Call Delivery
Redirects an incoming call to a mobile subscriber to the system currently providing service to the mobile subscriber.

Call Diversion
Similar to call forwarding, except that the condition may be more complex (e.g., calling party number, calling party entry of a valid password).

Call Forwarding
Any of several features that redirect a call to another directory number (or voice mail) if a certain condition is met.

Call ID
Unique identifier for all messages during a subject's call. The following rules apply to call ID:

- A new call ID is generated when a subject originates a call from an idle state.
- A new call ID is generated when an incoming call is attempted to a subject.
- The oldest call ID is used for subsequent messages when two calls for a subject are merged.

Call-identifying Information
Dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a TC.

Call Transfer
When a party of a call in progress causes the other party to be connected to a third party and the controlling party leaves the call.

Called Party
The destination or termination party on a call.

Calling Party
The originating party on a call.

Called Party ID
Identification of the destination party.

Calling Party ID
Identification of the originating party.

Communications
Communications, as used herein, refers to the communications *content.* It includes "electronic communications," as defined in 18, U.S.C. 2510(12), any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system, etc. As used herein, the term also includes "wire communications," as defined in 18, U.S.C. 2510(1).

Channel
An independent path for communicating between two points.

Circuit
A physical manifestation of all or part of a channel. On an end-to-end circuit, separate facilities may be used for each segment of the circuit.

Circuit Mode
A communication in which entire physical circuits are switched by an accessing telecommunication system.

Complete
A call attempt that is answered.

Connection
A relationship between two or more parties of a call to allow communication between them.

Controlling Party
The party with the feature invoked.

Cut-through (Full)
Completion of a connection in both directions.

Cut-through (Partial)
Completion of a connection in one direction, usually to allow the calling party to monitor call progress tones from the called end.

Disconnect
A request from one of the parties of the call to release a connection.

Electronic Surveillance
The statutory-based legal authorization, process, and associated technical capabilities and activities of law enforcement agencies related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of call-identifying information.

Idle state
A state when there is no active communication path between a subscriber and the network (i.e., on-hook).

Intercept Access Point (IAP)
A point within a TC network where the call content and/or call-identifying information of a subject are accessed.

Intercept Subject
Same as "subject." The *equipment, facilities, or services of a subscriber* whose incoming, outgoing, and redirected communications and/or call-identifying information is to be accessed and delivered to law enforcement pursuant to a court order or lawful authorization.

Intercepted Call or Call Attempt
As used in this document, refers to a call or call attempt to and from a subject.

Law Enforcement Agency (LEA)
A federal, state, or local entity with the legal authority to conduct electronic surveillance.

Origination
An outgoing call attempt.

Packet Mode
A communication in which individual packets or virtual circuits within a physical circuit are switched or routed by the accessing telecommunication system.

Redirecting system
The system where incoming calls bound to a subscriber arrive for redirection instruction. This is called an originating system in IS-41, although the calls may be originated on another system.

Release
To place facilities used for connection in the idle state.

Subject
Same as "intercept subject." The *equipment, facilities, or services of a subscriber* whose incoming, outgoing, and redirected communications and/or call-identifying information is to be accessed and delivered to law enforcement pursuant to a court order or lawful authorization.

Surveillance
The statutory-based legal authorization, process, and associated technical capabilities and activities of law enforcement agencies related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of call-identifying information. As used in this document, "surveillance" refers to a single pen register, trap and trace, or communications interception. Its use in this document does not include administrative subpoenas for obtaining a subscriber's toll records and information about a subscriber's service that an LEA may employ before the start of a pen register, trap and trace, or communications interception.

Telecommunications Carrier (TC)
A person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, and includes 1) a person or entity engaged in providing commercial mobile service, or 2) a person or entity engaged in providing wire or electronic communications switching or transmission service to the extent that the Federal Communications Commission finds such service is a replacement for a substantial portion of local telephone exchange service. This does not include 1) persons or entities insofar as they are engaged in providing information services, and 2) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the U.S. Attorney General (Public Law 103-414, Sec. 102(8)).

Termination
An incoming call attempt.

Transmission
The act of transferring a message, signal, writing, image, sound, data, or other form of intelligence (information) from one location or another by a wire, radio, electromagnetic, photoelectronic or photo-optical system.

Virtual circuit
A packet-mode connection between two end-points. A virtual circuit may be permanent (with only a data transfer phase) or switched (with setup, data transfer, and release phases).

(This page is intentionally left blank)

List of Acronyms

AIN	Advanced Intelligent Network
ANSI	American National Standards Institute
ANSM	Answer Message
ASN.1	Abstract Syntax Notation One
B channel	ISDN Bearer channel
BER	Basic Encoding Rules
BRI	ISDN Basic Rate Interface
CALEA	Communications Assistance for Law Enforcement Act
CAM	Connection Activated Message
CCC	Call Content Channel
CCM	Connection Cleared Message
CDC	Call Data Channel
CDM	Call Diversion Message
CSEM	Call Surveillance End Message
dB	Decibel
D channel	ISDN Delta channel
DN	Directory Number
DS0	Digital Signal Level 0 (zero)
DS1	Digital Signal Level 1
DTMF	Dual-Tone Multi-Frequency
ESI	Electronic Surveillance Interface
FBI	Federal Bureau of Investigation
FSM	Feature Status Message
FTAM	File Transfer, Access and Management
GSM	Global Systems for Mobile Communications
Hz	Hertz
HDLC	High Level Data Link Control
IAP	Intercept Access Point
ICSM	Incoming Call Start Message

IN	Intelligent Network
ISDN	Integrated Services Digital Network
IXC	Inter-exchange Carrier
ITU-T	International Telecommunications Union - Telecom
LAPB	Link Access Procedures as used in ITU-T X.25
LAPB	Link Access Protocol, Balanced
LEA	Law Enforcement Agency
LEC	Local Exchange Carrier
MSC	Mobile Switching Center
NAIM	Non-Analyzed Input Message
NSM	Network Signal Message
OCSM	Outgoing Call Start Message
OSI	Open Systems Interconnection
PCM	Pulse Code Modulation
PDM	Party Disconnect Message
PEM	Packet Envelope Message
PHM	Party Hold Message
PJM	Party Join Message
POTS	Plain Old Telephone Service
PRI	ISDN Primary Rate Interface
PSPDN	Public Switched Packet Data Network
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
ROSE	Remote Operations Service Element
SAPI	Service Access Point Identifier
SIAM	Subject Input Analyzed Message
SIM	Subject Input Message
SIMPLE	Surveillance Interface Message Protocol for Law Enforcement
SMM	Subject Mobility Message
SSIM	Serving System Identification Message

SSM	Surveillance Status Message
SVC	Switched Virtual Call service
SVC	Switched Virtual Circuit
TC	Telecommunications Carrier
TILU	Telecommunications Industry Liaison Unit
UPT	Universal Personal Telecommunications

1 **(This page is intentionally left blank)**

References

ANSI T1.403, *Telecommunications - Network to Customer Installation - DS1 Metallic Interface.*

Bellcore TR-NWT-000507, *LSSGR Transmission Section 7.*

ITU-Recommendation G.711, *Pulse code modulation (PCM) of voice frequencies.*

ITU-Recommendation V.32, *A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits.*

ITU-Recommendation V.32 bis, *A duplex modem operating at data signalling rates of up to 14400 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits.*

ITU-Recommendation V.34, *A modem operating at data signalling rates of up to 28800 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits.*

ITU-Recommendation V.38, *A 48/56/64 kbit/s data circuit terminating equipment standarized for use on digital point-to-point leased circuits.*

ITU-Recommendation X.21, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for synchronous operation on public data networks.*

ITU-Recommendation X.21 bis, *Use on public data networks of data terminal equipment (DTE) which is designed for interfacing to synchronous V-Series modems.*

ITU Recommendation X.25, *Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*

ITU-T Recommendation X.121, *International numbering plan for public data networks.*

ITU Recommendation X.208, *Specification of Abstract Syntax Notation One (ASN.1).*

ITU Recommendation X.209, *Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).*

PROJECT:	Lawfully Authorized Electronic Surveillance (LAES)
TITLE:	SP-3580A Ballot Comments
SOURCE:	Federal Bureau of Investigation (FBI) – Telecommunications Industry Liaison Unit (TILU)
DATE:	October 28, 1997
DISTRIBUTION:	TIA Subcommittee TR45.2, Intersystem Operations
ABSTRACT:	These comments are provided by TILU to TIA on behalf of the United States Government.

The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text in this contribution and any modification in the creation of a TIA standards publication; to copyright in TIA's name any TIA standards publication even though it may contain portions of this contribution; and at TIA's sole discretion to permit others to reproduce in whole or in part the resulting TIA standards publication.

TIA committee participants are granted permission to copy any portion of this contribution for the legitimate TIA purposes. Copying for monetary gain or other non-TIA related purposes is prohibited.

The contributor does not hold any patents that cover the standard for which the contribution has been made.

This contribution has been prepared to assist the TIA. It may be modified, amended, or withdrawn at any time and it is not binding on the contributor. Nothing in this contribution shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent, or copyright. The contributor reserves the right to use all material submitted in this contribution for the contributor's own purposes including replication and distribution to others. Publication and distribution of this contribution does not constitute any commitment by the FBI to design, develop, purchase, reimburse others, or implement the products or services described herein.

SP-3580A BALLOT COMMENTS

The contribution is ordered according to deficiencies in SP-3580A and contains bold-type references to related sections within SP-3580A.

1. Problem: The first sentence of the definition of "call-identifying information" is appropriate inasmuch as it quotes from CALEA's definition of this term. The additional language is without authoritative grounding in CALEA and is inconsistent with other CALEA provisions. The "interpretation" of call-identifying information offered in this standard language has been rejected by law enforcement as unacceptable and unduly restrictive. This interpretation would lead to the loss of the critical signaling information law enforcement now obtains, and historically has obtained, in electronic-surveillance-related efforts. CALEA's legislative history makes abundantly clear that CALEA was intended to preserve law enforcement electronic surveillance capabilities.

   Recommendations:

   a. **Section 3 Definitions and Acronyms:** Page 5, lines 24-31: Delete the second sentence of the definition.

   b. **Section 4.2.1 Assumptions:** Page 13, lines 45-51: Delete the second sentence of the definition.

2. Problem: The phrase "reasonably available if the information is present at the IAP" is unacceptable and unreasonably restrictive. "Reasonably available ... at an IAP" is an unwarranted "rewriting" of CALEA. CALEA specifies that the carrier is responsible for providing to law enforcement call-identifying information that is "reasonably available to the carrier." (CALEA section 103(a)(2)) The interpretation of "reasonably available ... at the IAP" in the proposed standard's language is without authoritative grounding in CALEA. This interpretation would undermine the provision of critical dialing and signaling information that law enforcement now obtains, historically has obtained, and that CALEA was intended to ensure that law enforcement would obtain in the future in electronic-surveillance-related efforts. CALEA's legislative history makes abundantly clear that CALEA was intended to preserve law enforcement electronic surveillance capabilities.

   Recommendation: **Section 4.2.1 Assumptions:** Page 13, lines 54-59: Change "reasonably available at an IAP" to "reasonably available to the carrier." Alternatively, add the statement, "IAPs shall be provisioned in the network such that all required call-identifying information reasonably available to the carrier will be reasonably available to at least one IAP."

3. Problem: Page 29, lines 6-8: The first sentence of section 5.3.1.1 is inconsistent with text used for the other functions.

   Recommendation: Change to read: "The Access Function, through its constituent Intercept Access Points (IAPs), *is responsible for providing* access to an intercept subject's communications, call-identifying information, or both."

4. Problem: Page 43, lines 4-6: The first sentence of Section 6.2.3 appears to be a requirement.

   Recommendation: Change to read: "The transferred information and messages *shall be encoded* to be binary compatible with X.208 Abstract Syntax Notation One (ASN.1) and X.209 Basic Encoding Rules (BER)."

5. Problem: Page 50, lines 8-9: In Section 6.4.2, it states: "A CallIdentity may be released for other uses with a *CCClose*, Release, or Change message." The CCClose message no longer contains a CallIdentity parameter.

   Recommendation: Remove *CCClose* from the sentence.

6. Problem: Page 50, lines 9-10: In Section 6.4.2, it states: "CallIdentity shall be *immediately* re-used." *Immediately* can not be objectively tested.

   Recommendation: The requirement should specify when a number can be reused. Replace the above text at page 50, lines 9-10, with: "The values used in the sequenceNumber sub-parameter (defined below) shall cycle through all other numbers in the numbering space before a particular sequence number value is reused."

7. Problem: Page 50, lines 10-12: In Section 6.4.2, it states: "Special consideration may be needed for the *CCOpen* usages, so that the CallIdentity is not prematurely released with the Release message." The relationship between the CCOpen and Release messages is unclear. It appears that CCClose rather than CCOpen was deleted during editing.

   Recommendation: Replace CCOpen with CCClose.

8. Problem: Page 52, lines 10-14: Law enforcement needs to know the nature of the numbers used to setup a call and whether the subject's or the associate's name and telephone number is signaled to the other parties to the call due to presentation or restriction indicators.

   Recommendation: Add on page 51 at line 26: "The nature of the telephone number and any presentation or restriction indicators associated with a telephone number shall be reported in the context [18] parameter below."

9. Problem: SP-3580A does not specify any mechanism to associate call-identifying information with call content. For evidentiary purposes, law enforcement must be able to correlate a set of call-identifying information messages from the CDC to a segment of call content received on a CCC. Although any set of messages from one call may share a common call identity, call identities will be reused frequently. In addition, several calls may be received sequentially over the same CCC within a short time period. Because network and collection equipment clocks are not synchronized and may differ by minutes or hours, an additional measure is needed for correlation. Law enforcement recommends one of the following mechanisms to enable call-identifying information to be associated with call content:

1) Add a unique serial number parameter to the CCOpen message and transmit that serial number along with the CCOpen time stamp using tones in-band on the CCC immediately before call content delivery.

2) Synchronize the CCOpen message time stamp to an event on the CCC and deliver the CCOpen message within 500 milliseconds.

Recommendations:

ALTERNATIVE 1:

a. **Section 4.2.3 Call Content Channels and Call Data Channels:** Page 15-16: Add the following requirement:

The following mechanism shall be used to associate call-identifying information to the communications (call content) to which it pertains. The values of the CCOpen message TimeStamp parameter and CCCSerialNumber parameter shall be transmitted using DTMF tones in-band on the CCC immediately before call content delivery. Call content delivery may be delayed up to 2 seconds to prevent the serial number from causing loss of the beginning of the call content.

b. **Section 5.4.3 CCOpen:** Page 34: To provide an association between the CCOpen message and the reference event on the CCC, add the following text:

The transmission of the CCOpen message TimeStamp concatenated by the CCCSerialNumber in-band on the CCC immediately prior to transmission of call content enables that content to be directly associated with that CCOpen message.

Add the following parameter after the time stamp to the message description:

CCC Serial Number	M	Uniquely correlates CDC messages to a particular call content transmitted on the CCC.

c. **Section 6.3.3 CCOpen Message:** Page 45: Add a serial number parameter to the encoding:

```
CCOpen ::= SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP  when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CCCSerialNumber,                    -- for correlation of CDC to CCC
        CHOICE {
                [4]     SEQUENCE OF CallIdentity, -- for circuit-mode intercepts
                [5]     PDUType,                  -- for packet-mode intercepts
        },
        [6]     EXPLICIT CCCIdentity
}
```

d. **Section 6.4 CDC Parameter Definitions:** Add the following parameter definition:

6.4.X CCCSerialNumber

The CCCSerialNumber parameter is used in conjunction with the TimeStamp parameter to correlate CDC messages to a particular call transmitted on the CCC. This parameter value shall be a number that is assigned sequentially on a per CCC basis and shall not repeat within a 24 hour period.

```
CCCSerialNumber ::= VisibleString (SIZE (1..4) )
```

BOTH ALTERNATIVES:

a. **Section 6.5.1 CCC Encoding for Circuit-Mode Services:** Page 54, lines 14-15: To provide an event on the CCC with which the CCOpen message time stamp can be associated, change current text to state:

> Signaling on the CCC or out-of-band signaling *shall* be used to inform the LEA when call content is being delivered.

b. **Section B.3.5 Associate Intercept Subject and Call Identity to the CCC:** Page 75, lines 6-9: Modify the paragraph to read as follows:

> The CCOpen message *shall be used to initially* associate a particular call with *a CCC on* the dedicated circuit. If that call is later merged into another call and supported by another CCC, the TSP shall use the Change message to maintain the association between the communication and the channel(s) on which it is delivered.

ALTERNATIVE 2:

a. **Section 4.2.3 Call Content Channels and Call Data Channels:** Page 15-16: Add the following requirement:

> The following mechanism shall be used to associate call-identifying information to the communications (call content) to which it pertains.
>
> The CCOpen message time stamp shall be synchronized to an event on the CCC. The CCC event shall be either the removal of DTMF C-tone from the CCC or a signaling message (e.g., IAM) used on the same physical circuit as the CCC to activate the CCC. (The CCOpen can be that signaling message only if the CDC and CCC share the same physical circuit.) The appropriate signaling message and C-tone shall be considered synonymous in the following requirements.
>
> When a CCC is opened, C-tone shall be turned off (signaling message sent) for that CCC and a CCOpen message shall be transmitted on the CDC. The time stamp used in the CCOpen message shall be within 100 ms of the actual time when the event (C-tone off) occurred. The first bit of the CCOpen message shall begin transmission on the government procured link from the Delivery Function toward the Collection Function within 500 milliseconds of the CCC event.
>
> When a CCC is closed, C-tone shall be turned on (signaling message sent) for that CCC and a CCClose message shall be transmitted on the CDC. The time stamp used in the CCClose message shall be within 100 ms of the actual time when the event (C-tone on or signaling message) occurred. The first bit of the CCClose message shall be transmitted from the Delivery Function to the Collection Function within 500 milliseconds of the CCC event.

b. **Section 5.4.2 CCClose:** Page 33: To provide an association between the CCClose message and a reference event on the CCC, add the following:

> The time stamp of the CCClose message shall coincide with the release of the CCC. This shall be indicated by the re-application of DTMF C-tone (or the occurrence of an equivalent event) on the CCC.

c. **Section 5.4.3 CCOpen:** Page 34: To provide an association between the CCOpen message and a reference event on the CCC, add the following:

> The time stamp of the CCOpen message shall coincide with the start of delivery on the CCC. This shall be indicated by the removal of DTMF C-tone (or the occurrence of an equivalent event) on the CCC.

10. Problem: SP-3580A does not require call-identifying information to be expeditiously accessed and delivered to law enforcement contemporaneously with or in a manner that allows it to be associated with the communications to which it pertains. Law enforcement has the responsibility to minimize (stop listening and recording) call content unrelated to criminal activity. To support minimization through the timely identification of parties to a call, call event messages should be delivered immediately.

Recommendation: **Section 6.2 CDC Protocol Definition:** Add the following paragraphs:

> Each CDC message contains a time stamp required to associate and synchronize the message to the call content delivered separately over a CCC. The time stamps are generated using the clock of the network element containing the IAP. The time stamp on each of the call event messages shall be accurate within 100 milliseconds of the triggering events described in Stage 2 for each message.
>
> The activation of a CCC must contain an event that marks a change from an idle state to an active state (e.g., removal of C-tone and transmission of the time stamp and serial number) that is detectable at the collection function. The CCOpen message time stamp shall mark (within 100 ms) that state change and shall be the timing reference for synchronization of CDC message times to the CCC call content flow.
>
> Call event messages shall be delivered from the IAP to the demarcation point at the carrier facility within 500 milliseconds, with a probability of 99%. The demarcation point is that point separating the service provider facilities and government-procured delivery facilities. The following messages shall be delivered within 5 seconds (99% probability):
>
> - Serving System Message
> - Feature Status Message
> - Surveillance Status Message.

11. Problem: Law enforcement is not provided all call content from a subject's services, i.e., access to all call content of a subject's service-controlled conference.

Recommendation: **Section 4.5.1 Circuit IAP:** For subject-initiated multiparty calls, insert the following new paragraph on page 20, line 44:

> Multiple CCCs may be necessary for intercept subjects with services that support communications with two or more associates. The first CCC (pair) shall follow the subject's terminal. The second CCC (pair) is required to monitor the subject's conference service when the subject's terminal is separated from the subject's conference. The second CCC is required whenever the subject's service continues to support the communications of the associates.

12. Problem: Law enforcement may be unable to distinguish parties on a multiparty call.

Recommendation: **Section 4.5.1 Circuit IAP:** For separate delivery channels for subject-initiated multiparty calls, add a new paragraph on page 20, line 50:

> Specific lawful authorizations may additionally require a separate CCC for each associate's talk path to the subject's multiparty service when two or more associates are part of a subject-initiated multiparty call. These CCCs shall be in addition to the CCCs monitoring the following:
>
> - Subject's listen path (combined voices) from the multiparty service
> - Subject's listen path from an associate separate from the multiparty service
> - Subject's talk path to the multiparty service or to a separate associate

13. Problem: Law enforcement is not provided all call-identifying information for a call. Changes of parties to each of multiple simultaneous communications are not reported. Law enforcement recommends one of two possible alternative solutions:

1) Modify the Change message by adding a Party Identities parameter and requiring "holds" and "joins" to be treated as splitting and merging of calls. Each termination attempt to a subject already in a call also must be treated as a separate call until merged into the first call.

2) Add the Party Drop, Party Hold, and Party Join messages as described below.

Recommendations:

ALTERNATIVE 1:

a. **Section 4.4 Call Associated Information Surveillance Service Description—Call Identifying Information IAP:** Add the following text to the Change call event:

Party identities or CCC identities change with respect to call identities.

b. **Section 5.4.4:** Modify the text to read as follows:

5.4.4 Change

The Change message reports a change in circuit-mode call identity(ies), especially when merging or splitting calls. *Placing a party on hold shall be represented by splitting a call into two or more call identities. Retrieving a party from hold shall be represented by merging call identities. The Change message shall also report the addition of a call party through barge-in or the release of a call party when the call identity remains active.*

The Change message shall be triggered when:

- two or more call identities are merged into one call identity,
- an additional call identity is associated with an existing call,
- a call identity is split into two or more call identities,
- a call identity is changed to another call identity, or
- *a party identity is added to or released from an active call.*

The Change message includes the following parameters:

Table 4: Change Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
PreviousCalls	M	Identifies the call identities previously used in messages for existing calls. Any call identity that was previously used, but is not mentioned as a resulting call identity, is released and may be reassigned to other calls.
ResultingCalls	M	Identifies the CallIdentity(ies) and CCCIdentity(ies) in each of the resulting calls. New unique call identities may be generated for the Change message, which is used to correlate subsequent messages with the delivered call content. *Any party identity that was previously associated with a call identity, but is not mentioned in the resulting call identity, is released.*

c. **Section 6.3 CDC Message Definitions:** Modify the following message definition:

6.3.4 Change Message

The Change message is used to report merging or splitting of connection-oriented call identities *or when party identities or CCC identities change with respect to call identities.*

```
Change :: = SEQUENCE {
            [0]     CaseIdentity,
            [1]     IAPSystemIdentity           OPTIONAL,
            -- Include to identify the system containing the IAP when the
            -- underlying data carriage does not imply that system.
            [2]     TimeStamp,
previous    [3]     SEQUENCE OF -- previous call(s)
                    SEQUENCE OF CallIdentity, -- identities of a previous call
resulting   [4]     SEQUENCE OF SEQUENCE { -- resulting call(s)
                    [0] SEQUENCE OF CallIdentity, -- identity(ies) of resulting call
                    [1] SEQUENCE OF PartyIdentity    OPTIONAL,
                    -- identity(ies) of resulting parties, required when call identity to
                    -- party identity relationship is one-to-many, not required when
                    -- call identity to party identity relationship is always one-to-one
                    [2] EXPLICIT CCCIdentity   OPTIONAL
                    -- included when the content of the resulting call is delivered
                    -- to identify the CCC(s).
            }
}
```

ALTERNATIVE 2:

a. **Section 4.4 Call Associated Information Surveillance Service Description—Call Identifying Information IAP:** Add the following messages to the existing list of call events:

PartyDrop

A party to a call is released, and the call continues with two or more other parties. (Note: Release of an entire call is reported by the Release message.)

PartyHold

One or more parties of a call are placed on hold by the intercept subject.

PartyJoin

A call party is added to an active call or a held call is retrieved by the intercept subject. One or more previously held associates are added to the current call or an associate joins an existing call with an intercept subject (e.g., barge-in).

b. **Section 5.4:** Add the following message:

5.4.X PartyDrop Message

The PartyDrop message reports when parties to a call are released and the call continues with two or more other parties.

The PartyDrop message shall be triggered when a party is released from a multi-way call (e.g., three-way calling, conference call, meet-me conference).

The PartyDrop message shall not be triggered when an entire call is released, which is reported by the Release message.

The PartyDrop message includes the following parameters:

Table X: PartyDrop Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
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.
One of Released Party Identities Remaining Party Identities	M	 Identifies parties released from the call. Identifies parties remaining in the call.

c. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X PartyDrop

The PartyDrop message reports when parties to a call are released and the call continues with two or more other parties.

```
PartyDrop :: = SEQUENCE {
                    [0]     CaseIdentity,
                    [1]     IAPSystemIdentity          OPTIONAL,
                    -- Include to identify the system containing the IAP when the
                    -- underlying data carriage does not imply that system.
                    [2]     TimeStamp,
                    [3]     CallIdentity,
                    CHOICE {
    releasedParties     [4]     SEQUENCE OF PartyIdentity,
    remainingParties    [5]     SEQUENCE OF PartyIdentity
}
```

d. **Section 5.4:** Add the following message:

5.4.X PartyHold Message

The PartyHold message reports the placing of one or more parties of a call on hold by the intercept subject.

The PartyHold message shall be triggered when one or more parties are no longer connected to a call through use of one of the following features:

- Call hold
- Call waiting
- Three-way calling
- Conference call or Meet-me conference.

The PartyHold message includes the following parameters:

Table X: PartyHold Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
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.
One of Held Party Identities Remaining Party Identities	M	 Identifies parties placed on hold. Identifies parties remaining in the call.

e. **Section 6.3 CDC Message Definitions:** Add the following message definition:

6.3.X PartyHold

The PartyHold message reports the placing of one or more parties of a call on hold by the intercept subject.

```
PartyHold :: = SEQUENCE {
                    [0]    CaseIdentity,
                    [1]    IAPSystemIdentity          OPTIONAL,
                    [2]    TimeStamp,
                    [3]    CallIdentity,
                    CHOICE {
    heldParties          [4]    SEQUENCE OF PartyIdentity,
    remainingParties     [5]    SEQUENCE OF PartyIdentity
}
```

f. **Section 5.4:** Add the following message:

5.4.X PartyJoin Message

The PartyJoin message reports the addition of a call party to an active call or the retrieval of a held call by the intercept subject.

The PartyJoin message shall be triggered when:

- One or more previously held associates are added to the current call (e.g., call waiting, three-way calling, conference calling)
- An associate joins an existing call with an intercept subject (e.g., barge-in).

The PartyJoin message includes the following parameters:

Table X: PartyJoin Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
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.
Joined Party Identities	M	Identifies parties that joined the call.

g. **Section 6.3 CDC Message Definitions:** Add the following message definitions:

6.3.X PartyJoin

The PartyJoin message reports the addition of call parties to an active call or the retrieval of held parties by the intercept subject.

```
PartyJoin :: = SEQUENCE {
                    [0]    CaseIdentity,
                    [1]    IAPSystemIdentity          OPTIONAL,
                    -- Include to identify the system containing the IAP when the
                    -- underlying data carriage does not imply that system.
                    [2]    TimeStamp,
                    [3]    CallIdentity,
      joinedParties [4]    SEQUENCE OF PartyIdentity
}
```

14. Problem: Law enforcement is not provided all call-identifying information regarding subject signaling toward the network on a call.

Recommendation: **Section 5.4.5 Origination:** Add to the first paragraph:

> For voice-activated dialing, the user input parameter shall indicate "voice" and the called PartyIdentity shall contain the resulting translated number.
>
> The Origination message shall report intercept subject inputs of flash hooks and other key usage signaled to the network.

Add the following to the list of triggers for the Origination message:

- A switchhook flash or its equivalent is detected.
- A key press signaled to the network is detected.

15. Problem: No mechanism is described to enable carriers to provide to law enforcement all post-cut-through digits dialed by the intercept subject. Such post-cut-through dialed digits clearly constitute call-identifying information.

Recommendations:

a. **Section 4.4 Call Associated Information Surveillance Service Description—Call Identifying Information IAP:** Add the following event to the existing list of call events:

<u>InBandDigits (Post-Cut-Through)</u>

> The subject dials following cut-through at the access point.

b. **Section 5.4:** Add the following message to ensure the delivery of post-cut-through dialed digits (Note: This text was previously included in the proposed standard.):