take reasonabie steps to ensure that-,

(a) any telecommunication service provider or storage provider involved in the storing, provisioning or routing of real-time communication-related information is given no more information relating to operational activities than is strictly necessary to store, provide or route real-time communication-related information; and

(b) any telecommunication service provider or storage provider involved in the co-operative storing, provisioning or routing of real-time communication-related information is given no more information relating to operational activities than is strictly necessary to allow the storing, provision or routing of real-time communication-related information.

12.10 When the provision or routing of all the requested real-time communication-related information is, in exceptional cases, not possible the remainder of the real-time communication-related information shall nevertheless be provided to the law enforcement agency or routed to the IC.

12.11 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only the requested real-time communication information without unreasonable effort or delay.

12.12 The MCO shall ensure that more than one direction for real-time communication-related information can be operated simultaneously for one and the same storage device or media.

12.13 If one or more direction for real-time communication-related information are processed, MCOs shall take reasonable precautions to safeguard the identities of the law enforcement agencies and to ensure the confidentiality of the investigations and information.

PART 4: ROUTING, PROVISION AND STORING OF ARCHIVED COMMUNICATION-RELATED INFORMATION

13. General requirements in respect of archived communication-related information

13.1 A MCO must provide a telecommunication service in respect of which all archived communication-related information in respect of the target service can be securely stored, retrieved and duplicated for-

(a) routing to the IC; or
(b) provision to a law enforcement agency.

13.2 Archived communication-related information must be available in the storage facility of the MCO for the period specified in paragraph 17.

13.3 Archived communication-related information must be retrievable from the storage facility of the MCO.

13.4 A MCO must ensure that archived communication-related information can within the period specified in the direction, be-

(a) duplicated and routed to the IC; or
(b) provided to the law enforcement agency.

13.5 Archived communication-related information must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction.

13.6 When real-time communication-related information is transferred to an archived storage facility, the MCO must ensure that-

(a) all the information is transferred;
(b) the information is not transferred before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
(c) the integrity of the information is not compromised.

13.7 After a direction has been presented, the routing or provision of the archived communication-related information shall proceed in accordance with that direction.

14. Content of archived communication-related information

MCOs shall be able to provide the following archived communication-related information in respect of successful calls:

(a) Global System for Mobile Communication (GSM), including telephony, fax, circuit switched data (CSD), as well as Wireless Application Protocol (WAP) over CSD and Multimedia Message Service (MMS) over CSD:

(i) 'Called number (destination of **an** outgoing communication by the target identity).

(ii) Date and time of the start and duration of the communication, when applicable.

(iii) Type *of* communication (outgoing, link through, conference).

(iv) IMSI number, IMEI number (where available) and MSISDN number of target identity.

(v) Identification **of** the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.

(vi) Forwarding call number.

(vii) For outbound roaming where the target identity roams on a foreign network, the information set out in the above subparagraphs, **if** and when available.

(b) General Packet Radio Service (GPRS), including Wireless Application Protocol (WAP) over GPRS and Multimedia Message Service (MMS) over GPRS:

(i) Called address, Access Point name or APN (destination of an outgoing communication by the target identity).

(ii) Date and time **of** the start and duration of the communication, when applicable.

(iii) Data volume.

(iv) IMSI number, IMEI number (where available) and **MSISDN** number of target identity.

(v) Identification of the base station and cell (including micro cell) that were used to link the target identity **at** the start of an indirect communication.

(c) Short Messaging Service (SMS), including outgoing and terminating short messages:

(i) Called number (destination of an outgoing communication by the target identity where receipt of the message has been confirmed by the controlling network element, SMSC).
(ii) Date and time of the communication, when applicable.
(iii) IMSI number, IMEI number (where available) and MSISDN number of target identity.
(iv) Identification of the base station and cell (including micro cell) that were used to link the target identity at the start of an indirect communication.

(d) Unstructured Supplementary Service Rata (USSD): The information available in the records of the MCO on the same basis as set out in subparagraph (c), above.

(e) Universal Mobile Telephone Service (UMTS): The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

(f) Any other data service not mentioned in subparagraphs (a) to (e), above: The information available in the records of the MCO on the same basis as set out in subparagraph (b), above.

15. Security requirements in respect of archived communication-related information

15.1 Information on the manner in which storage measures in respect of archived communication-related information are implemented by a MCO shall not be made available to unauthorised persons.

15.2 Archived communication-related information shall not be made available to unauthorised persons.

15.3 The MCO shall agree confidentiality on the manner in which storage measures in respect of archived communication-related information are implemented with the manufacturers of his technical systems for the implementation of storage measures.

15.4 The technical arrangements required within a MCO, to allow implementation of the storage measures in respect of archived communication-related information, shall be realised with due care exercised in operating telecommunication systems, particularly with respect to the following:

(a) The need to protect information on which and how many target identities are or were subject to a archived communication-related direction and the periods in respect of which the directions were applicable.

(b) The restriction to a minimum number of staff engaged in implementation and operation of storing measures in respect of archived communication-related information,

(c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, storing facilities in respect of archived communication-related information shall be accessible only by authorised personnel.

(d) Archived communication-related information shall be delivered through a handover interface to the IC or provided to a law enforcement agency.

(e) No access of any form to the handover interface shall be granted to unauthorised persons.

(f) A MCO shall take all necessary measures to protect the handover interface against misuse.

(g) Archived communication-related information shatl only be routed to the IC as indicated in the direction when proof of the authority to receive of the IC, and proof of the authority to send of the interface, has been furnished.

(h) Authentication and proof of authentication shall be implemented subject to national laws and regulations.

(i) Where switched lines to the IC are used, such proaf shall be furnished for each routing of information.

(j) In certain interception cases appticants may stipulate, at the cost of the IC, the use of additional security devices to protect the routing of archived communication-related information.

(k) MCOs shall ensure that their HI2 (CRI) handover interfaces support the use of encryption, authentication, integrity checking or other confidentiality measures and shall co-operate with applicants or the IC, or a person authorised by them, to

implement such measures if required in terms of subparagraph (j), above.

(l) In order to prevent or trace misuse of the technical functions integrated in the telecommunication system enabling the storing, routing and provision of archived communication-related information, any activation or application of these functions in relation to a given target identity shall be fully recorded, including any activation or application caused by faulty or unauthorised input, and the records shall cover all or some of-

(i) the target identities of the target service or target services concerned;
(ii) the beginning and end *of* the activation or apptication of the archived communication-related direction;
(iii) the IC to which the archived communication-related information is routed OF law enforcement agency to which it is provided;
(iv) an authenticator suitable to identify the operating staff (including date and time of input); and
(v) a reference to the direction.

15.5 The MCOs shall take reasonable steps to ensure that the records referred to in paragraph 15.4(l) are secure and only accessible to specific authorised staff.

15.6 The MCO **shall** take reasonable steps to ensure the integrity of archived communication-related information when it is stored, during transfer thereof to any storage device or media and for the entire storage period set out in paragraph **17.**

15.7 A MCO shall take reasonable steps to ensure the physical, environmental and logical security of all stored archived communication-related information.

15.8 A MCO shall employ reasonable measures to ensure the availability of archived communication-related information.

16. Technical and functional requirements in respect of archived communication-related information

16.1 The technical handover interfaces shall provide 'all the relevant requested archived communication-related information only, in a readable, intelligible and understandable format, and in accordance with the direction.

16.2 The configuration of the handover interface shall be such that the routing to the LC of the requested archived communication-related information provided at the interface can be implemented with industry standard, generally available transmission paths, protocols and coding principles.

16.3 Each instance of requested archived communication-related information shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.

16.4 The format for routing the requested archived communication-related information to the LC must be an industry standard format.

16.5 **MCOs** must be able to route the requested archived communication-related information to the LC via fixed or switched connections.

16.6 The LC will be informed of-

(a) any change of the storage system, measures and functionality that may impact on the routing, provision or configuration of the archived communication-related information ; and

(b) the temporary unavailability of stored archived communication-related information.

16.7 A MCO shall take reasonable steps to ensure that the configuration of the storage system is such that it can store, maintain, extract, process, transmit or provide archived communication-related information with no or the minimum involvement of third parties.

16.8 Where a MCO makes use of any telecommunication service provider's telecommunication system or storage provider's service, that MCO and other telecommunication service provider or storage provider must co-operate in the storing, routing or provision of archived communication-related information, if required.

16.9 A MCO must ensure that-

(a) any telecommunication service provider or storage provider involved in the storing, provision or routing of archived communication-related information is given no more information relating to aperationat activities than is strictly necessary to store, provide or route archived communication-related information; and

(b) any telecommunication service provider or storage provider involved in the co-operative storing, provision or routing of archived communication-related information is given no more information relating to operational activities than is strictty necessary to allow the storing, provision or routing of archived communication-related information.

16.10 When the provision or routing of all the requested archived communication-related information is, in exceptional cases, not possible the remainder of the archived communication-related information shall nevertheless be provided to the law enforcement agency or routed to the IC.

16.11 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested archived communication-related information without unreasonable effort or delay.

16.12 The MCO shall ensure that more than one direction for archived communication-related information can be operated simultaneously for one and the same storage device or media.

16.13 If one or more direction for archived communication-related information are processed, MCOs shall take reasonable precautions to safeguard the identities of the law enforcement agencies and ensure the confidentiality of the investigations and information.

PART 5: STORAGE PERIOD FOR COMMUNICATION-RELATED INFORMATION

17. Period for which communication-related information must be stored

Communication-related information, whether real-time or archived communication-related information, must be stored for a cumulative period of three (3) years from the date on which the indirect communication to which the communication-related information relates, is recorded.

PART 6: DETAILED SECURITY, FUNCTIONAL AND TECHNICAL REQUIREMENTS OF THE FACILITIES AND DEVICES FOR LAWFUL INTERCEPTION

MCOs 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.

18. Facitities and Devices

18.1 The operator is expected to implement a marking facility for lawful interception (LI) compliance purposes.

18.2 Within this marking facility, the operator must implement an Interception Management System (IMS) for the centralised marking and management of targets and interceptions.

18.3 Where necessary, the operator must implement mediation device(s) for the collection from network elements, normalisation and delivery to an interception centre (IC) of intercept related information (IRI) tickets in the format specified within the technical requirement section of this document.

18.4 The internal interception function (IIF) of network elements (when provided by the vendor) must be used in preference to physical wiretap and external interception equipment.

18.5 When external interception equipment is necessary (i.e. no IIF is provided by the equipment vendor), the interception function must be implemented in dedicated hardware or firmware and must be connected in a manner as to:

- not disrupt normal operation of the telecommunication network when the equipment fails; and
- provide the same coverage of interception as an equivalent IIF solution would provide.

19. Security Requirements

19.1 It is recommended that the operator applies the following guidelines in securing the marking facility implementation for lawful interception purposes:

- the physical and information security measures and practices outlined in the Minimum Information Security Standards (MISS) national information security policy as approved by Cabinet on 4th December 1996.

- 19.2 The marking facility must be hosted within a physically secured environment,

19.3 Physical access control to the marking facility must be implemented using an electronic access control mechanism.

19.4 The access controi system to the marking facility must provide detailed logs of both successful and failed access attempts to the facility and must be hosted within the marking facility itself. These logs must be maintained for a period of thirty (30) days.

19.5 The mechanical key mechanism should only be used in the event of the electronic access control mechanism or the access control system failing. Access to this key must be strictly controlled.

19.6 Logical access control to the marking facility must be implemented using a token-based authentication mechanism such as a digital certificate enabled smart card or a one-time password token.

19.7 The logical access control system on the provisioning and mediation platforms at the marking facility must provide detailed logs of both successful and failed access attempts to these platforms. These logs must be maintained for a period of thirty (30) days.

19.8 The marking facility network must be secured through means of a network firewall based on protocol proxy or statefui protocol inspection technology.

19.9 The rule set on the firewall must explicitly deny all externally originated communication sessions unless stipulated otherwise by the interception centre (IC) and agreed upon by the MCO.

19.10 The firewall security must be augmented with intrusion detection systems capable of identifying and blocking network

hacking attempts on the marking facility. The IDS pattern files must be updated regularly from the vendor of the IDS solution.

19.11 Both network and server based anti-virus solutions must be implemented for the marking facility. The anti-virus definition files must be updated on regularly from the vendor of the anti-virus software.

19.12 The communication link between the marking facility and the IC for the delivery of intercept related information (i.e. HI2) must be encrypted using an IPSEC based link encryption device working in ESP mode. The encryption algorithm to be used is either 168-bit EDE mode Triple DES or 192-bit CBC mode AES.

20. Functional Requirements

20.1 The following minimum functions must be implemented within the operator's marking facility; 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 by means of either:
  - a physically delivered hardcopy from the OIC;
  - an oral direction from the appointed judge;
  - a secure telefax from the OIC i.e. an encrypted facsimile facility (to be provided by the OIC); 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 based on the telephonic or online verification of the Lawful Interception Identifier (LIID) stipulated in the warrant or direction with the OIC;
- Provision of the warrant or direction into the IMS 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 IMS;
- Administration of the physical, logical and IMS security and access control mechanisms;
- Day-to-day systems maintenance on the software and hardware implemented in the marking facility;
- Regular provision of reports available in the LI marking facility to the IC;
- Reporting on security breach attempts and failed access attempts to the OIC; likewise, reporting by the OIC on security breach attempts and failed access attempts to the MCO in so far as it affects the MCO's network; and
- Regular internal audits of security and operations within the marking facility by the MCO to manage information security risks associated with providing this facility and capability.

21. Technicat Requirements

21.1 Intercept related call content must be transmitted from the operator network to the interception centre through one or more gateway switches close to the interception centre via ISDN (ITU-T Q.931-DSS1) links. The hardware costs incurred to support this connectivity from the switch will be borne by the operator.

21.2 As far as is possible, the operator must 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 Technicat Specification	Title	Descrlptlon
TS 101 331 Version 1.1.1 2001-08	Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies	LI requirements from an Law Enforcement Agency (LEA) point of view
ES 201 158 Version 1.2.1 2002-04	Telecommunications security; Lawful Interception (LI); Requirements for network functions	Derived network functions and the general architecture (or functional model) for LI
TS 101 671 Version 2.5.1 2003-01	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic	Generic flow of information, the procedures, the information elements and the network/service specific protocols relating to the provision of lawful interception at the handover interface

21.3 The ETSI specifications for LI in Release Phase 2+ for GSM and GPRS services must be adopted and complied with.

21.4 The following ETSI specifications for LI in 3GPP Release '99 for UMTS services must be adopted and complied with when UMTS services are provided by the MCO:

- **TS 133 106** – LI Requirements for UMTS
- **TS** 133 107 – LI Architecture and Functions for UMTS
- **TS** 133 108 – LI Handover Interface for UMTS

2t.5 The operator must ensure that a sufficiently current software version release is implemented on all the switching elements to support **ETSI** compliance within its network.

21.6 **All** of the LI features required for the compliance to the requirements stipulated in this directive and implemented in the switching element software must be installed and enabled.

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
2. Application
3. Statement of general duties

PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS

4. General requirements in respect of interception
5. Unchanged state of service
6. Security requirements for interception
7. Technical and functional requirements in respect of interception

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

8. Facilities and Devices
9. Security Requirements
10. Functional Requirements
11. Technical Requirements

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.