

# SCTE • ISBE<sup>®</sup>

# S T A N D A R D S

---

**Data Standards Subcommittee**

---

**AMERICAN NATIONAL STANDARD**

**ANSI/SCTE 165-13 2019**

**IPCablecom 1.5 Part 13: Electronic Surveillance Standard**

## NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2019  
140 Philips Road  
Exton, PA 19341

Note: DOCSIS® and PacketCable™ are registered trademarks of Cable Television Laboratories, Inc., and are used in this document with permission.

# Contents

|          |                                                                                             |           |
|----------|---------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>INTRODUCTION AND BACKGROUND .....</b>                                                    | <b>6</b>  |
| 1.1      | SCOPE .....                                                                                 | 6         |
| 1.2      | REQUIREMENTS AND CONVENTIONS .....                                                          | 6         |
| 1.3      | ELECTRONIC SURVEILLANCE REQUIREMENTS .....                                                  | 6         |
| 1.4      | ELECTRONIC SURVEILLANCE ASSUMPTIONS .....                                                   | 7         |
| 1.5      | DEFINITIONS AND ACRONYMS .....                                                              | 9         |
| <b>2</b> | <b>REFERENCES .....</b>                                                                     | <b>13</b> |
| 2.1      | NORMATIVE REFERENCES .....                                                                  | 13        |
| 2.2      | INFORMATIVE REFERENCES .....                                                                | 13        |
| <b>3</b> | <b>ELECTRONIC SURVEILLANCE IN THE IPCABLECOM NETWORK .....</b>                              | <b>14</b> |
| 3.1      | SUBSCRIBER EQUIPMENT .....                                                                  | 14        |
| 3.2      | ACCESS FUNCTION (AF) AND INTERCEPT ACCESS POINTS (IAPs) .....                               | 15        |
| 3.3      | DELIVERY FUNCTION (DF) .....                                                                | 15        |
| 3.4      | SERVICE PROVIDER ADMINISTRATION FUNCTION (SPAF) .....                                       | 16        |
| 3.5      | COLLECTION FUNCTION (CF) .....                                                              | 16        |
| 3.6      | LAW ENFORCEMENT ADMINISTRATIVE FUNCTION (LEAF) .....                                        | 16        |
| <b>4</b> | <b>INTERFACE BETWEEN THE DELIVERY FUNCTION (PC/TSP) AND COLLECTION FUNCTION (LEA) .....</b> | <b>17</b> |
| 4.1      | GENERAL INTERFACE REQUIREMENTS .....                                                        | 17        |
| 4.2      | NETWORK LAYER INTERFACE .....                                                               | 17        |
| 4.3      | LINK-LAYER INTERFACE .....                                                                  | 17        |
| 4.4      | PHYSICAL INTERFACE .....                                                                    | 18        |
| 4.5      | SECURITY .....                                                                              | 18        |
| <b>5</b> | <b>CALL CONTENT CONNECTION (CCC) INTERFACE .....</b>                                        | <b>19</b> |
| 5.1      | CALL CONTENT CONNECTION IDENTIFIER .....                                                    | 20        |
| 5.2      | ORIGINAL IP HEADER .....                                                                    | 20        |
| 5.3      | ORIGINAL UDP HEADER .....                                                                   | 20        |
| 5.4      | ORIGINAL RTP HEADER .....                                                                   | 20        |
| 5.5      | ORIGINAL PAYLOAD .....                                                                      | 20        |
| 5.6      | TRANSCODING .....                                                                           | 20        |
| <b>6</b> | <b>CALL DATA CONNECTION (CDC) INTERFACE .....</b>                                           | <b>22</b> |
| 6.1      | CDC MESSAGES .....                                                                          | 22        |
| 6.2      | BASIC CALL SERVICES .....                                                                   | 23        |
| 6.2.1    | <i>Originating Call from a Surveillance Subject .....</i>                                   | <i>23</i> |
| 6.2.2    | <i>Call Termination to a Surveillance Subject .....</i>                                     | <i>24</i> |
| 6.3      | SPECIFIC CALL SERVICES .....                                                                | 24        |
| 6.3.1    | <i>Call Hold .....</i>                                                                      | <i>24</i> |
| 6.3.2    | <i>Call Redirection .....</i>                                                               | <i>24</i> |
| 6.3.3    | <i>Call Waiting .....</i>                                                                   | <i>25</i> |
| 6.3.4    | <i>Call Transfer .....</i>                                                                  | <i>25</i> |
| 6.3.5    | <i>Three-Way Calling .....</i>                                                              | <i>27</i> |
| 6.3.6    | <i>Call Block .....</i>                                                                     | <i>28</i> |
| 6.3.7    | <i>Repeat Call .....</i>                                                                    | <i>28</i> |
| 6.3.8    | <i>Return Call .....</i>                                                                    | <i>28</i> |
| 6.3.9    | <i>911 Emergency and N11 Services .....</i>                                                 | <i>28</i> |

|                                                          |                                                                 |           |
|----------------------------------------------------------|-----------------------------------------------------------------|-----------|
| 6.3.10                                                   | <i>Mid-Call CODEC Change</i> .....                              | 29        |
| 6.3.11                                                   | <i>Post-Cut-Through Dialing</i> .....                           | 29        |
| 6.4                                                      | CDC MESSAGE DESCRIPTIONS .....                                  | 29        |
| 6.4.1                                                    | <i>Answer</i> .....                                             | 29        |
| 6.4.2                                                    | <i>CCChange</i> .....                                           | 30        |
| 6.4.3                                                    | <i>CCClose</i> .....                                            | 30        |
| 6.4.4                                                    | <i>CCOpen</i> .....                                             | 31        |
| 6.4.5                                                    | <i>ConferencePartyChange</i> .....                              | 32        |
| 6.4.6                                                    | <i>DialedDigitExtraction</i> .....                              | 32        |
| 6.4.7                                                    | <i>MediaReport</i> .....                                        | 33        |
| 6.4.8                                                    | <i>NetworkSignal</i> .....                                      | 34        |
| 6.4.9                                                    | <i>Origination</i> .....                                        | 35        |
| 6.4.10                                                   | <i>Redirection</i> .....                                        | 35        |
| 6.4.11                                                   | <i>Release</i> .....                                            | 36        |
| 6.4.12                                                   | <i>ServiceInstance</i> .....                                    | 37        |
| 6.4.13                                                   | <i>SubjectSignal</i> .....                                      | 37        |
| 6.4.14                                                   | <i>TerminationAttempt</i> .....                                 | 38        |
| 6.5                                                      | CDC MESSAGES AND PARAMETER DEFINITIONS .....                    | 38        |
| <b>APPENDIX I IPCABLECOM-SPECIFIC REQUIREMENTS .....</b> |                                                                 | <b>46</b> |
| I.1                                                      | TIMING REQUIREMENTS .....                                       | 46        |
| I.2                                                      | DIALED DIGIT EXTRACTION CDC MESSAGE .....                       | 46        |
| I.3                                                      | NETWORK SIGNAL CDC MESSAGE .....                                | 46        |
| I.4                                                      | SUBJECT SIGNAL CDC MESSAGE .....                                | 49        |
| I.5                                                      | CORRELATING CONTENT PACKETS WITH EVENT MESSAGES .....           | 50        |
| I.6                                                      | INSTRUCTING COMPONENTS TO PERFORM ELECTRONIC SURVEILLANCE ..... | 51        |
| I.6.1                                                    | <i>COPS Interface Requirements</i> .....                        | 51        |
| I.6.2                                                    | <i>TGCP Interface Requirements</i> .....                        | 51        |
| I.7                                                      | TIMING INFORMATION .....                                        | 51        |
| I.8                                                      | FILTERING CDC EVENTS IN REDIRECTED CALLS .....                  | 51        |

## List of Figures

|                                                |    |
|------------------------------------------------|----|
| FIGURE 1 - ELECTRONIC SURVEILLANCE MODEL ..... | 14 |
|------------------------------------------------|----|

## List of Tables

|                                                                   |    |
|-------------------------------------------------------------------|----|
| TABLE 1 - PAYLOAD OF CALL CONTENT CONNECTION DATAGRAMS .....      | 19 |
| TABLE 2 - INTERCEPTED INFORMATION .....                           | 19 |
| TABLE 3 - ANSWER MESSAGE .....                                    | 29 |
| TABLE 4 - CCCHANGE MESSAGE .....                                  | 30 |
| TABLE 5 - CCCLOSE MESSAGE .....                                   | 31 |
| TABLE 6 - CCOOPEN MESSAGE .....                                   | 31 |
| TABLE 7 - CONFERENCEPARTYCHANGE MESSAGE .....                     | 32 |
| TABLE 8 - DIALED DIGIT EXTRACTION MESSAGE .....                   | 33 |
| TABLE 9 - MEDIA REPORT MESSAGE .....                              | 34 |
| TABLE 10 - NETWORK SIGNAL MESSAGE .....                           | 34 |
| TABLE 11 - ORIGINATION MESSAGE .....                              | 35 |
| TABLE 12 - REDIRECTION MESSAGE .....                              | 36 |
| TABLE 13 - RELEASE MESSAGE .....                                  | 36 |
| TABLE 14 - SERVICE INSTANCE MESSAGE .....                         | 37 |
| TABLE 15 - SUBJECT SIGNAL MESSAGE .....                           | 38 |
| TABLE 16 - TERMINATION ATTEMPT MESSAGE .....                      | 38 |
| TABLE 17 - MAPPING OF NCS SIGNALS TO NETWORK SIGNAL MESSAGE ..... | 46 |
| TABLE 18 - MAPPING OF NCS SIGNALS TO SUBJECT SIGNAL MESSAGE ..... | 49 |

# 1 INTRODUCTION AND BACKGROUND

## 1.1 Scope

This specification defines the interface between a telecommunications carrier that provides telecommunications services to the public for hire using IP Cablecom capabilities (a “PC/TSP”) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. Companies using IP Cablecom capabilities will not in the normal case be “telecommunications carriers.” Instead they will be providers of information services. However, some companies using IP Cablecom capabilities may, by virtue of other actions, be “telecommunications carriers” for purposes of the Communications Assistance for Law Enforcement Act (CALEA) with respect to their use of IP Cablecom capabilities. The purpose of this specification is to assist those companies in meeting their obligations under CALEA. In this regard, a telecommunications carrier that complies with a publicly available technical requirement or standard adopted by an industry association or standards-setting organization shall be found to be in compliance with the assistance capability requirements of CALEA.

As noted, cable operators are not ordinarily telecommunications carriers, but if a cable operator has taken the steps to become a carrier, and uses IP Cablecom to provide carrier services, then CALEA might apply to the equipment used to implement IP Cablecom. For this reason, we are providing consideration of CALEA concerns as part of the IP Cablecom specification, for the benefit of anyone who might use this architecture/technology as part of their carrier activities.

Accordingly, a PC/TSP, manufacturer, or support provider that is in compliance with this document will have “safe harbor” under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001 et seq.

This specification defines services and features to support Lawfully Authorized Electronic Surveillance, and the interfaces to deliver intercepted communications and reasonably available call-identifying information to a LEA when authorized.

## 1.2 Requirements and Conventions

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

|              |                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| “MUST”       | This word or the adjective “REQUIRED” means that the item is an absolute requirement of this specification.                                                                                                                                                                       |
| “MUST NOT”   | This phrase means that the item is an absolute prohibition of this specification.                                                                                                                                                                                                 |
| “SHOULD”     | This word or the adjective “RECOMMENDED” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.                              |
| “SHOULD NOT” | This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. |
| “MAY”        | This word or the adjective “OPTIONAL” means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.                      |

## 1.3 Electronic Surveillance Requirements

Congress passed CALEA October 1994. It requires telecommunications carriers and manufacturers to provide certain capabilities to LEAs with the proper court authorization. Although a cable operator may not have any obligations under CALEA, a cable operator that has taken steps to become a telecommunications carrier, and uses IP Cablecom capabilities to provide telecommunications services (as used here, a PC/TSP) that is found in compliance with a publicly available technical requirement or standard adopted by an industry association or

standards-setting organization shall be found to be in compliance with the assistance capability requirements of CALEA. Accordingly, when designing a surveillance protocol, it is prudent to consider and incorporate CALEA requirements.

Although CALEA may not apply to any particular cable operator, in general, it requires certain telecommunications carriers to ensure that their equipment, facilities, or services have the capability to:

1. Expeditiously isolate and enable the LEA to access reasonably available call identifying information.
2. Expeditiously isolate and enable the LEA to intercept all communications carried by a carrier within a service area to or from the equipment, facilities or services of a subscriber, concurrently with the communications' transmission.
3. Make intercepted communications and call identifying information available to the LEA in a format available to the carrier so they may be transmitted over lines or facilities leased or procured by the LEA to a location away from the carrier's premises.
4. Meet these requirements with a minimum of interference with the subscriber's services and in such a way that protects the privacy of communications and call identifying information that are not authorized to be intercepted, and that maintains the confidentiality of the LEA's wiretaps.
5. The Telecommunications Industry Association has promulgated a standard [19] for lawfully authorized electronic surveillance for traditional voice telephony. However, the electronic surveillance features and capabilities for traditional voice telephony provided for in [19] are not readily applicable to telephony provided by means of a cable system, including telephony provided using IPCablecom capabilities.<sup>1</sup> This document was produced for electronic surveillance specific to telephony services provided by cable operators which are acting as telecommunications carriers and performing their carrier functions using IPCablecom capabilities.

## 1.4 Electronic Surveillance Assumptions

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

LEAs may be authorized to conduct any of three specific types of surveillance: (1) "pen register," which records call-identifying information for all calls originated by a subject, (2) "trap and trace," which records call-identifying information for all calls received by a subject, and (3) "interception," which allows LEAs to listen to the conversations of the subject, as well as access to call-identifying information. Approximately 90% of all surveillance orders are of the first two types; Federal law and laws of 42 states only allow the use of the third technique in the investigation of serious criminal offenses, and when other techniques have not worked, will not work, or are too dangerous.

As a precondition for a PC/TSP's assistance with Lawfully Authorized Electronic Surveillance, a LEA must serve a PC/TSP with the necessary legal authorization identifying the intercept subject, the communications and information to be accessed, and service areas where the communications and information can be accessed.<sup>2</sup> Once this authorization is obtained, the PC/TSP shall perform the access and delivery for transmission to the LEA's procured equipment, facilities, or services.

---

<sup>1</sup> Although the specifications and requirements of [19] are not applicable to IPCablecom-based telephony, the focus group preparing this specification sought to employ similar messaging, where possible, so as to minimize the development efforts for manufacturers of Delivery Function devices and law enforcement Collection Function devices. However, it is important to note that the IPCablecom messages defined in this specification are very different from those defined in [19], employing different parameters and being triggered by different events.

<sup>2</sup> To obtain a court order authorizing the interception of a wire or electronic communication, a law enforcement officer must submit a written application to a court of competent jurisdiction. The application must include information such as the identity of the officer making the application, a complete statement of facts supporting the application, a statement of whether other investigative procedures have been tried and failed or of why they appear reasonably unlikely to succeed or are too dangerous to attempt, and a statement of the period of time for which the interception is required (18 U.S.C. 2518(1)).

Communications in progress at the time a PC/TSP receives a legally authorized request will not be subject to surveillance. Only communications initiated after the legally authorized request will be subject to surveillance.

A PC/TSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subject or associate, unless the encryption was provided by the PC/TSP and the PC/TSP possesses the information necessary to decrypt the communication (18 U.S.C. 2602(b)(3)). Nothing in CALEA would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access.

Only packets sent or received by the intercept subject that utilize the capabilities of the Call Management System to establish the communication, and utilize enhanced Quality of Service as authorized by the Call Management System, are considered "calls" as defined by CALEA. Cable operators that have deployed IPCablecom capabilities will offer a range of other services to their customers that make use of packet-switched communications, such as email and Internet access. Other than the packets identified in the first sentence of this paragraph, packets sent or received by the intercept subject are considered Information Services.

One or more Delivery Functions may be utilized to deliver the call content and call-identifying information associated with a particular surveillance order. For example, call content and call-identifying information of a redirected call may not be present at the facilities normally used for surveillance of a subject. It is the responsibility of the PC/TSP to designate a Delivery Function that will deliver call content and call identifying information to a CF for a particular surveillance order. Procurement of the physical facilities connecting this Delivery Function to its Collection Function is the responsibility of the LEA.

In most cases, a PC/TSP should be able to intercept calls redirected by a surveillance subject to other locations either in its own network or in the networks of other telecommunications carriers. However, where a subject has redirected incoming calls to a location served by another PC/TSP, the resulting connection may be established without touching the equipment or facilities of the subject's PC/TSP. Instead, the connections will be made directly from the PC/TSP originating the incoming call to the PC/TSP serving the location to which the subject redirected incoming calls. Because the subject's original PC/TSP will not be aware of these resulting connections, access to these connections will have to be obtained from the PC/TSP serving the location to which calls have been redirected.

When a surveillance subject initiates the placement of an associate on hold for a two-way call, the PC/TSP is not required to deliver call content for the associate to the LEA while the associate is on hold. However, depending on implementation, the PC/TSP might deliver this call content to the LEA.

A subject's call content and call data is transmitted to the LEA over one or more logical channels known as Call Content Connection (CCC) and Call Data Connection (CDC). The actual number of logical channels supported will vary. Factors influencing connection capacity include (1) the number of CCCs and CDCs ordered by the LEA for subjects associated with a given Delivery Function (DF), (2) the number of surveillance orders required to be supported for any single subject, (3) the availability of resources to transport call content and call data information from the DF to the CF, (4) the availability of resources to transport call content and call data information from the IAP to the DF, and (5) the availability of resources to transport redirected call content and call data information between DF's within the PC/TSP network.

Capacity requirements are fundamental to the design and development of any technical standard or specification (as well as for the equipment developed in compliance with such standards). Several technical considerations, pivotal to the design process, are affected by capacity requirements. However, so far, the Attorney General has not identified capacity requirements for telecommunications carriers that use IPCablecom capabilities to provide telecommunications services. In the absence of these formal capacity requirements, certain reasonable assumptions were made in this document about capacity in order to proceed with developing this standard. It is believed that these assumptions reflect reasonable estimates based on industry's technical expertise as well as law enforcement's historical requirements on other technologies. However, to the extent that these reasonable assumptions differ from whatever formal capacity requirements the Attorney General eventually identifies, substantial modifications to this standard may be required (with resulting delays and lost effort in the design and development of equipment consistent with this standard).

As such, the following assumptions are made: (1) the IAP supports a maximum number of intercepts of 5% of its active calls, (2) the DF supports a maximum of five surveillance orders for any single subject, (3) the DF to CF interface must be capable of supporting the maximum number of intercepts times the maximum number of intercepts per subject, (4) it is the responsibility of the PC/TSP to provide adequate resources to transport call

content and call data information from the IAP to the DF based on statistical call models, (5) it is the responsibility of the PC/TSP to provide adequate resources to transport redirected call content and call data information between DFs within the PC/TSP network based on statistical call redirection models, (6) when adequate resources are not available, situations may arise where call content and call identifying information are not delivered to the LEA.

## 1.5 Definitions and Acronyms

**AF:** Access Function

**ANSI:** American National Standards Institute.

**Associate:** a telecommunication user whose equipment, facilities, or services are communicating with a subject.

**CALEA:** Communications Assistance for Law Enforcement Act.

**Call:** a telecommunication originated by or terminated to a customer that enters or leaves the IP/Cablecom network at a PC/TSP-operated PSTN gateway, or a telecommunication that originates or terminates at a PC/TSP customer's MTA that 1) makes a request to the proper Call Management System for that endpoint, which then authorizes enhanced QoS facilities, 2) is granted the request for enhanced QoS facilities, and 3) uses those enhanced QoS facilities for transfer of packetized information. For purposes of pen register and trap and trace intercepts, a call is a communication that makes a request to the proper Call Management System for that endpoint.

**Call Content:** see Content.

**Call Content Connection:** the logical link between the device performing an electronic surveillance delivery function and the LEA, that primarily carries the call content passed between an intercept subject and one or more associates. At the demarcation point, Call Content Connections are identified by the combination of Protocol type of UDP (in the IP header), CF address (in the IP header), CF port number (in the IP header), and the CCC-Identifier (in the CCC payload).

**Call Data Connection:** the logical link between the device performing an electronic surveillance delivery function and the LEA that primarily carries call-identifying information. At the demarcation point, Call Data Connections are identified by the combination of Protocol type of TCP (in the IP header), CF address (in the IP header), CF port number (in the TCP header), and the Call-ID (in the PCESP message).

**Call-identifying information:** defined in CALEA Section 102(2), 103(a)(2), and 18 U.S.C. § 2601(a) to be “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 telecommunications carrier” but “does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).” See destination, direction, origin and termination.

**Call under interception:** A call that is 1) originated by a PC/TSP subscriber that is under an interception order, 2) terminated to a PC/TSP subscriber that is under an interception order, or 3) redirected by the service of a PC/TSP subscriber that is under an interception order to another service provided by the same PC/TSP. Once a call is identified by the PC/TSP as a call under interception, it maintains that status through all redirections utilizing that PC/TSP's network even if the resulting communicating parties are not themselves surveillance subjects.

**Call under surveillance:** A call that is 1) originated by a PC/TSP subscriber that is under a surveillance order, 2) terminated to a PC/TSP subscriber that is under a surveillance order, or 3) redirected by the service of a PC/TSP subscriber that is under a surveillance order to another service provided by the same PC/TSP. Once a call is identified by the PC/TSP as a call under surveillance, it maintains that status through all redirections utilizing that PC/TSP's network even if the resulting communicating parties are not themselves surveillance subjects.

**CCC:** Call Content Connection

**CDC:** Call Data Connection

**CF:** Collection Function

**CMS:** Call Management System, an IP-Cablecom element that performs telecommunications-specific functions in the establishment of a call, such as address translation, call routing, directory services, usage recording, and authorization of QoS.

**Commission:** defined in CALEA Section 102(3) to be “the Federal Communication Commission.”

**Communication:** any wire or electronic communication, as defined in 18 U.S.C. § 2510.

**Communication Intercept:** see intercept.

**Content:** defined in 18 U.S.C. § 2510(8) to include “when used with respect to any wire or electronic communications, ... any information concerning the substance, purport, or meaning of that communication.”

**Controlling Party:** the party invoking a feature.

**Demarcation Point:** a physical point between the PC/TSP’s Delivery Function and the LEA’s Collection Function where responsibility of the PC/TSP ends and the LEA assumes responsibility.

**Destination:** defined in [13] to be “a party or place to which a call is being made (e.g., the called party).”

**DF:** Delivery Function.

**Dialed digit extraction:** the capability that permits a LEA to receive digits dialed by a surveillance subject after a call is connected.

**Direction:** defined in [13] to be “a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., a redirected-to party or redirected-from party).”

**DOCSIS®:** Data-Over-Cable Service Interface Specification. A set of standards that define methods and procedures for use of cable networks to provide information services.

**Electronic Communication:** defined in 18 U.S.C. § 2510(12) to be “any transfer of signs, 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.”

**Electronic Storage:** defined in 18 U.S.C. § 2510(17) to be “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

**Electronic Surveillance:** the statutorily-based legal authorization, process, and associated technical capabilities and activities of LEAs 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 specification, surveillance refers to a single communication intercept, pen register, or trap and trace. Its usage in this specification does not include administrative subpoenas for obtaining a subscriber’s toll records and information about a subscriber’s service that a LEA may employ before the start of a communication intercept, pen register, or trap and trace.

**Government:** defined in CALEA Section 102(5) to be “the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.”

**IAP:** Intercept Access Point.

**Information Service:** defined in CALEA Section 102(6) to be “(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and (B) includes – (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a telecommunications carrier’s internal management, control, or operation of its telecommunications network.” See also Telecommunication Carrier and TSP.

**Intercept:** defined in 18 U.S.C. § 2510 (4) to be “the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”

**Intercept Access Point:** a point within a communication system where some of the communications or call-identifying information of an intercept subject’s equipment, facilities and services are accessed. In the IP-Cablecom

network, the Intercept Access Point of a surveillance subject is the CMTS serving the subject, and the CMS designated by the PC/TSP which processes calls for the subject.

**Intercept Subject:** see Subject.

**IP:** Internet Protocol.

**Law Enforcement Agency:** a government entity with the legal authority to conduct electronic surveillance.

**LEA:** Law Enforcement Agency.

**LEAF:** Law Enforcement Administration Function.

**MTA:** Multi-media terminal adapter.

**Origin:** defined in [13] to be “a party initiating a call (e.g., a calling party), or a place from which a call is initiated.”

**Party hold, join, drop on conference calls:** The capability that permits a LEA to identify the parties to a subject-initiated conference call conversation at all times.

**PC/TSP:** IPCom Telecommunications Service Provider. As used in this specification, a PC/TSP is an entity, typically a cable operator, that has (a) taken the steps necessary to be a “telecommunications carrier” for purposes of CALEA, and (b) provides its telecommunications services using IPCom capabilities. The fact that an entity may use IPCom, including the use of IPCom for voice telephony applications, does not mean that the entity is a “telecommunications carrier” for purposes of CALEA or any other regulatory purpose.

**PCESP:** IPCom Electronic Surveillance Protocol.

**Pen Register:** defined in 18 U.S.C. § 3127(3) to be “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.”

**POTS:** Plain Old Telephone Service. This usually refers to loop start lines with DTMF (tone) dialing or decadic (rotary) dialing.

**PSTN:** Public Switched Telephone Network.

**QoS:** Quality of Service.

**Reasonably Available:** is defined in the Commission’s Third Report and Order [14]. Call identifying information is *reasonably available* if the information “is present at an Intercept Access Point (IAP) and can be made available without the carrier being unduly burdened with network modifications.” Network protocols do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves.

**Redirected call:** a call that is transferred (see Transferred call), or redirected as a service provided to a terminating subscriber, such as unconditionally, or when the terminating subscriber’s line is busy, or when the terminating subscriber doesn’t answer.

**SPAF:** Service Provider Administration Function.

**Subject:** a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to a LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity). The “equipment and facilities of the subscriber” in the IPCom network consist of the CMTS serving the subscriber and the CMS designated by the PC/TSP which processes calls for the subscriber.

**Surveillance:** within this specification surveillance refers to electronic surveillance; see Electronic Surveillance.

**Surveillance Subject:** See Subject.

**TCP:** Transmission Control Protocol.

**Telecommunications Carrier:** defined by CALEA Section 102(8) as “a person or entity engaged in the transmission or switching of wire or electronic communication 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 Commission finds such service is a replacement for a substantial portion of local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title. 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.” Some entities that use IP-Cablecom to provide telecommunications to customers may be “telecommunications carriers” for purposes of CALEA. See PC/TSP.

**Telecommunications Support Services:** defined in CALEA Section 102(7) to be “a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunication network.”

**Termination:** defined in [13] to be “a party or place at the end of a communication path (e.g., the called or call-receiving party, or the switch of a party that has placed another party on hold).”

**Transferred call:** A call that changes either the originating party or terminating party, based on action taken by one of the parties in the call.

**Transmission:** the act of transferring communications from one location or another by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

**Trap and Trace Device:** defined in 18 U.S.C. § 3127(4) to be “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.”

**TSP:** Telecommunication Service Provider. Some TSPs may also be “telecommunications carriers” for purposes of CALEA. See Telecommunications Carrier and PC/TSP.

**Unobtrusive:** not undesirably noticeable or blatant; inconspicuous; within normal call variances.

**U.S.C.:** United States Code.

**Wire Communications:** defined in 18 U.S.C. § 2510 (1) to be “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point or reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.”

## 2 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision, and while parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

### 2.1 Normative References

In order to claim compliance with this standard, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this standard. Intellectual property rights may be required to implement these references.

- [1] IETF RFC 768/ST0006, User Datagram Protocol, August, 1980.
- [2] IETF RFC 791/STD0005, Internet Protocol, September, 1981.
- [3] IETF RFC 793/STD0007, Transmission Control Protocol, September, 1981.
- [4] IETF RFC 826/STD0037, November, 1982.
- [5] IETF RFC 894/STD0041, Standard for the Transmission of IP Datagrams over Ethernet Networks, 1984.
- [6] IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January, 1996.
- [7] IETF RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, January, 1996.
- [8] IETF RFC 2327, SDP: Session Description Protocol, April, 1998.
- [9] ISO/IEC 8802-3:2000, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
- [10] ITU-T Recommendation X.690 (07/02): Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
- [11] IETF RFC 1305, Network Time Protocol (Version 3), Specification, Implementation and Analysis, March 1992.

### 2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

- [12] ANSI/SCTE 23-01 2017, DOCSIS 1.1 Part 1: Radio Frequency Interface.
- [13] FCC 02-108, CC Docket No. 97-213, Order on Remand, April 11, 2002.
- [14] FCC 99-230, CC Docket No. 97-213, Third Report and Order, August 31, 1999.
- [15] SCTE 165-02 2016, IPCablecom 1.5 Part 2: Audio/Video Codecs.
- [16] SCTE 165-09 2019, IPCablecom 1.5 Part 9: Event Messages.
- [17] SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [18] SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [19] ANSI/J-STD-025-A-2003, Lawfully Authorized Electronic Surveillance, April 17, 2003.

### 3 ELECTRONIC SURVEILLANCE IN THE IPCABLECOM NETWORK

The intercept function is viewed as five broad categories: access, delivery, collection, service provider administration, and law enforcement administration. These functions are discussed functionally in this section without regard to their implementation. The relationships between these functional categories are shown in Figure 1.

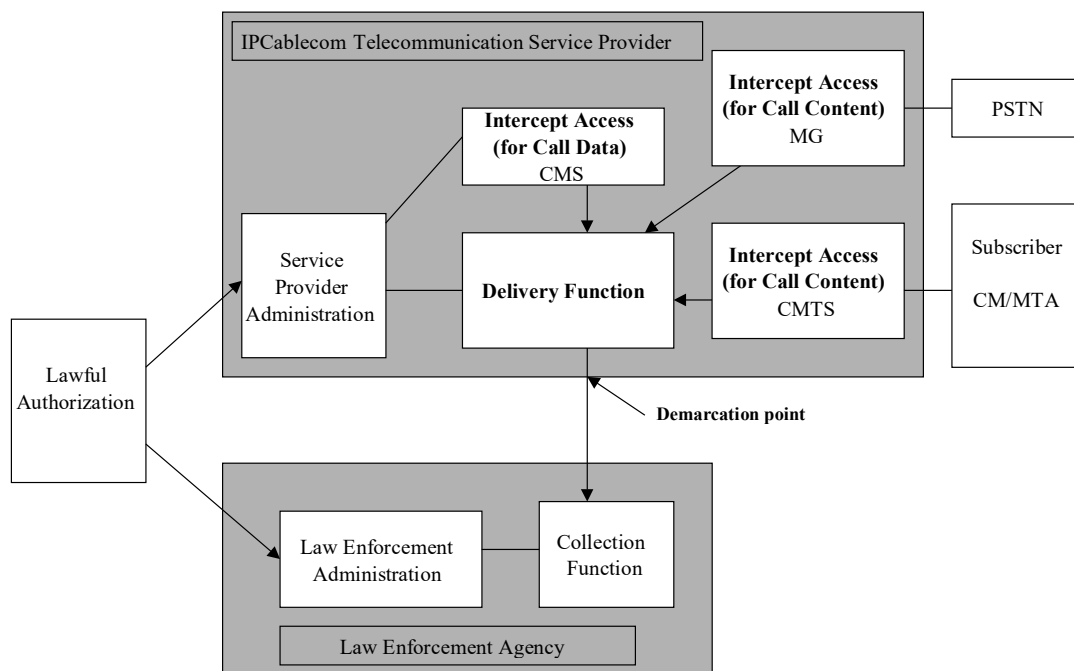


**Figure 1 - Electronic Surveillance Model**

The lawful authorization, while neither a network entity nor an interface reference point, is an important part of electronic surveillance. Surveillance MUST NOT take place without specific lawful authorization.

#### 3.1 Subscriber Equipment

The core of providing all IPCablecom services, including any telecommunications services that a provider might offer, is the broadband access network. This network is characterized as a DOCSIS® [12] access network, but may be provided over access networks supporting other standards. The access network consists of the cable modem, the cable modem termination system, and the Media Access Control and Physical access layers.

The subscriber equipment includes those elements of the access network that are located in the customer's home. This includes the Cable Modem (CM) and the Multi-media Terminal Adapter (MTA).

The CM is an IPCablecom network element as defined by the DOCSIS specification. The CM plays a key role in handling the media stream. Services which may be provided by the CM include classification of traffic into service flows according to classification filters, rate shaping, and prioritized queuing.

An MTA is a single hardware device that incorporates audio and optionally video IP telephony. An MTA may optionally incorporate a DOCSIS cable modem (an Embedded MTA) or may connect through external means to a DOCSIS cable modem (a Standalone MTA).

An MTA supports the following functionality:

- Provides one or more RJ11 interfaces to 2500-series phones
- Performs call signaling with the CMS to originate and terminate calls
- Supports QoS signaling with the CMS and the CMTS
- Supports security signaling with the CMS and other MTA devices
- Supports provisioning signaling with the Provisioning server(s)
- Performs encoding/decoding of audio streams
- Provides multiple audio indicators to phones, such as ringing tones, call waiting tones, stutter dial tone, dial tone, etc.
- Provides standard PSTN analog line signaling for audio tones, voice transport, caller-id signaling, and message waiting indicators

The IPCablecom system design places much of the session control intelligence at the endpoints, where it can easily scale with technology and provide new and innovative services. While this “future-proofing” is a goal of the design, we recognize that it leaves open a wide range of fraud possibilities. The basic assumption is that the MTA is not immune to customer tampering, and that the significant incentive for free service will lead to some very sophisticated attempts to thwart any network controls placed on the MTA.

Under these circumstances, it is important to realize that an MTA under customer control will likely not cooperate with electronic surveillance, and methods are therefore described here that do not depend in any way on cooperation with the MTA.

### 3.2 Access Function (AF) and Intercept Access Points (IAPs)

The Intercept Access Function, performed by the Intercept Access Points (IAPs), isolates an intercept subject’s communication or reasonably available call-identifying information unobtrusively. The Access Function is responsible for the collection of call content and reasonably available call-identifying information and making such information available to the Delivery Function.

In an IPCablecom network, four elements are designated as Intercept Access Points:

- The Cable Modem Termination System (CMTS) which controls the set of cable modems attached to the shared medium of the DOCSIS network. The CMTS is responsible for intercepting the Call Content, and certain call-identifying information.
- The Call Management System (CMS) which provides service to the subscriber. The CMS is responsible for intercepting the Call-Identifying information.
- The Media Gateway (MG) is designated as an Intercept Access Point for purposes of intercepting Call Content for redirected calls to the PSTN.
- The Media Gateway Controller (MGC) is designated as an Intercept Access Point for purposes of intercepting the Call-identifying information for redirected calls to the PSTN.

The equipment and facilities of each subscriber include two Intercept Access Points (CMTS and CMS), and call-identifying information reasonable available at these IAPs is provided to LEA. Redirected calls in the IPCablecom network might not utilize the equipment or facilities of the subscriber who initiated the redirection. Accordingly, the Intercept Access point for a call that has been redirected will be either the CMS/CMTS of the new destination (if redirected to another IPCablecom endpoint within the same provider’s network) or the MGC/Media Gateway of the PSTN interconnection (if redirected to a PSTN endpoint).

### 3.3 Delivery Function (DF)

The Delivery Function includes the interface responsible for delivering intercepted communication expeditiously from the Intercept Access Functions to the demarcation point. The Delivery Function delivers reasonably available

call-identifying information and call content based on the requirements of the lawful authorization. The Delivery Function includes the ability to:

- Collect and deliver call content and reasonably available call-identifying information for each intercept subject over the procured law enforcement facilities
- Ensure that the call content and call-identifying information delivered from the Delivery Function is authorized for a particular LEA
- Protect (i.e., prevent unauthorized access to, or manipulation and disclosure of) intercept controls, intercepted call content, and call-identifying information, through methods that are consistent with the normal security policies of the affected PC/TSP
- Ensure that delivery of surveillance information is only available for the time stated in the lawful authorization
- Deliver call content and reasonably available call-identifying information using the PCESP protocol
- Support environments with multiple CMSs, MGCs, MGs, and CMTSs by accepting call content and call data related to a single intercept from multiple IAPs
- Support multiple DF environments by forwarding call content and call data, in the form of Event Messages (EMs), to other DFs

Enabling and disabling the Delivery Function is the responsibility of the PC/TSP.

The Delivery Function delivers information over two distinct types of connections: Call Content Connections (CCCs) and Call Data Connections (CDCs). The CCCs are generally used to transport call content, such as voice communications. The CDCs are generally used to transport messages which report call-identifying information, such as the calling party identities and called party identities.

Call-identifying information, call content, or both, associated with a particular subject may need to be delivered to more than one LEA Collection Function simultaneously. This will occur when different LEAs are conducting independent investigations on the same subject. The Delivery Function duplicates the call content, call-identifying information, or both, and deliver authorized information to each LEA.

Call-identifying information, call content, or both, from multiple surveillances may need to be delivered simultaneously to a single LEA's CF.

### **3.4 Service Provider Administration Function (SPAF)**

The Service Provider Administration Function is responsible for controlling PC/TSP Access and Delivery Functions. The PC/TSP administrative functions are outside the scope of this specification.

### **3.5 Collection Function (CF)**

The Collection Function is responsible for collecting intercepted communication and call-identifying information from the demarcation point. The Collection Function is the responsibility of the LEA. Enabling and disabling the activation of the LEA-provided interface is the responsibility of the LEA Administrative Function and is beyond the scope of this specification.

### **3.6 Law Enforcement Administrative Function (LEAF)**

The Law Enforcement Administration Function is responsible for controlling the LEA Collection Function. The Law Enforcement Administration Function is the responsibility of the LEA.