EUROPEAN UNION
THE COUNCIL

Brussels, 3 September 1998 (17.09)
(OR. d)

10951/98

LIMITE

ENFOPOL 98

NOTE

from : Austrian Presidency

to : Police Cooperation Working Party

No. prev. doc.: OJ C 329, 4.11.1996, p. 1, 10102/98 ENFOPOL 87

Subject: **Interception of telecommunications**
Draft Council Resolution on new technologies

Preliminary remark:

For the expert meeting of the Working Party on Police Cooperation on 3 and 4 September 1998, delegations will find attached a draft Council Resolution on the interception of telecommunications, which deals with Explanatory Memoranda, supplementary requirements and definitions in relation to new technologies such as S-PCS, Internet, provision of subscriber-related and call-associated data, cryptography and security measures for network operators/service providers; the various text passages having been drafted by the technical expert groups ILET, STC and IUR.

D R A F T

COUNCIL RESOLUTION
of .....

on the lawful interception of telecommunications
in relation to new technologies

THE COUNCIL OF THE EUROPEAN UNION

(P R E A M B L E)

HAS ADOPTED THIS RESOLUTION:

1. The Council notes that, as a result of ongoing progress in telecommunications technology, the requirements of law enforcement agencies in regard to network operators and service providers for the purposes of lawful interception of telecommunications, as described in the Council Resolution of 17 January 1995 (96/C 329/01), have also changed.

2. The Council considers that the requirements contained in the Council Resolution of 17 January 1995 are also appropriate to be applied analogously both to existing new technologies, in particular satellite communications, Internet, cryptography, prepaid cards etc., and as to future technologies.

3. The Council further considers that progress in telecommunications technology has created a need both for supplementary requirements, including those on security measures in regard to network operators and service providers, and for supplementary definitions.

4. The Council considers that the aforementioned Explanatory Memoranda and supplementary requirements as annexed should also be taken into account in the implementation of measures for the lawful interception of telecommunications, and requests Member States to call upon the Ministers responsible for telecommunications to support this view and to cooperate with the Ministers responsible for Justice and Home Affairs with a view to implementing the supplementary requirements and definitions in relation to network operators and service providers.

REGARDING NEW TECHNOLOGIES

to the Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01) published in the Official Journal of the European Communities

Part 1: Explanatory Memoranda

Introduction regarding S-PCS:

The purpose of this Explanatory Memorandum is to provide an assessment of applicability of law-enforcement requirements to mobile satellite services (MSS). Specifically, for each of the requirements, an assessment of technical and jurisdictional issues is provided. The technical issues relate to capability and capacity of an intercept solution in an MSS network. The jurisdictional issues relate to national procedures that may have an impact on the ability of law-enforcement agencies to deal with a multinational service provider.

These services are made up of various operational architectures including voice, data and paging services. Operational scenarios include mobile-to-mobile (satellite); mobile-to-mobile (terrestrial); mobile (satellite or terrestrial)-to-public switch telephone network (PSTN); and PSTN-to-mobile (satellite or terrestrial). The interception of such satellite services is subject both to the national laws of the requesting law-enforcement agency and to those of the gateway host country.

Introduction regarding the INTERNET:

The International Requirements for Interception were developed by law-enforcement agencies to express their common requirements for the guidance of the telecommunications industry. These Requirements (Version 1.0) were adopted by the Council Resolution of 17 January 1995 on the lawful interception of telecommunications and published in the Official Journal of the European Communities No C 329, 4.11.1996, p 1. The Governments of the United States of America, Canada and Australia have formally agreed to take the Requirements into account in national policies and to recommend that they be used as a basis for discussion with the telecommunications industry, standardisation bodies and others.

The Requirements document contains all of the requirements of the agencies, but experience has shown that further explanation is needed in some cases and that their application to new and emerging technologies also needs to be clarified.

To ensure that the International Requirements for Interception continue to serve the purpose for which they were intended, Explanatory Memoranda expand and clarify the basic document in a manner agreed by the law enforcement agencies as expressing their common requirement.

SCOPE

General

This Explanatory Memorandum relates to the requirements of law-enforcement agencies for the interception of public IP-based (Internet) services.

Applicable Services

Examples of Internet services to which this Memorandum applies include but are not limited to:

- dial-in services
- services connected by HFC cable

- services supplied by satellite
- directly connected services, e.g. LANs connected via a router.

1. Law-enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law-enforcement agencies also require access to the call-associated data that are generated to process the call (Requirements Item 1 – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The terrestrial network architecture for an MSS network is very similar to that of cellular or PCS networks. The MSS networks employ similar concepts of mobility as in the IS-41 or GSM-based terrestrial wireless networks. Data services may have a different architecture without such components.

Terrestrial gateway stations are a common and easy location for intercept solutions for accessing telecommunications and call-associated data, but mobile-to-mobile communications may allow mobiles to communicate with each other without inclusion of terrestrial gateway stations, thereby necessitating additional complexity to the intercept solution.

The number of the target service used by the interception subject may be either part of the existing country code or a separate country code for an MSS provider.

Capacity in most MSS networks is limited to the amount of frequency bandwidth and/or satellite power available within the satellite constellation. The intercept requirement will have an impact on MSS network capacity for mobile-to-mobile calls that would typically not require a link to a terrestrial gateway.

Most MSS providers are planning their network architecture on the basis of technical and cost issues. The current proposed architectures accommodate some of these issues by serving multiple States from a single terrestrial gateway. This raises several national policy and sovereignty issues for the States involved.

Accessing information on subscribers or from gateways associated with other States may raise sovereignty issues for each State involved.

Interception orders from one State may have to be transferred to another State for the service provider to activate intercepts.

Explanation with regard to the INTERNET:

The term "telecommunications" is defined in the glossary of the International Requirements. In the Internet context, telecommunications to and from the target service (see below) means all IP datagrams transmitted to and from the target host plus e-mail deposited in an e-mail server for later collection by the interception subject. It also includes telecommunications between the interception subject and the Internet service provider, for example for the purpose of changing a password.

The identifier for an Internet service which is a target service will usually be the means by which the service is known to the service provider and used to authenticate (and possibly to bill) a person attempting to use the service and/or the means by which traffic is directed to the service. Examples of service identifiers are:

- IP address (for services with a fixed IP address)
- account number
- logon ID/password

- PIN number
- e-mail address

Call-associated data refers to the signalling information contained within the IP datagrams and also, where appropriate, to the calling line identifier of the telephone service used by the interception subject to connect to the Internet provider. Call-associated data is discussed in more detail later in this Memorandum.

1.1. Law-enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system (Requirements Item 1.1. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Separated or partitioned gateways may physically or logically separate subscriber profile data and channel resources by service provider or State, thereby creating a barrier to law enforcement access to a subscriber's or user's profile data, call-associated data and telecommunications.

The definition of a "telecommunications system" may have a major impact for an MSS provider. For some MSS providers, the system covers the entire globe. A telecommunications system's access by Law enforcement may need to be limited to a nation.

If the MSS is an international service provider, international law may become applicable making acquisition of a subscriber's or user's communications possible.

Explanation with regard to the INTERNET:

An interception subject is considered to be operating permanently within a network if the host has a permanent physical connection to the Internet Service provider this is analogous to a wireline telephone service.

Access is also required when an interception subject has personal or terminal mobility as is the case for dial-in access. This is analogous to a roaming mobile telephone service. Access is required whenever the interception subject is connected to the Internet.

It should be noted that national laws may restrict the conditions under which an interception order is valid. In some cases for example, it may not be lawful to intercept a service if the interception subject or the point-of-presence is outside the jurisdiction of the interception order.

1.2. Law-enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications services or terminal equipment, including calls that traverse more than one network or are processed by more than one operator/service provider before completing (Requirements Item 1.2. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Any impacts associated with supplementary services used within cellular, PCS, and wireless networks such as advanced calling features, voice mail, etc. also will be relevant to MSS due to similarities in terrestrial infrastructure. There is a distinction between inter-network and intra-network traffic.

Explanation with regard to the INTERNET:

In the circuit-switched environment, this requirement relates to calls directed towards the target service. In the Internet environment it relates to sessions that are not initiated by the target service (usually e-mail directed towards the target service). In these cases, access is required to all telecommunications, even when they are diverted to another destination as, for example, when e-mail is redirected.

1.3. Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorisation (Requirements Item 1.3 – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS should be able to meet this requirement.

Explanation with regard to the INTERNET:

For both circuit-switched and packet-switched services, this requirement means that law-enforcement agencies require the network operator/service provider to extract interception product from a composite or multiplexed data stream before providing it to the law-enforcement agency.

1.4. Law-enforcement agencies require access to call-associated data such as (Requirements Item 1.4 – OJ 96/C 329/01):

1.4.1. Signalling of access-ready status (Requirements Item 1.4.1. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Physically separated or logically partitioned gateways may separate subscriber profile data by service provider or State, which may be different from the service provider or State served with a request for an intercept from law enforcement. This separation may create an obstacle to Law-enforcement's agencies' access to a subscriber's or user's profile data.

Law-enforcement requires this data during the initial and all subsequent registrations of the mobile to the network.

Explanation with regard to the INTERNET:

Requirement 1.4.1. describes the signalling information required by law-enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.4.2. Called-party number for outgoing connections even if there is no successful connection established (Requirements Item 1.4.2. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

If a mobile is in a State temporarily, this information may not be available for unsuccessful connections.

Physically separated or logically partitioned gateways may separate subscriber profile data by service provider or State, which may be different from the service provider or State served with a request for an intercept from law enforcement. This separation may create an obstacle to law enforcement's access to a subscriber's call-associated data.

It is essential that this information be available to law-enforcement agencies.

Explanation with regard to the INTERNET:

Requirement 1.4.2. describes the signalling information required by law-enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.4.3. Calling-party number for incoming connections even if there is no successful connection established (Requirements Item 1.4.3. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

MSSs with intersatellite links can minimise connection charges by routing calls through the intersatellite links to the nearest MSS gateway instead of to the specific intercept-provisioned MSS gateway (if different) for mobile originated calls. For MSSs with gateways serving large areas, least-cost routing to a gateway redundant to the subscriber's intercept-provisioned gateway may circumvent intercepts for both internationally and nationally originated calls.

It is essential that this information be available to law-enforcement agencies regardless of what gateway is being utilised by the subscriber's or user's service.

Explanation with regard to the INTERNET:

Requirement 1.4.3. describes the signalling information required by law-enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.4.4. All signals emitted by the target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer (Requirements Item 1.4.4. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS should be able to meet this requirement.

This includes call origination signalling and post cut-through signalling.

Explanation with regard to the INTERNET:

Requirement 1.4.4. describes the signalling information required by law-enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.4.5. Beginning, end and duration of the connection (Requirements Item 1.4.5. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS should be able to meet this requirement.

Explanation with regard to the INTERNET:

Requirement 1.4.5. describes the signalling information required by law-enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.4.6. Actual destination and intermediate directory numbers if call has been diverted (Requirements Item 1.4.6. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

For calls forwarded over a satellite channel, pared down satellite signalling (due to scarcity of satellite resources) compared to wireline signalling may present a limit to the depth of call-associated data that is available to law-enforcement agencies.

Protocol translation between national networks may introduce a loss of information.

Explanation with regard to the INTERNET:

Requirement 1.4.6. describes the signalling information required by law enforcement agencies in regard to circuit-switched services.

In the Internet context, this specific requirement is irrelevant as the signalling information is contained within the header of the IP datagrams.

1.5. Law-enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers (Requirements Item 1.5. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The distance of satellites from earth introduces a high level of granularity for subscriber location compared to terrestrial wireless systems ranging from hundreds of meters to many kilometres.

Because the location capability is not precise, an MSS may be unable to correctly associate an intercept subject that is within several kilometres of more than one national border with the correct nation.

Explanation with regard to the INTERNET:

For dial-in services, law-enforcement agencies require the calling-line identifier where this is available to the service provider.

1.6. Law-enforcement agencies require data on the specific services used by the interception subject and the technical parameters for those types of communication (Requirements Item 1.6. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

For an interception subject roaming from one State to another, only a portion of the subscriber profile will be available at the roaming gateway. Law-enforcement agencies would need a means of acquiring the remaining information from the home gateway that is in another State.

Explanation with regard to the INTERNET:

For an Internet service, this includes the means of connection (dial-in, LAN, satellite, cable, etc.), the transmission speed in each direction and information relating to e-mail servers used by the interception subject.

2. Law-enforcement agencies require a real time, full-time monitoring capability for the interception of telecommunications. Call-associated data should also be provided in real time. If call-associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination (Requirements Item 2. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The global topology of MSS may add more delay to the delivery of call-associated data than terrestrial cellular-type wireless services.

Call content should be delivered to law-enforcement agencies in real time.
Call-associated data should be made available within milliseconds of the call event rather than the call completion. 100 milliseconds to 500 milliseconds is the desirable target. It is imperative that the call-associated data be available within this short time frame to allow for correlation of call event with call details.

Explanation with regard to the INTERNET:

In the Internet context, reference to call-associated data is not applicable.

3. Law-enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law-enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries (Requirements Item 3. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The interception may be provisioned on an MSS gateway located in any number of States, various types of transmission facilities or signalling protocols could be used for transfer of the intercepted telecommunications and call-associated data to law enforcement.

During such transmission or transfer, the intercepted data cannot be altered or corrupted in any way.

There must be coordination between the network operator(s) and service provider(s) and between the network operator(s) and service provider(s) and law-enforcement agencies.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

Explanation with regard to the PROVISION OF SUBSCRIBER-RELATED DATA AND CALL-ASSOCIATED DATA:

This requirement includes provision of commonly agreed interfaces that will allow transmission of subscriber details.

3.1. Law-enforcement agencies require network operators/service providers to provide call-associated data and call content from the target service in a way that allows for the accurate correlation of call-associated data with call content (Requirements Item 3.1. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Law-enforcement agencies need to know from where this information is originating.

Explanation with regard to the INTERNET:

This requirement is not applicable.

3.2. Law-enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format. This format will be agreed upon on an individual-country basis (Requirements Item 3.2. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The format utilised must not be a "proprietary" format, but should be a readily available and "reasonable" format.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

3.3. If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law-enforcement agencies require the network operators/service providers to provide intercepted communications en clair (Requirements Item 3.3. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

This requirement includes call-detail information as well as call-content data.

Explanation with regard to the INTERNET:

This requirement also applies unchanged to Internet services. Note that where a target modifies the traffic by encoding or encryption or by applying any other process, it is the responsibility of the intercepting agency to extract intelligence from the received product.

3.4. Law-enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law-enforcement monitoring facility via fixed or switched connections (Requirements Item 3.4. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS should be able to meet this requirement.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

3.5. Law-enforcement agencies require that the transmission of the intercepted telecommunications to the monitoring facility meet applicable security requirements (Requirements Item 3.5. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS provider should be able to meet this requirement. Reference is made to the International User Requirements (IUR) – Security document for additional details.

The definition of "applicable security requirements" may have a major impact on multinational MSS providers.

Security issues for international information exchange may face sovereignty issues.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

4. Law-enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorised person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service must appear unchanged to the interception subject (Requirements Item 4. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There can be no degradation of voice quality of the target's service due to the interception. This includes, but is not limited to, things such as: delay of call setup; delay of voice transmission; delay of ability to initiate features; denial of service; degraded voice quality, and "anomalous" indications displayed on the target's mobile.

The need for international law-enforcement cooperation may increase significantly the number of "authorised" personnel with access to an interception order.

The definition of "unauthorised person" may have a severe impact on the intercept administration for an MSS provider. In the case of a gateway serving more than one State foreign citizens may have access to interception orders.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

5. Law-enforcement agencies require the interception to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the interception (Requirements Item 5. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

The need for international law-enforcement cooperation may increase significantly the number of "authorised" personnel with access to an interception order.

The definition of "unauthorised person" may have a severe impact on the intercept administration for a MSS provider. In the case of a gateway serving more than one State foreign citizens may have access to interception orders.

Unauthorised personnel cannot have access to the "product" of the intercept or audit information or other intercept-related data.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

Explanation with regard to the PROVISION OF SUBSCRIBER-RELATED DATA AND CALL-ASSOCIATED DATA:

This requirement includes a requirement to protect all information associated with requests for subscriber details.

5.1. Law-enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out (Requirements Item 5.1. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to a MSS provider. Every MSS should be able to meet this requirement.

This requirement includes target identification information.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

5.2. Law-enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorisation (Requirements Item 5.2. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to an MSS provider. Every MSS should be able to meet this requirement.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

5.3. According to national regulations, network operators/service providers could be obliged to maintain an adequately protected record of activations of interceptions (Requirements Item 5.3. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to a MSS provider. Every MSS should be able to meet this requirement.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

6. Based on a lawful enquiry and before implementation of the interception, law-enforcement agencies require: (1) the interception subject's identity, service number or other distinctive identifier, (2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and (3) information on the technical parameters of the transmission to the law-enforcement monitoring facility (Requirements Item 6. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

This includes the terrestrial telecommunications service provider(s), if any, to whom the subscriber or user has access.

The information needed by law-enforcement agencies for an intercept may reside on gateways owned and operated by a foreign organisation or company.

This information may also reside with the service provider providing the targeted service.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

7. During the interception, law-enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries (Requirements Item 7. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

There should be no impacts or issues specific to a MSS provider. Every MSS should be able to meet this requirement. If a country requires that a person from a network operator/service provider be present in a court to verify, this may be an issue for multinational MSS providers.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

Explanation with regard to the PROVISION OF SUBSCRIBER-RELATED DATA AND CALL-ASSOCIATED DATA:

With the introduction of such telecommunication-network functionality as number portability, this requirement is extended to include the requirement for the network operator/service provider to notify the intercepting agency if the target service is "ported" to another network operator/service provider while an interception order is in force.

8. Law-enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law-enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements (Requirements Item 8. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Because a given MSS gateway may serve satellite coverage to more than one State, capacity for intercepts should include the requirements of each State served.

The maximum number of simultaneous interceptions for a given subscriber may need to abide by the capacity requirements of more than one State. More than one State may have interceptions for the same mobile subscriber being served out of one gateway.

National requirements are defined as multiple-country requirements.

"Flagged" numbers must be such as to accommodate all the capacity needs of the national law-enforcement agencies' requirements.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

9. Law-enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law-enforcement agencies will vary by country and by the type of target service to be intercepted (Requirements Item 9. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Language, time differences, technical interfaces may increase significantly the sophistication, and therefore, the time required to carry out intercepts in a gateway serving more than one State.

Sovereignty issues may cause further delays if cooperation between law-enforcement agencies from different countries is required.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

Explanation with regard to the PROVISION OF SUBSCRIBER-RELATED DATA AND CALL-ASSOCIATED DATA:

This requirement includes providing access to subscriber data needed to obtain and implement the warrant as quickly as possible.

10. For the duration of the interception, law-enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law-enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers (Requirements Item 10. – OJ 96/C 329/01)

Explanation with regard to S-PCS:

Performance standards must be of an acceptable level and are subject to the standards of the original call.

Explanation with regard to the INTERNET:

This requirement applies unchanged to Internet services.

Part 2: Supplementary Requirements

A. REQUIREMENTS RELATING TO THE PROVISIONS OF SUBSCRIBER-RELATED DATA AND CALL-ASSOCIATED DATA

General

This Explanatory Memorandum relates to the requirements of law-enforcement agencies for information about:

- the identity of subscribers;
- the services, equipment and features used by subscribers, and
- the use made by subscribers of telecommunications services (billing records, Internet footprints, etc.).

Applicable services

Law-enforcement agencies require access to information about subscribers to all telecommunications services including, but not limited to, the following:

- circuit-switched telephony services, e.g. PSTN, ISDN;
- terrestrial mobile services, e.g. GSM, AMPS, D-AMPS, CDMA, DCS-1800;
- satellite-based mobile services, e.g. IRIDIUM, Globalstar, ICO;
- Trunked mobile services, e.g. TETRA;
- Internet services both dial-in and fixed based;
- calling-card services both pre-paid and account based;
- call-back services;
- long-distance and international services;
- paging services;
- data services, e.g. X.25, X.400, ATM, frame relay, and
- voice-mail services.

Law-enforcement agencies also require the means to access information about subscribers in other countries in situations where those subscribers may be operating within the agency's jurisdiction. Examples of these situations include, but are not limited to the following:

- Internationally roaming mobile subscribers;
- subscribers to S-PCS services such as Iridium, and
- subscribers to international carriers where the subscriber database is in another country.

Requirements

On the basis of the Council Resolution of 17 January 1995, the existing requirements as specified in item 6 shall be supplemented with items 6.1 to 6.7.

6. Based on a lawful enquiry and before implementation of the interception, law-enforcement agencies require: (1) the interception subject's identity, service number or other distinctive identifier, (2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and (3) information on the technical parameters of the transmission to the law-enforcement monitoring facility (Requirements Item 6. – OJ 96/C 329/01).

SUPPLEMENTARY REQUIREMENTS WITH REGARD TO ITEM 6

6.1. Law-enforcement agencies require access to information kept by the operators/providers of telecommunications networks, telecommunications services and Internet services on the subject's identity. Examples of such information include, but are not limited to, the following:

- *** the full name and address of the interception subject, including postal code;**
- *** the full name and address, including postal code, of the party which pays the bill for the services provided to the interception subject;**
- *** sufficient credit-card details to identify the account if the interception subject pays by credit card, and**
- *** the directory name and address as shown in the directory.**

6.2. Law-enforcement agencies require the means to access information on the numbering plans or identification numbers for telecommunications services to help identify an interception subject's operator. Typical service plans that may require identification include, but are not limited to, the following:

- *** ISDN-services;**
- *** packet-switched services and circuit-switched services;**
- *** telex services, and**
- *** Internet-domain names;**

6.3. Law-enforcement agencies require access to information kept by the operators/providers of telecommunications networks, telecommunications services and Internet services on the interception subject's service number or other distinctive identifier. Examples of such information include, but are not limited to, the following:

- **types of services and features used by the interception subject;**
- **wireline directory numbers;**
- **technical identifiers and codes of the telecommunications equipment such as the MSISDN, IMSI and IMEI GSM identifiers, which are supplied by the operator to the interception subject;**
- **the means by which an operator identifies a subscriber of Internet on cable TV;**
- **user identifier or code given by a caller and used by an Internet provider to authenticate and bill the user;**
- **cable or channel identifiers for fixed-point services;**
- **IP address for users of fixed Internet services;**
- **associated directory number on a voice-mail service;**
- **e-mail address;**
- **the PIN or code given by the caller and used by the provider to authenticate and bill a user of calling card services, and**
- **the means by which an international or long-distance service operator authenticates a caller.**

6.4. Law-enforcement agencies require access to information kept by the operators/providers of telecommunications networks, telecommunications services and Internet services on the interception subject's optional services and features. Examples of such information include, but are not limited to, the following:

*** for wireline PSTNs these features include call diversion, call waiting, call completion, pre-selection of a long-distance carrier, voice-mail and abbreviated dialling;**

*** for GSM mobile these features further include additional MSISDN for fax and data, voice-mail, SMS, special roaming approval and high-speed data, and**

*** for Internet services these may include both e-mail and e-mail redirection.**

This requirement is also applicable for those services which incorporate the use of prepaid card technology.

6.5. Law-enforcement agencies require access to traffic and billing records of an interception subject.

6.6. Law-enforcement agencies require the operators/providers of telecommunications networks, telecommunications services and Internet services to keep an up-to-date register of Individual Mobile Equipment Identity codes of mobile communications equipment which is sold by such operators to their clients.

6.7. Law-enforcement agencies require all subscriber information to be obtained from a search commencing with:

*** the service number or other distinctive identifier, or**

*** any of the elements of the subscriber's identity as outlined in the sections above, such as name or address or credit card service.**

B. REQUIREMENTS RELATING TO SECURITY MEASURES FOR NETWORK OPERATORS/SERVICE PROVIDERS

Introduction

The requirements relating to security measures are specified for network operators/service providers to comply with. These requirements are laid down in order to safeguard the interests of the services authorised by law to carry out telecommunications interceptions (Law-Enforcement Agencies).

These requirements can be seen as a further elaboration on the requirements of the Council Resolution of 17 January 1995 (items 3.5, 5., 5.1, 5.2, 5.3), (OJ 96/C 329/01).

Compliance with the requirements is intended to ensure that:

- the interests of those affected by an intercept are protected from disclosure of their telecommunications to parties other than the intercepting agency;
- the telecommunication access of intercepting agencies is prevented from being blocked, and
- the abuse of the technical telecommunications intercept facilities used by network operators/service providers is prevented and also traced.

SUPPLEMENTARY REQUIREMENTS:

11. Law-enforcement agencies require that the network operator/service provider implements security procedures on its site.
These procedures have to be agreed with the Law-enforcement agencies.

11.1. The network operator/service provider shall co-operate with regular security reviews by the Law-enforcement agencies.

11.2. Interception orders and interception data shall be classified in accordance with the appropriate national security level. Law-enforcement agencies require that the network operator/service provider ensure the confidentiality of all interception orders and interception data.

11.3. Interception orders must be destroyed by the network operator/service provider within a certain period, as required by national legislation and procedures.

11.4. Law-enforcement agencies require that in the case of violation of the integrity and/or the confidentiality of the interception order or interception data, the network operator/service provider take all necessary action to prevent dissemination of the information. It will notify the agency responsible of the host state as soon as possible about the violation. Furthermore the Law-enforcement agencies require the network operator/service provider to take all due action to prevent such an event from occurring in future.

12. Law-enforcement agencies require that all people who handle or control interception orders or who are involved in the interception process, have undergone a security check, as required by national authorities.

12.1. A list with the names and job descriptions of such persons has to be handed over to the Law-enforcement agencies.

13. Law-enforcement agencies require the network operator/service provider to take all necessary organisational and technical measures in order to protect all technical interfaces used to route intercepted telecommunications and all administration components serving to implement or change interceptions, from abuse.

13.1. The network operator/service provider has to assure that the integrity and the confidentiality of the interception data during transmission is safeguarded to the level required by the Law-enforcement agencies. All communication lines used for interception purposes are therefore to be protected.

13.2. Law-enforcement agencies require that information with regard to the actual interceptions implemented in a particular telecommunications system not be made available to unauthorised persons.

14. Law-enforcement agencies require that the sites containing interception orders and data be restricted areas with controlled access. The network operator/service provider has to notify the Law-enforcement agencies about the location of the sites and the security measures implemented, and has to hand over a list of the employees who have authorised access to these sites.

14.1. Law-enforcement agencies require the network operator/service provider to store the interception order as specified by national security standards. The network operator/service provider is not allowed to store the call content.

C. REQUIREMENTS RELATING TO SERVICE PROVIDERS WITH REGARD TO CRYPTOGRAPHY

15. Based on a lawful enquiry and given a target identifier or other information about the target or encrypted data with related information, law-enforcement agencies require:

- **full details of the target including service number;**
- **information that will fully identify the cryptographic services used by the target and**
- **the technical parameters of the method used to implement the cryptographic service.**

16. Law-enforcement agencies require access to the decrypted message as quickly as possible (in urgent cases within a few hours or minutes). The law-enforcement agency will specify how it wishes to achieve this result; either through the provision of cryptographic key material and all necessary information to decrypt the data or by provision of the data en clair. Access to the decrypted message must be available for those encryption systems that allow for both national and international operation.

16.1. The handover of cryptographic key material should be immediate. The computational and operational process a law-enforcement agency needs to undertake to decrypt the data, including any reconstruction or rebuilding of keys, should involve minimal time and resources to ensure an efficient, economic and timely operation.

16.2. The provision of data en clair should take place as soon as possible, in urgent cases within a few hours or minutes.

17. Law-enforcement agencies require the decryption process to be designed and implemented so as to preclude unauthorised or improper use and to safeguard the information relation to the operation.

17.1. Where cryptographic key material is being provided, it must be delivered either in electronic format or another agreed format using a secure means of transmission. This must be protected to ensure the authenticity, integrity and confidentiality of such material, and it must be provided in a non-repudiational manner.

17.2. The cryptographic key material or data en clair must only be transmitted to the agency specified in the authorisation.

17.3. Law-enforcement agencies require providers of cryptographic services not to disclose to the target or any third party:

*** that there has been an authorisation;**

*** the target of the authorisation;**

*** that cryptographic key material data en clair has been supplied, and**

*** any information on how the operation has been carried out.**

18. Subject to national regulations, providers could be obliged to maintain an adequately protected record of provision of key material and data which may nevertheless only be made available to authorised personnel.

Part 3: Additional definitions supplementing the Glossary contained in the Council Resolution of 17 January 1995

CALL (Glossary OJ 96/C 329/01)

Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.

DATA (New)

The representation of information in a manner suitable for communication, interpretation, storage or processing.

QUALITY OF SERVICE (Glossary OJ 96/C 329/01)

The quality specification of a communications channel, system, virtual channel, computer-communications 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.

AUTHENTICITY (New)

Establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.

DECRYPTION (New)

The inverse function of encryption.

LAW-ENFORCEMENT AGENCY (Glossary OJ 96/C 329/01)

A service authorised by law to carry out telecommunications interceptions.

LAW-ENFORCEMENT AGENCY WITH REGARD TO CRYPTOGRAPHY (New)

An organisation authorised by law to receive cryptographic key material and all necessary information to decrypt the data or the data en clair.

HOST (New)

Any (end-user) computer system that connects to a network.

INTEGRITY (New)

The property that data or information has not been modified or altered in an authorised manner.

INTERNET (New)

The collection of networks and gateways that use the TCP/IP protocol suite and function as a single, cooperative virtual network.

INTERNET PROTOCOL/IP (New)

Internet Protocol. The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an internet and provides the basis for connectionless, best-effort packet-delivery service. IP includes the ICMP (Internet Control and Error Message Protocol) as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.

IP ADDRESS/Internet-Address (New)

The 32-bit address assigned to hosts that want to participate in a TCP/IP internet.

IP DATAGRAM (New)

The basic unit of information passed across a TCP/IP internet. It contains a source and destination address along with data.

IUR (New)

International User Requirements for Interception.

PLAINTEXT/EN CLAIR (New)

Intelligible data.

CRYPTOGRAPHY (New)

The discipline which embodies principles, means and methods for transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorised use.

CRYPTOGRAPHIC SERVICES (New)

The facilities which provide cryptographic services.

CRYPTOGRAPHIC KEY (New)

Parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

NETWORK OPERATOR/SERVICE PROVIDER (Glossary OJ 96/C 329/01)

Network operator = the operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means, and

Service provider = the natural or legal person providing a public telecommunications service whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks.

LAWFUL AUTHORISATION (Glossary OJ 96/C 329/01)

Permission granted to a law-enforcement agency under certain conditions to intercept specified telecommunications. Typically this refers to an order or warrant issued by a legally-authorised body.

ROAMING (Glossary OJ 96/C 329/01)

The ability of subscribers to mobile telecommunications services to place, maintain and receive calls even when they are located outside their designated home-service area.

SESSION (New)

A related set of transactions between the same two parties.

TCP (New)

Transmission Control Protocol. The TCP/IP standard transport level protocol that provides the reliable, full duplex, stream service on which many application protocols depend.

TELECOMMUNICATION (Glossary OJ 96/C 329/01)

Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnet, photoelectronic or photo-optical system.

INTERCEPTION (Glossary OJ 96/C 329/01)

As used here, the statutory-based action of providing access and delivery of a subject's telecommunication and call-associated data to law-enforcement agencies.

INTERCEPTION ORDER (Glossary OJ 96/C 329/01)

An order placed on a network operator/service provider for assisting a law-enforcement agency with a legally-authorised telecommunications interception.

INTERCEPTION DATA (New)

It means call content, call-associated data and subscriber-related data.

LAW-ENFORCEMENT MONITORING FACILITY (Glossary OJ 96/C 329/01)

A law-enforcement facility designated as the transmission destination for the intercepted communications and call-associated data for a particular interception subject. The site where monitoring/recording equipment is located.

INTERCEPTION INTERFACE (Glossary OJ 96/C 329/01)

The physical location within the network operator's/service provider's telecommunications facilities where access to the intercepted communications or call-associated data is provided. The interception interface is not necessarily a single, fixed point.

INTERCEPTION SUBJECT (Glossary OJ 96/C 329/01)

Person or persons identified in the lawful authorisation and whose incoming and outgoing communications are to be intercepted and monitored.

TARGET SERVICE (Glossary OJ 96/C 329/01)

A service associated with an interception subject and usually specified in a lawful authorisation for interception.

CALL-ASSOCIATED DATA (Glossary OJ 96/C 329/01)

Signalling information passing between a target service and the network or another user. Includes signalling information used to establish the call and to control its progress (e.g. call hold, call handover). Call-associated data also includes information about the call that is available to the network operator/service provider (e.g. duration of connection.

AVAILABILITY (New)

The property that data information and information and communications systems are accessible and usable in a timely basis in the required manner.

ENCRYPTION (New)

The transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

CONFIDENTIALITY (New)

The property that data or information is not made available or disclosed to unauthorised individuals, entities or processes.

ACCESS (Glossary OJ 96/C 329/01)

The technical capability to interface with a communications facility, such as a communications line or switch, so that a law-enforcement agency can acquire and monitor communications and call-associated data carried on the facility.

RELIABILITY (Glossary OJ 96/C 329/01)

The probability that a system or service will perform in a satisfactory manner for a given period of time when used under specified operating conditions.