International Packet Communications Consortium

Lawfully Authorized Electronic Surveillance For Softswitch-based Networks

July 2003

2694 Bishop Drive, Suite 275

San Ramon, CA 94583

+1 925 275 6635

www.packetcomm.org

Note: Development of this document was suspended in consideration of similar work being performed in other industry/standards groups. This document is NOT complete and does NOT offer Safe Harbor under CALEA.

Table of Contents

Table of Figures

1 Introduction & Background

This informational document describes services and features to support lawfully authorized electronic surveillance of packet-mode communications provided by Telecommunications Carriers. Use of a specific packet-mode data protocol or technology does not imply that any person or entity utilizing this protocol or technology is or is not a Telecommunications Carrier, nor does it imply, implicitly or explicitly, the applicability of assistance capability requirements set forth in Section 103 of the Communications Assistance for Law Enforcement Act [CALEA] to such person or entity.

1.1 Scope

The purpose of this document is to record the lawful intercept work done by the International Packet Communications Consortium's (IPCC's) Legal Intercept (LI) Working Group. This document describes the interfaces between a Telecommunications Carrier that provides telecommunications services and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance.

This document demonstrates the progress made by the IPCC LI group in their initial efforts to define a CALEA Safe Harbor document for Softswitch-based Networks. The group addressed CALEA requirements for the benefit of any affected party who might use this architecture or technology. However, since the document is incomplete, it does not provide "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001 et seq and is furnished for information only.

This document defines technical requirements to support Lawfully Authorized Electronic Surveillance, and the interfaces to deliver intercepted communications and reasonably available call-identifying information to a LEA.

The IPCC is an industry association that, in addition to providing a forum for promoting global compatibility and interoperability of SIP and softswitch operation, may sponsor technical specifications. The Telecommunications Industry Association (TIA) has promulgated a safe harbor specification [J-STD-025A] for Lawfully Authorized Electronic Surveillance for traditional voice telephony. In addition, CableLabs™ has promulgated a safe harbor specification [PKT-SP-ESP-101-991229] for Lawfully Authorized Electronic Surveillance for telephony using the PacketCable™ architecture. However, the electronic surveillance features provided for in J-

STD-025A are not readily applicable to telephony provided by means of softswitch-based networks. Furthermore, the electronic surveillance features provided for in PKT-SP-ESP-101-991229 were designed for use only by cable operators. Accordingly, the IPCC initiated development of a specification for electronic surveillance specific to telephony services provided over softswitch-based networks. Since the inception of the IPCC effort, other standards groups have progressed in addressing the needs of the IPCC, specifically with regard to electronic surveillance of voice service over managed packet networks. Therefore, to avoid redundancy of effort and development of potentially inconsistent specifications, the IPCC has suspended work on this document. The IPCC shall monitor the efforts of those other groups for completeness with respect to the scope of IPCC architectures and services and for consistency with the requirements and objectives of the IPCC Carrier Community. The IPCC may resume work on this document if it determines the needs and requirements of its members are not being met by other organizations.

1.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED, "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.3 Electronic Surveillance Requirements

In connection with certain facilities and services, CALEA requires telecommunications carriers to provide specified capabilities to LEAs when presented with the proper lawful authorization. CALEA also requires manufacturers of equipment used in connection with the covered telecommunications facilities and services to make available the features or modifications necessary to permit carriers to comply with the capabilities requirements.

More specifically, in connection with services provided by telecommunications carriers (but not information services) that provide customers with the ability to originate, terminate, or direct communications, CALEA requires telecommunications carriers to ensure that their equipment, facilities, or services have the capability, pursuant to a court order or other lawful authorization, to:

1. Expeditiously isolate and enable the LEA to intercept all communications (i.e., call content) carried by a carrier within a service area to or from the equipment, facilities, or services of a subscriber, concurrently with the communications' transmission.

2. Expeditiously isolate and enable the LEA to access reasonably available call-identifying information, concurrently with the communications' transmission and in a manner that correlates with such communications.

3. Deliver the intercepted communications and call-identifying information to the LEA so they may be transmitted over facilities procured by the LEA to a location away from the carrier's premises.

4. Meet these requirements unobtrusively, with a minimum of interference with the subscriber's services, and in a manner that both protects the privacy of communications and call-identifying information that are not authorized to be intercepted and maintains the confidentiality of the LEA's wiretaps.

As a precondition for a carrier's assistance with Lawfully Authorized Electronic Surveillance, a LEA must serve the telecommunications carrier with the necessary legal authorization, which typically consists of a court order. Once this authorization is provided to the telecommunications carrier, federal and state law requires the carrier to assist the LEA in effectuating the authorized surveillance. CALEA specifies the type of communications information that carriers must access and deliver expeditiously to the Collection Function. Only communications initiated after receipt of necessary legal authorization by the telecommunications carrier may be intercepted.

1.4 Electronic Surveillance Assumptions

CALEA does not authorize any LEA or law enforcement officer to require any specific design of equipment, facilities, services, features, or system configurations. Nor does CALEA prohibit the adoption of any equipment, facility, service, or feature by any telecommunications provider.

CALEA does not prohibit a telecommunications carrier from transporting encrypted communications. If, however, the carrier provides the encryption and possesses the information necessary to decrypt the communication, then CALEA requires the carrier to assist LEAs in decrypting the communication.

CALEA mandates capacity requirements as well as capability requirements with which carriers and manufacturers must comply. CALEA's capacity requirements are beyond the scope of this document.

1.5 Definitions and Acronyms

LAES Lawfully Authorized Electronic Surveillance

SP Service Provider: Within this document, this term refers to a telecommunications carrier as defined in Section 102 in CALEA that may be providing a service to which CALEA applies.

DP Demarcation Point: The Demarcation Point is the point between the Delivery Function and Collection Function where the transport responsibility of the Service Provider ends and that of the Law Enforcement Agency begins.

cut-through: When an endpoint has received via call signaling the information needed to communicate with the remote endpoint and a communication path exists from the endpoint to the remote endpoint.

1.6 References

[CALEA] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C. §§ 229, 1001-1010, 1021).

[FCC3] Communications Assistance for Law Enforcement Act, Third Report and Order, CC Docket No. 97-213, 14 FCC Rcd 16794 (1999).

[FCCOR] Communications Assistance for Law Enforcement Act, Order on Remand, CC Docket No. 97-213, FCC 02-108, Released 4/11/2002

[J-STD-025A] ANSI/J-STD-025-A-2003, Lawfully Authorized Electronic Surveillance, 2003.

[PKT-SP-ESP-101-991229] PacketCable™ Electronic Surveillance Specification, PKT-SP-ESP-I01-991229, Cable Television Laboratories, Inc., 12/29/1999

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

2 Electronic Surveillance In A Softswitch-based Network

Figure 1 provides a reference diagram for LAES showing key functions. The two shaded boxes separate functions within the service provider (SP) network from those in the Law Enforcement Agency (LEA). The demarcation point shown on the diagram is where the responsibility of SP ends and that of the LEA begins. One of the major purposes of this document is to describe the two interfaces at this demarcation point:

- The call content interface, and
- The interface for call-identifying information

Internal interfaces within the SP and LEA networks will not be described. However, this section will give a brief description of the various functions involved.

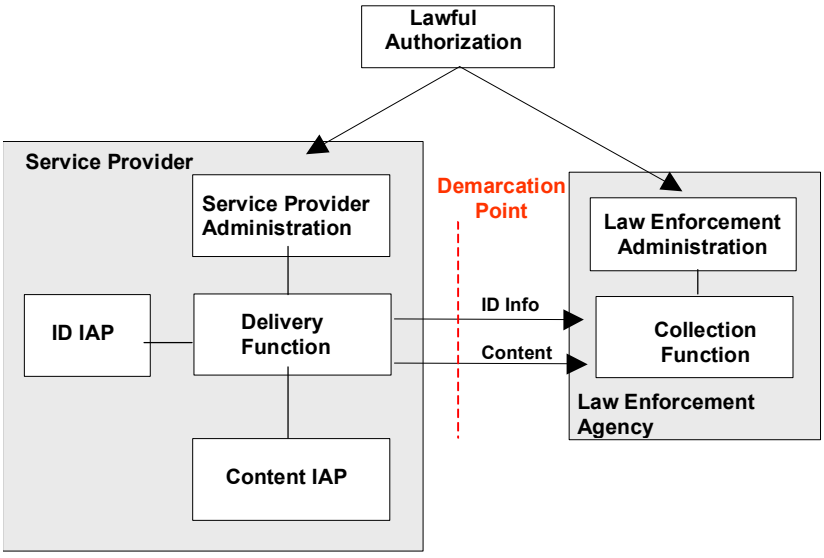

Figure 1 - Reference Diagram for LAES

The key functions involved in LAES can be briefly broken down into:

- Administration
- Access:
  - To Call-Identifying Information: shown on the diagram as the ID Intercept Access Point (ID IAP)

- To Call Content Information: shown on the diagram as the Content Intercept Access Point (Content IAP).

- Delivery

- Collection

These functions are described in more detail in the following sub-sections. The subscriber's customer premises equipment (CPE) is also described although it is not directly involved in LAES.

2.1 Administration Function

Administration functions are available within both the service provider network and the LEA for provisioning Lawful Intercepts. These are referred to here as the Service Provider Administration Function (SPAF) and Law Enforcement Administration Function (LEAF).

2.1.1 Service Provider Administration Function (SPAF)

The SPAF is the provisioning interface for LAES within the Service Provider's Network. This function may be provided as an interface to one or more components that are involved in LAES within the Service Provider's network (e.g. the component that also provides the Delivery Function).

2.1.2 Law Enforcement Administrative Function (LEAF)

The LEAF is the provisioning interface for LAES within the LEA. The LEAF is responsibility of the LEA.

2.2 Access Function (AF) and Intercept Access Points (IAPs)

Access functions are of two types: functions that provide access to call-identifying information (ID Intercept Access Points), and Content Intercept Access Points.

2.2.1 ID Intercept Access Point

An ID Intercept Access Point (ID IAP) is a point in the service provider's network where access call-identifying information can be obtained and sent to the delivery function. Call-identifying information refers to data about a call such as the number dialed, information as to when the call was made, etc. One example of an ID IAP in a softswitch-based network might be a Call

Agent/Media Gateway Controller, although other components (e.g. SIP Proxy) may also be considered ID IAP(s).

2.2.2 Content Intercept Access Points

Content intercepts MUST not be detectable by the subscriber under surveillance and as such, content interception MUST not involve:

- Special requests to the subscriber equipment, or
- Special treatment of the media stream that may be detectable by the subscriber's equipment.

The best candidate for a Content Intercept Access Point (Content IAP) is an existing component that is along the normal media path for the call.

[Editor's Note: Need contributions to align subscriber equipment with Section 2.5]

2.3 Delivery Function (DF)

The Delivery Function receives the data from the Content and ID IAPs. It then formats the call content and call-identifying information into the formats described in sections 4 and 5 of this document and delivers it to the LEA. In cases where multiple law enforcement agencies are performing LAES on the same subject, the Delivery Function must provide the required information to each of the LEAs in a transparent manner (i.e. in a manner such that a given LEA will only receive the information relevant to its authorization request).

2.4 Collection Function (CF)

The Collection Function receives the call content and call-identifying information from the Delivery Function and presents it to the LEA. The Collection Function is the responsibility of the LEA.

2.5 Subscriber Equipment

The subscriber equipment is the customer premises equipment (CPE) being used by the subscriber under surveillance. It may be managed/controlled by components within the service provider network in order to provide a service (i.e. telephony). However, the CPE cannot be directly controlled for the purposes of providing LAES since that would be detectable (i.e. it

cannot be a content IAP). As such, the details of the control and operation of the subscriber equipment are not described in this document.

3 Interface Between The Delivery Function & Collection Function

One of the primary purposes of this document is to describe the interface between the Delivery Function and the Demarcation Point. The Demarcation Point, which is between the Delivery Function and Collection Function (as illustrated in Figure 1) is the point where the responsibility of the Service Provider ends and that of the Law Enforcement Agency begins.

Call content and call-identifying information are formatted as described in sections 4 and 5 of this document, respectively, and delivered to a LEA at the Demarcation Point. The delivery of call-identifying information and call content will not necessarily be synchronized when received by a LEA. The call content and call-identifying information will be delivered to a LEA on call content connections (CCCs) and call data connections (CDCs) respectively, and MAY be provided over different networks or different facilities.

Procurement, engineering, and sizing of the physical facilities connecting the Demarcation Point to the Collection Function (CF) are the responsibility of the LEA. Engineering and sizing of the Collection Function is also the responsibility of the LEA. If the LEA provides insufficient transmission capacity to the LEA's Collection Function, then the intercepted information MAY be delayed or discarded by the Delivery Function.

3.1 General Interface Requirements

It is the Service Provider's responsibility to deliver call content and call-identifying information to a Demarcation Point. The Demarcation Point consists of a physical interconnect adjacent to the DF. The LEA is responsible for providing the equipment, facilities, and maintenance needed to deliver this information from the Demarcation Point to the CF.

This document defines a default physical and link level interface at the Demarcation Point. It is left to the discretion of any affected Service Provider whether to provide alternative interconnect choices.

The Service Provider MUST ensure that only those packets that have been authorized to be examined by the LEA are delivered to the Demarcation Point. If there is more than one LEA doing surveillance on the Service Provider's network at a given point in time, the Service Provider MUST send to each LEA only the data that the LEA is authorized to receive.

3.2 Transport Layer

3.2.1 Call Data Connection (CDC)

Call-identifying information is transported from the Delivery Function to the Collection Function over a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. The TCP/IP connection MUST be capable of transporting call-identifying information for multiple surveillance cases to a given LEA. The format of the call-identifying messages is described in section 5 of this document.

3.2.2 Call Content Connection (CCC)

The Service Provider is responsible for the delivery of call content to the Demarcation Point over User Datagram Protocol (UDP). The LEA might transport the call content via some other transport (e.g., TCP) from the Demarcation Point to the Collection Function. Section 4 describes the format of messages used in the Call Content Connection.

3.3 Network Layer Interface

The Internet Protocol (IP) is the network layer protocol used for delivery of both call-identifying and call content information.

Contained in the IP header is the source IP address, which is the address of the DF, and the destination IP address, which is the address of the CF provided by the LEA. All transfer of packets other than those operationally required to maintain the link MUST be from the DF to the CF only. The LEA MUST NOT send unsolicited packets from the CF to the DF.

3.4 Link-layer Interface

Ethernet is the default link-layer protocol between the DF and the Demarcation Point. However, alternate link-layer protocols MAY be used at the discretion of the SP based on negotiated agreements with the LEA.

3.5 Security

The Service Provider is not required to supply encryption on call content and call data connections between the DF and the Demarcation Point. However, the LEA could provide encryption from the Demarcation Point to the CF by supplying the necessary equipment and facilities.

3.6 Reliability

In a case where there is a network failure between the DF and Demarcation Point or between the DF and CF, the call content and call-identifying information MAY be lost. However, call-identifying information MAY be temporarily stored until the network is restored.

4 Call Content Connection (CCC) Interface

This section describes the packet format for call content connections between the DF and the Demarcation Point. Call content MUST be delivered as a stream of UDP/IP datagrams sent to an IP address and UDP port number provided by the LEA. The UDP/IP payload consists of the intercepted IP packet with a 32 bit Call Content Connection Identifier (CCC ID) added as shown in Figure 2.

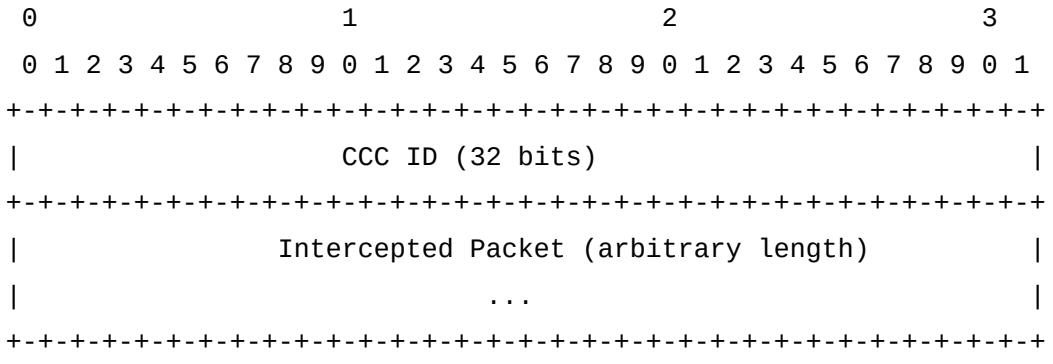

Figure 2 Call Content Connection Packet Format

4.1 Call Content Connection Identifier (CCC ID)

A 32-bit CCC ID is provided with each CCC packet as shown in Figure 2. The CCC ID is provided by the Delivery Function in CCOpen messages along with the intercept case identifier (Case_Identity). This allows the LEA to correlate a given CCC with a particular intercept order.

A communication between two endpoints in a network typically consists of two separate packet streams, each corresponding to a direction of the communication. The packet streams MUST be delivered to the Demarcation Point either with the same CCC ID for both streams or with a different CCC ID for each stream. The party listening to the communication is identified by the combination of Destination Address (from Original IP Header) and Destination Port (from the Original UDP Header). The Destination Address and Destination Port for both parties involved in the communication are provided in the Session Description Protocol (SDP) session description provided to the LEA as part of the CCOpen message (refer to section 5 for details).

[Editor's Note: There was a request to change this text to allow different CCC ID's per direction.]

4.2 Intercepted Packet

The Intercepted Packet field contains the original intercepted packet to be delivered to the LEA. This packet is delivered without modification by the Service Provider.

[Editor's Note: Contributions are welcome on text clarifying encapsulation.]

4.2.1 Original IP Header

The original IP packet with the original header information is provided in the payload of the CCC packet. Contained within the IP header is the IP Source Address and IP Destination Address that identify the IP addresses of the source and destination of the original packet. The IP addresses are provided in the SDP session description in the CCOpen message.

4.2.2 Original UDP Header

The source and destination ports for the intercepted packet can be obtained from original UDP header which is included as part of the Intercepted Packet Field. The UDP ports are provided in the SDP session description in the CCOpen message.

4.2.3 Original Payload

The original payload of the communication is contained in the UDP data field of the intercepted packet. A description of the payload characteristics (codec, etc.) is provided by the SDP session description included with the CCOpen message; however, the payload is carried end-to-end transparently to the SP. The SP cannot guarantee that the information carried in the payload matches what is in the SDP session description provided in the CCOpen message.

In cases where the Real-Time Transport Protocol (RTP) is used for communications (e.g., normal voice calls), the original payload contains the RTP header and RTP Payload. The RTP header contains the original packet sequence number, packet formation timestamp and RTP payload type as generated by the source endpoint. The payload type value along with the name of the associated codec is also referenced in the SDP session description provided in the CCOpen message.

In the case of voice, the RTP Payload contains the voice samples. If the SDP session description received by the SP contains encryption and encoding information, this information will be delivered to the LEA in the SDP session description contained in the CCOpen message.

5 Call Data Connection (CDC) Interface

5.1 CDC Message Descriptions

This section describes the CDC messages sent by the Delivery Function to the Collection Function.

Each message is described as consisting of a set of parameters. Each parameter is either:

- mandatory (M) — required for the message,
- conditional (C) — required in situations where a condition (defined in the usage column of the table row in which it appears) is met, or
- optional (O) — provided at the discretion of the implementation.

Whether the parameter is mandatory, conditional or optional is indicated in the “Type” column of the parameter table for each message. The information to be carried by each parameter is identified. Please note that both optional and conditional parameters in the CDC message descriptions (in Section 5.1) are considered to be OPTIONAL syntactically in the ASN.1-based CDC message definitions (in Section 5.2). The message description inclusion requirements MUST take precedence over the message definition syntax.

5.1.1 Answer

The Answer message reports when a call or call leg has been answered.

The Answer message MUST be generated when an IAP detects one of the following events:

a) The intercept subject answers a call or call leg (including calls for which the intercept subject is alerted in response to a previous call).

b) A call originated by the intercept subject is answered or cut-through in both directions.

c) A call for which the intercept subject is the destination is terminated at another endpoint or agent due to special call handling or redirection by the softswitch (e.g., call forwarding, voicemail).

The Answer message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system, where applicable. *[Editor's Note: Insert the following descriptive text in the Parameter Definition section in 5.2.9 for CallIdentity: "The CallIdentity included in this message is the same as in the message that created the CallIdentity for this call, call appearance or call leg."]*
AnsweringPartyIdentity	C	Include to identify the answering party or agent, when known.
Location	C	Include to identify the location of the intercept subject's mobile wireless terminal (e.g., cell site, sector and/or other information) when known and access to location information is authorized.

[Editor's Note: Possibly move other descriptive or procedural information to Section 5.2.9. Maintain the description of the parameter and the conditional in the table.]

[Editor's Note: Discussions regarding inclusion of media information in this message or in a separate media reporting message are incomplete.]

[Editor's Note: A proposal to update all occurrences of the description of the Location parameter in the baseline text to support both personal and terminal mobility was not addressed due to suspension of work on the document.]

5.1.2 CCChange

The CCChange message reports a modification to the media characteristics (e.g., network address, media format) of an existing call. The CCChange message is generated for surveillances that require the delivery of call content and provides the LEA collection equipment with the updated information needed to process the voice packets for the call.

The CCChange message MUST be generated for surveillances that require the delivery of call content when call content is delivered to the LEA as packets and an IAP detects that the media characteristics of an active call under surveillance have been modified.

The CCChange message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
OriginatingMediaInformation	C	Include to identify the new media characteristics (e.g., network address, media format) for the originating endpoint, when the characteristics have changed. This attribute could be SDP information.
TerminatingMediaInformation	C	Include to identify the new media characteristics (e.g., network address, media format) for the terminating endpoint, when the characteristics

		changed. This attribute could be SDP information.
CCCIdentity	M	Uniquely identifies a CCC.
Direction	M	Include to identify the direction of the media stream (from the originating endpoint, from the terminating endpoint or both).

5.1.3 CCClose

The CCClose message reports the disabling of delivery of call content to the LEA.

The CCClose message MUST be generated for a call or call leg under surveillance when a CCC has been opened (through a CCOpen message) and an IAP detects through call signaling that the call or call leg is released or merged with another call or call leg.

The CCClose message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CCCIdentity	M	Uniquely identifies a CCC.

5.1.4 CCOpen

The CCOpen message reports the start of delivery of call content. The CCOpen message is generated for surveillances that require the delivery of call content.

For surveillances that require the delivery of call content, the CCOpen message MUST be generated when call content delivery is enabled.

[Editor's Note: Further work is needed to identify what happens when the Softswitch provider doesn't have access to call content. This could occur on a per-call basis (e.g., call forwarding) or on a permanent basis.]

The CCOpen message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system, where applicable.
OriginatingMediaInformation	C	Include to identify the media characteristics (e.g., network address, media format) for the originating endpoint when call content is delivered as packets and either: 1. a combined CCC is used, or 2. separate CCCs are used and the connection direction is from the originating endpoint. This attribute could be SDP information.
TerminatingMediaInformation	C	Include to identify the media characteristics (e.g., network address, media format) for the terminating endpoint when call content is delivered as packets and either: 1. a combined CCC is used, or 2. separate CCCs are used and the connection direction is from the terminating endpoint. This attribute could be SDP information.
CCCIdentity	M	Uniquely identifies a CCC.
Direction	M	Include to identify the direction of the

		media stream (from the originating endpoint, from the terminating endpoint or both).

5.1.5 Change

The Change message reports a change in call identity(ies).

The Change message MUST be generated when an IAP detects one of the following events:

a) Two or more call identities are merged into one call identity.

b) An additional call identity is now associated with an existing CCCIdentity.[1]

c) A call identity is split into two or more call identities.

d) A call identity is changed to another call identity.

This message is not required when the information reported would duplicate information reported by other LAES messages.

The Change message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
PreviousCalls	M	Identifies all of the existing calls to which the change applies. A CallIdentity that is

[1] Trigger (b) applies to a CALEA implementation where a separate call identity is used for each call leg of a multi-party call sharing the same call content channel (same CCCIdentity). For example, within the operation of a three way calling scenario, the intercept subject, while on a two-way communication mode with the intercept associate (call id #1), hook-flashes to initiate the second leg (call id #2). The switch places the first leg on hold. As an implementation choice, the IAP may use the same call content channel for the second leg. In this case, a new call identity is associated (i.e., when the second leg is initiated) with an existing CCC Identity.

In this example, when the intercept subject hook-flashes a second time to join the two call legs into a three-way conference, the two call identities can be merged into one call identity (trigger (a)). An alternative implementation might treat the two separate call legs as separate calls and will issue an Originate instead of a Change.

Even though a call content channel is not used in a call data only type of intercept (e.g., Pen Register), trigger point (b) can still be used in an implementation where a separate call identity is used with each leg of a multi-party call and the IAP wishes to associate all the call identities associated with the multi-party call.

		contained in the PreviousCalls parameter, but not in the ResultingCalls parameter, is released and MAY be reassigned to other calls.
ResultingCalls	M	Identifies the CallIdentity(ies) and CCCIdentity(ies) for each of the resulting calls. The Change message MAY generate new unique CallIdentity(ies) in the ResultingCalls parameter.

[Editor's Note: A substantial amount of explanatory text is required (Section 5.2.9?) to explain the usage of this message and the parameters for each of the events described (a-d).]

5.1.6 MediaReporting

[Editor's Note: Discussion on proposal to include this message is incomplete.]

5.1.7 NetworkSignal

The NetworkSignal message reports signals generated or sent by the softswitch-based network toward the intercept subject.

The NetworkSignal message MUST be generated when an IAP detects that the softswitch initiates or receives information that indicates the occurrence of one of the following events:

a) Application of alerting toward the intercept subject.

b) Application of a network-initiated tone toward the intercept subject (e.g., dial tone, busy tone, ringback tone, recall tone, DTMF tones).

c) Sending of a call-associated display message toward the intercept subject (e.g., identifying the calling party name and number, providing a message waiting indicator, providing call progress).

d) Application of a call-associated network announcement toward the intercept subject.

e) Sending of a message toward the intercept subject's equipment to instruct it to remove tones or visual indicators.

The NetworkSignal message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Uniquely identifies a call, call appearance, or call leg within a system, where applicable, when the network signal is associated with a particular call.
SubscriberIdentity	C	Include to identify the subscriber, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity. *[Editor's Note: This parameter needs to be synchronized with other standards groups.]*
Signal One or more of the following:	M	Identifies the audio signals, visual signals, or displayed text applied by the softswitch-based network that would normally be sensed by the intercept subject.
AlertingSignal	C	Include when alerting is applied toward the intercept subject.
SubjectAudibleSignal	C	Include when an audible signal is applied toward the intercept subject.
TerminalDisplayInfo	C	Include when a display message is sent toward the intercept subject.
Other	C	Include when DTMF digits are signaled toward the intercept subject or standard announcements are played toward the intercept subject. Can also be used as an alternative means of reporting the signaling information.

5.1.8 Origination

The Origination message reports call originations and call origination attempts by the intercept subject.

The Origination message MUST be generated when an IAP detects one of the following events:

a) A call or call leg is originated by the intercept subject and routed toward an on-net or off-net destination.

b) The destination address for a call or call leg originated by the intercept subject is translated to another address (e.g., speed number expansion, toll-free number translation).

c) A call is attempted by the intercept subject, but the softswitch-based network cannot complete the call. This includes the case of receipt of complete, partial or no addressing information.

d) A call is attempted by the intercept subject, but the intercept subject abandons the call. This includes the case of receipt of complete, partial or no addressing information.

A call origination might be initiated by use of a feature code (e.g., *69). Such a feature code would be included as UserInput or InterimTranslationInput

The triggers MAY be supported through the generation of one or multiple Origination messages, as long as the required information is reported.

The Origination message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance or call leg within a system, where applicable. *[Editor's Note: Insert the following explanatory text in 5.2.9: "The CallIdentity included in this message is used to correlate with other messages."]*

CallingPartyIdentity	M	Include to identify the calling party.
CalledPartyIdentity	C	Include to identify the called party (e.g., result of final translation if any), when known. This parameter is not included for partially dialed calls.
UserInput	C	Include to identify the input digits, address or name signaled by the calling party to originate the call, when known. One and only one of UserInput or InterimTranslationInput MUST be present in this message..
InterimTranslationInput	C	Include to identify the input to an interim address translation process, when an interim address translation occurs. One and only one of UserInput or InterimTranslationInput MUST be present in this message.
Location	C	Include to identify the location of the intercept subject's mobile wireless terminal (e.g., cell site, sector and/or other information) when known and access to location information is authorized.
TransitCarrierIdentity	C	Include to identify the transit carrier, when a transit carrier is involved and the transit carrier identity is known.

[Editor's Note: A new MediaReporting message is to be defined to carry call media parameters]

[Editor's Note: Discussion on proposal to modify this message to report address resolution and admission control is incomplete.]

5.1.9 Redirection

The Redirection message reports when a call is redirected such that the intercept subject's equipment, facilities or service causes or is made aware of the call redirection. For example, Call redirection can occur for features such as call forwarding (e.g., call forwarding variable, call forwarding busy, selective call forwarding). Call redirection could also occur for an intercept subject having terminal or personal mobility to redirect calls to the subject's current location.

The Redirection message MUST be generated when an IAP detects one of the following events:

a) An incoming call attempt to the intercept subject is redirected by the intercept subject's service (e.g., call forwarding, terminal or personal mobility).

b) An incoming call attempt to the intercept subject is redirected by the intercept subject's action (e.g., call waiting deluxe).

c) For implementations in which call transfers are treated as redirections, an answered call is redirected by the intercept subject (e.g., call transfer). The answered call could originally have been originated by or terminated to the intercept subject.

The Redirection message MAY be generated when the IAP detects that a call originated, terminated or redirected by the intercept subject is subsequently redirected (forwarded, deflected or transferred) by an associate such that the intercept subject's equipment, facilities or service is made aware of the redirection.

The Redirection message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system., where applicable
NewCallIdentity	C	Included when the redirected call will be identified by a different CallIdentity in future messages. When NewCallIdentity is included, the call identity included in the CallIdentity parameter is released and MAY be reassigned to other calls.

RedirectedFromPartyIdentity	C	Include to identify the party from whom the call is redirected if known.
RedirectedToPartyIdentity	M	Identifies the redirected-to party.
TransitCarrierIdentity	C	Include to identify the transit carrier, when a transit carrier is involved and the transit carrier identity is known.
VisitedSystemIdentity	C	Include to identify the system to which the call has been redirected, when a call to an intercept subject is redirected by the intercept subject's service to another SP and the system identity of that SP is known..

[Editor's Note: The parameters description section should include text describing the ambiguity of Redirection & RedirectedFromPartyIdentity in the following cases:

The redirected-to party redirects the call again.

The associate redirects the call (with subsequent redirections).]

5.1.10 Release

The Release message reports the release of the resources used for a call, call appearance or call leg.

The Release message MUST be generated when an IAP detects one of the following events:

a) A call attempt is abandoned by the calling party.

b) An answered call is released (including abnormal release detected by the softswitch-based network).

The Release message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system., where applicable.
Location	C	Include to identify the location of the intercept subject's mobile wireless terminal (e.g., cell site, sector and/or other information) when known and access to location information is authorized.
ReleaseCause *[Editor's Note: new; further study required]*	C	Include to identify the cause of the call release (e.g., normal call clearing, call rejected), when known.

[Editor's Note: Discussion on proposal to modify this message to report address resolution and admission control is incomplete.]

5.1.11 ServingSystem

The ServingSystem message reports the identity of the visited SP providing service to an intercept subject with terminal or personal mobility, when the terminal or intercept subject is authorized for service.

The ServingSystem message MUST be generated when an IAP detects that an intercept subject or terminal of an intercept subject has been authorized for service with another SP or in another service area.

The ServingSystem message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
VisitedSystemIdentity	C	Include to identify the visited SP, when known.
NetworkAddress	C	Include to identify the network address of the network element providing service to the intercept subject, when known.

[Editor's Note: Usage of VisitedSystemIdentity and NetworkAddress needs to be clarified.]

[Editor's Note: Discussion of proposal to modify the ServingSystem message to cover reporting of address registration and deregistration is incomplete.]

5.1.12 SubjectSignal

The SubjectSignal message reports dialing and signaling initiated by the intercept subject to control (including invocation and use) a feature or service (e.g., call forwarding, call waiting, call hold, three-way calling). *[Editors Note: The following sentence is still under discussion: "The SubjectSignal message* is *generated even when the user input is uninterpretable or results in no change in the control of a feature or service."]*

The subject signal could be call-associated or non call-associated. Digits dialed post cut-through MUST NOT be provided in a SubjectSignal message. These digits are provided in the Dialed Digit Extraction message as defined in Section 5.3.xx.

The SubjectSignal message MUST be generated when an IAP detects that the intercept subject has signaled information to control services or features provided by the softswitch-based network *[Editor's Note: The following parenthetical is still under discussion: "(whether or not sufficient input was provided)"]*.

The SubjectSignal message is not required when the information reported would be redundant with the information reported by other CDC messages.

The SubjectSignal message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Uniquely identifies a call, call appearance, or call leg within a system, where applicable, when the subject signal is associated with a particular call.
SubscriberIdentity	C	Include to identify the subscriber, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity. *[Editor's Note: This parameter is not included in J-STD-025 and is a new requirement in this message.]*
Signal	M	Identifies the signal the IAP detects as originating from the intercept subject.

		Include to report specific subject-initiated input when detected at the IAP.
One or more of the following:		
SwitchhookFlash	C	Included when a switchhook flash is signaled to the Softswitch.
DialedDigits	C	Includes digits signaled by the intercept subject to the Softswitch.
FeatureKey	C	Includes feature key information signaled to Softswitch by intercept subject.
OtherSignalingInformation	C	Included when the intercept subject initiates other signaling information.

5.1.13 TerminationAttempt

The TerminationAttempt message reports an incoming call attempt to the intercept subject. The TerminationAttempt message is sent regardless of the disposition of the call (e.g., busy, answered, redirected).

The TerminationAttempt message MUST be generated when an IAP detects an incoming call to the intercept subject. This includes calls for which the intercept subject receives a call while engaged in an existing call (e.g., call waiting) and calls for which the intercept subject is alerted in response to a previous call.

The TerminationAttempt message includes the following information:

Parameter	Type	Usage
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	M	Identifies the network node containing the IAP.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system, where applicable. *[Editor's Note: Insert the following text in Section 5.2.9: "The CallIdentity included in this message is used to correlate with other messages."]*
CallingPartyIdentity	M	Identifies the calling party, to the extent known.
CalledPartyIdentity	C	Include to identify the called party, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity.
Location	C	Include to identify the location of the intercept subject's mobile wireless terminal (e.g., cell site, sector and/or other information) when known and access to location information is authorized.
RedirectedFromInformation	C	Include when the signaling for the incoming call contains information regarding a previous redirection.

[Editor's Note: Discussion on proposal to modify this message to report address resolution and admission control is incomplete.]

5.1.14 Connection

[Editor's Note: A proposal for text for this section was not addressed due to suspension of work on this document.]

5.1.15 ConnectionBreak

[Editor's Note: A proposal for text for this section was not addressed due to suspension of work on this document.]

[Editor's Note: A proposal to add the following messages was not addressed due to suspension of work on this document:

- *DialedDigitExtraction*
- *FeatureManagement*
- *SurveillanceStatus]*

5.2 CDC Messages and Parameter Definitions

[Editor's note: This section will include a subsection for each message in Section 5.1.]

5.2.1 Answer

5.2.2 CCChange

5.2.3 CCClose

5.2.4 CCOpen

5.2.5 Origination

5.2.6 Redirection

5.2.7 Release

5.2.8 TerminationAttempt

5.2.9 Message Parameters

6 Architectures

[Discussions incomplete.]

Topics for possible inclusion:

SIP

Endpoint SDP negotiation issue

GCP

NCS versus DCS

Single network versus multi-network services

Firewall/NAT issues

7 APPENDIX A – Law Enforcement Perspective (Informative)

The information in this appendix is informative and is intended to provide Law Enforcement's perspective and assist in the development of the requirements contained in this document. This section identifies and describes the lawfully authorized electronic surveillance (LAES) capability from a user perspective; for this capability, the user is Law Enforcement (LE). The description of the user perspective consists of

– the identification and description of surveillance events for which LE needs communication-identifying information,

– description of the "triggers" (actions of subject/associate/network) that indicate when the event is considered to have occurred, and

– description of the information that LE needs for each event.

Understanding the user perspective/needs assists the development of requirements of the Delivery Function and the interface from the Delivery Function to the Collection Function, including the CDC messages that will communicate the event information to LE. (Note that it would not be necessary or even advisable to have a separate message for each surveillance event; however, the message sequence and parameters in the messages must be sufficient for the LE Collection Function to correctly interpret which event has occurred.)

The surveillance events described herein relate to voiceband calls.

It is further recognized that which surveillance events might occur in a specific network implementation are dependent on factors such as (1) the technology deployed, (2) the level of control of the softswitch (e.g., whether the softswitch is actively involved in call setup or simply provides end users with the information needed to directly set up a call), and (3) the features that are available as part of the carrier's service offering.

II. Proposed list of surveillance events

LE needs to be notified if any of the following surveillance events occurs:

1. Registration Events
    a. Terminal Registration

b. Terminal De-Registration

c. Wireless Authorization

2. Call Setup Events

    a. Call Origination

    b. Call Termination Attempt

    c. Call Answer

    d. Call Release

    e. Post-Cut-Through Dialing [*Note: Punch List Item*]

3. Call Management Events

    a. Address Resolution

    b. Call Admission Control

    c. Media Modification

4. Feature Use Events

    a. Call Redirection

    b. Party Hold [*Note: Punch List Item*]

    c. Party Retrieve [*Note: Punch List Item*]

    d. Party Join [*Note: Punch List Item*]

    e. Party Drop [*Note: Punch List Item*]

    f. Call Merge

    g. Call Split

5. Feature Management Events

    a. Feature Activation/Deactivation [*Note: Punch List Item*]

6. Signaling Events

    a. Subject Signal [*Note: Punch List Item*]

    b. Network Signal [*Note: Punch List Item*]

7. Communication Content Events

    a. Content Start

    b. Content Change

    c. Content Stop

8. Surveillance Status Events [*Note: Punch List Item*]

III. Proposed Draft of Surveillance Events Section

This section presents the user's view of surveillance events for a softswitch-controlled network. For each surveillance event, the event is defined, the triggers of the event are identified and the information needed by Law Enforcement for the event is presented.

Note: This section focuses on the communication-identifying information to which Law Enforcement needs access for surveillance events. This section does not presume an implementation for providing Law Enforcement with access to this information.

The following assumptions were made in the development of the material contained herein:

The "calls" referred to in this section include both on-net and off-net calls. (Note: these terms need to be defined in the document.)

There could be differing amounts of available information for particular surveillance events depending on whether a call is an on-net or off-net call, and whether a call is an originating, terminating or redirected call.

Event information for a particular surveillance event can be correlated to event information for previous associated surveillance events. As such, the set of event information identified in this section for a particular surveillance event does not include information elements that are presumed to be available for previous associated surveillance events.

1. Registration Events. This section provides a description of events pertaining to the registration and authorization of terminals.

    a. Terminal Registration: The Terminal Registration event occurs when an intercept subject attempts to gain access to a softswitch-controlled network or its services. It signifies the attempt of the intercept subject to enable the use of the fixed terminal by registering the terminal.

    b. Terminal De-Registration: The Terminal De-registration event occurs when access to a softswitch-controlled network and services has ceased.

    c. Wireless Authorization: The Wireless Authorization event is the authorization or authorization attempt of a mobile terminal to receive service from a different

Wireless Service Provider or in a different serving area. This event applies when the intercept subject has terminal mobility in association with the softswitch-controlled network service to which the intercept subject subscribes.

2. Call Setup Events. This section provides a description of events associated with the set up of a call.

    a. Call Origination: The Call Origination event occurs when the intercept subject originates or attempts to originate a call.

    b. Call Termination Attempt: The Call Termination Attempt event occurs when a terminating call attempt to the intercept subject has been detected.

    c. Call Answer: The Call Answer event occurs when a call or call leg has been answered and transmission is cut-through in both directions to the intercept subject or its agent (e.g., voicemail system), due to the receipt of an off-hook indication from the terminating end-user, or other user-network interaction.

    d. Call Release: The Call Release event occurs when a call, call appearance, or call leg is released. It indicates that network resources associated with the call have been released.

    e. Post-Cut-Through Dialing: [*Note: Punch List Item*] The Post-Cut-Through Dialing event occurs when the intercept subject dials digits after: (1.) a Call Origination event has occurred, (2.) the call has been routed to the same or another carrier's service for processing and routing, and (3.) an Answer event has occurred. The post-cut-through digits are digits dialed or signaled by the intercept subject after the initial call setup is completed and the call path is cut-through in both directions.

3. Call Management Events. This section provides a description of events related to the softswitch-controlled network's management of calls involving an intercept subject. The surveillance events defined in this section focus on capabilities employed by the softswitch-controlled network to perform call management.

    a. Address Resolution: The Address Resolution event occurs when the softswitch-controlled network performs an address translation and returns the translated address information to the intercept subject's equipment (e.g., user terminal) or

service for the purpose of allowing the intercept subject to **directly set up** a call with another user. The Address Resolution event also occurs when the softswitch-controlled network performs an address translation that results in a translated address that identifies the intercept subject's equipment, facilities or service, and returns the translated address information to an associate's equipment (e.g., user terminal) or service (or any other network entity) for the purpose of allowing an associate to **directly set up** a call to the intercept subject.

b. Call Admission Control: The Call Admission event occurs when the softswitch-controlled network interacts with an intercept subject's equipment, facilities or service regarding granting permission/admission for the intercept subject to originate and receive calls. This event also occurs when the softswitch-controlled network instructs an intercept subject's equipment, facilities or service to clear a call, or is notified of the clearing of a call.

c. Media Modification: The Media Modification event occurs when the softswitch-controlled network detects that the media characteristics of a call (e.g., QoS, data rates or bearer type) involving the intercept subject are being modified.

4. Feature Use Events. This section provides a description of events related to an intercept subject's use of service features. The surveillance events defined in this section focus on *what happens during the use* of particular service features, not on the features themselves.

   a. Call Redirection: The Call Redirection event occurs when a call is redirected through the use of an intercept subject's equipment, facilities and/or service. Call redirection occurs for service features such as call forwarding (e.g., call forwarding variable, call forwarding busy) and call waiting deluxe.

   b. Party Hold: [*Note: Punch List Item*] The Party Hold event occurs when the intercept subject places a party on an active call on hold. Placing a party on hold occurs during the use of service features such as call hold, call waiting, and multi-way conference calling (e.g., three-way calling).

   c. Party Retrieve: [*Note: Punch List Item*] The Party Retrieve event occurs when a party who had been placed on hold is retrieved using the same facilities that were used to place the party on hold. The retrieval of a party could occur during

the use of service features such as call hold, call waiting, three-way calling and conference calling.

d. Party Join: [*Note: Punch List Item*] The Party Join event occurs when a party joins an active call. A party can join a call during the use of service features such as multi-way conference calling.

e. Party Drop: [*Note: Punch List Item*] The Party Drop event occurs when a party drops off of a call, such that the call continues (without the dropped party). A party can drop off of a call during the use of service features such as multi-way conference calling.

f. Call Merge: The Call Merge event occurs when two or more active calls are merged. The merging of calls could occur during the use of service features such as multi-way conference calling and call transfer.

g. Call Split: The Call Split event occurs when one of the calls (or call legs) of a multi-way call (a call involving more than two parties) is separated by the conference controller. The "separated call" will continue to exist outside of the multi-way call. This separation of a call is the opposite of the Call Merge event.

5. Feature Management Events. This section provides a description of certain feature management events.

   a. Feature Activation/Deactivation: [*Note: Punch List Item*] The Feature Activation/Deactivation event occurs when a service feature (e.g., call forwarding variable) is activated or deactivated either on behalf of (e.g., network) or by an intercept subject. Feature activation/deactivation could occur through call-associated mechanisms (e.g., dialing a vertical feature code [i.e., *XY], pressing a feature key) or call-independent mechanisms (e.g., filling in a Web page form). However, this event only refers to feature activation/deactivations that occur through call-independent (i.e., non-call associated) mechanisms.

      The Feature Activation/Deactivation event only addresses feature activations/deactivations that result in updates to the softswitch-controlled network. Any feature activations/deactivations that only result in updates to the

softswitch-controlled network's operations support systems (e.g., Billing System) are not addressed.

6. Signaling Events. This section provides a description of signals sent from or to the intercept subject.

    a. Subject Signal: [*Note: Punch List Item*] The Subject Signal event occurs when the intercept subject initiates a signal to control a feature or service operation (e.g., call forwarding, call waiting, call hold and three-way calling).

    b. Network Signal: [*Note: Punch List Item*] The Network Signal event occurs when signals originated by the softswitch-controlled network are sent towards the intercept subject. These signals could be in the form of audio, text or visual signals.

7. Communication Content Events. This section provides a description of events related to access to communication content.

    The surveillance events described in this section are only relevant when Law Enforcement has access to the communication content for the particular LAES.

    a. Content Start: The Content Start event occurs when communication content becomes available to Law Enforcement.

    b. Content Change: The Content Change event occurs when there is a change to the controlled characteristics of the network connection over which communications content flows for a call.

    c. Content Stop: The Content Stop event occurs when communication content ceases to be available to Law Enforcement.

8. Surveillance Status Events. [*Note: Punch List Item*] This section will provide a description of events related to the activation and deactivation of surveillance, and the status of a surveillance (when it is changed and/or on a periodic basis).

[Editors' note: The following bullet list is a reminder of items to cover. Contributions are solicited on these subjects:

- *access to call-identifying information (pen register, trap and trace)*

- *access to call content (interception)*
- *non-detect-ability by intercept subject (transparency)*
- *multiple LEAs (up to five) may be intercepting the same subject - and LEAs shouldn't know about each-other*
- *communications in progress at the time of authorized request will not be intercepted - only communications initiated after the request.*
- *correlation between call-identifying information and call content provided]*

8 APPENDIX B

[Editor's note: Contributions requested to fill in this section.]

8.1 Basic Call Services

8.1.1 Originating call from a Surveillance Subject

8.1.2 Call Termination to a Surveillance Subject

8.2 Example Call Services

8.2.1 Call Hold

8.2.2 Call Redirection

8.2.3 Call Waiting

8.2.4 Call Transfer

8.2.5 N-Way Calling

8.2.6 Call Block

8.2.7 Repeat Call

8.2.8 Return Call

8.2.9 911 Emergency (future work for wireless location info)

8.2.10 Mid-Call CODEC Change