CALEA ASSISTANCE CAPABILITY REQUIREMENTS

47 USCS § 1002 (2001)

§ 1002. Assistance capability requirements.

(a) Capability requirements. Except as provided in subsections (b), (c), and (d) of this section and sections 108(a) and 109(b) and (d) [47 USCS §§ 1007(a) and 1008(b)], a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

(1) **expeditiously isolating and enabling the government**, pursuant to a court order or other lawful authorization, **to intercept**, **to the exclusion of any other communications**, all wire and **electronic communications** carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier **concurrently with their transmission** to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) **expeditiously isolating and enabling the government**, pursuant to a court order or other lawful authorization, **to access call-identifying information** that is reasonably available to the carrier—

(A) **before, during, or immediately after the transmission** of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) **in a manner that allows it to be associated with the communication** to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall 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);

(3) **delivering intercepted communications and call-identifying information to the government**, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information **unobtrusively and with a minimum of interference** with any subscriber's telecommunications service and in a manner that protects—

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

FROM THE FCC'S NOTICE OF PROPOSED RULEMAKING

C. REQUIREMENTS AND SOLUTIONS

62. In this section we discuss a carrier's obligations under section 103 and compliance solutions as they relate to broadband access and VoIP services. Based on the comments filed on the Petition, we believe there are several outstanding issues in each of these areas that must be addressed if we are to ensure successful implementation of CALEA.

1. Carrier obligations under section 103

63. Packet technologies are fundamentally different from the circuit switched technologies that were the primary focus of the Commission's earlier decisions on CALEA. These differences have led to disagreements among Law Enforcement and industry as to how to interpret and apply telecommunications carriers' obligations under section 103 of CALEA. Telecommunications carriers are required, under section 103, to enable LEAs, pursuant to a court order or other lawful authorization, (1) to intercept, to the exclusion of other communications, wire and electronic communications carried by the carrier to or from a subject, and (2) to access call-identifying information that is reasonably available to the carrier, subject to certain conditions. Further, the interception of communications or access to call-identifying information is to be delivered to LEAs in a format that may be transmitted, over the equipment, facilities or services procured by LEAs, to a location other than the provider's premises and in a way that protects the privacy and security of communications and information not authorized to be intercepted or accessed.

64. CALEA defines call-identifying information as "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." In applying this definition to the initial J-STD-025, which dealt primarily with circuit-switched networks, the Commission determined that call-identifying information was not limited to telephone numbers and that it was appropriate in some cases to use a functional equivalent to give meaning to the statutory terms (*e.g.*, wireless carriers identify the physical location of the antenna tower that a mobile phone uses to connect at the beginning and end of a call). The Commission adopted the following definitions of the component terms in the statutory definition of call-identifying information: **origin** is a party initiating a call (*e.g.*, a calling party), or a place from which a call is initiated; **destination** is a party or place to which a call is being made (*e.g.*, the called party); **direction** is 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); and **termination** is 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). The Commission concluded that these definitions defined call-identifying information in a manner that could be converted into actual network capabilities and would accommodate CALEA's intent to preserve the ability of LEAs to conduct electronic surveillance as technology changes.

65. We believe that carriers, manufacturers and Law Enforcement have applied the statutory definition of call-identifying information, as well as the Commission's definitions for the terms origin, destination, direction and termination, in developing standards or proprietary solutions for packet-mode technologies. However, the exact application of these terms is not always clear. Call-identifying information may be found within several encapsulated layers of protocols.[1] For

[1] In the Open System Interconnection ("OSI") model, layered network architecture for packet networks typically consists of seven layers: physical, data link, network, transport, session, presentation and

example, the data link layer (supported by switches or bridges) contains hardware source and destination address information; the network layer (supported by routers) contains the source and destination IP address; and the transport/session/presentation/application layers (supported by host devices and gateways) contain source and destination port addresses, session sources and destinations, and session start and stop times. As the packet makes its way through the network of the broadband access service and Internet service providers, these providers' equipment generally do not examine or process information in the layers used to control packet-mode services such as VoIP, and in fact operate at layers below the ones that carry control information for broadband access services. As a result, the broadband access service and Internet service providers may not be able to easily isolate call-identifying information for VoIP without examining the packet in detail, or in other words, examining the packet content.

66. There are potentially several kinds of information about broadband access service that Law Enforcement may seek under section 103's requirements. For broadband access these potentially include, but are not necessarily restricted, to the following: (1) information about the subject's access sessions, including start and end times and assigned IP addresses, for both mobile and fixed access sessions; (2) information about changes to the subject's service or account profile, which could include, for example, new or changed logins and passwords; and (3) information about packets sent and received by the subject, including source and destination IP addresses, information related to the detection and control of packet transfer security such as those in Virtual Private Networks ("VPNs"), as well as packet filtering to favor certain traffic going to or from certain customers. For VoIP, the concept of "call" seems well understood, and we might expect call-identifying information to include who called whom when for how long, and concepts similar to call-identifying information for circuit-mode calls.

67. We seek comment on whether the Commission needs to clarify the statutory term "call-identifying information" for broadband access and VoIP services. We ask that commenters provide specific suggestions for these definitional issues. A more precise understanding of these terms would support the Commission's efforts to encourage carriers' compliance with their CALEA obligations whether in acting on petitions filed under sections 107(c) or 109(b) or in pursuing enforcement actions for violations of the Commission's rules. We also invite comment as to how the Commission should apply the term "reasonably available" to broadband access. We observe that the Commission has previously determined that information may not be "reasonably" available if the information is only accessible by significantly modifying a network. The Commission applied these criteria when determining that dialed-digit extraction ("DDE") could be made available without significantly modifying a circuit-switched network because the information was present at the circuit intercept access point. Although carriers would have to incur some costs to extract the information, we did not view cost as a factor in whether information is "reasonably available" for purposes of section 103(a)(2). We determined that cost

---

application. The model calls for the independent operation of the layers, and supports the interaction of various applications and equipment that is designed to address separately each layer in a product offering. In the Transport Control Protocol ("TCP")-IP model, only four levels are used: link (combines OSI physical and data link levels), network, transport and application (combines OSI session, presentation and application levels). The functions supported at each layer are as follows: *physical*—represents electrical signaling, modulation, etc.; *data link*—moves packets (also called "datagrams") between hosts based on a protocol such as Ethernet, Asynchronous Transfer Mode, frame relay; *network*—defines how data is routed between hosts over one or several networks, often based on IP; *transport*—establishes the connection between two hosts, creating a "virtual" network, often based on TCP or Universal Datagram Protocol; *session*—controls the setup and termination of communications sessions; *presentation*—defines the format of the data exchanged (*e.g.*, text, graphic); *application*—defines how applications communicate with each other over the network (*e.g.*, e-mail) using various protocols.

concerns were best addressed as part of a section 107(b) analysis in deciding whether to require the provision of DDE.

68. We tentatively conclude that we should apply the same criteria—*i.e*. information may not be "reasonably" available if the information is only accessible by significantly modifying a network—to broadband access and VoIP providers. We seek comment on this tentative conclusion. We recognize that, when looking at end-to-end service architectures, it is not always readily apparent where call-identifying information is available. We seek comment on where content and various kinds of call-identifying information are available in the network and further whether the information is reasonably available to the carrier. We anticipate that some call-identifying information may be available from either a VoIP provider or a broadband access provider. In these instances, would the call-identifying information be reasonably available from one entity but not from the other? If the information is reasonably available from both carriers, we expect that both carriers would have a CALEA obligation with respect to that information and would work cooperatively with each other and with the LEA to provide the LEA with all required information. We seek comment on these issues.

OPERATIONAL RULES FOR CALEA COMPLAINCE

TITLE 47--TELECOMMUNICATION
CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION
PART 64--MISCELLANEOUS RULES RELATING TO COMMON CARRIERS
Subpart V--Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)

****

Sec. 64.**2103** Policies and procedures for employee supervision and control.

A telecommunications carrier shall:

(a) Appoint a senior officer or employee responsible for ensuring that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier.

(b) Establish policies and procedures to implement paragraph (a) of this section, to include:

(1) A statement that carrier personnel must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information;

(2) An interpretation of the phrase ``appropriate authorization'' that encompasses the definitions of appropriate legal authorization and appropriate carrier authorization, as used in paragraph (b)(1) of this section;

(3) A detailed description of how long it will maintain its records of each interception of communications or access to call-identifying information pursuant to Sec. 64.2104;

(4) In a separate appendix to the policies and procedures document:

(i) The name and a description of the job function of the senior officer or employee appointed pursuant to paragraph (a) of this section; and
(ii) Information necessary for law enforcement agencies to contact the senior officer or employee appointed pursuant to paragraph (a) of this section or other CALEA points of contact on a seven days a week, 24 hours a day basis.

(c) Report to the affected law enforcement agencies, within a reasonable time upon discovery:

(1) Any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities; and
(2) Any act of unlawful electronic surveillance that occurred on its premises.

Sec. 64.**2104** Maintaining secure and accurate records.

(a) A telecommunications carrier shall maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification.

(1) This certification must include, at a minimum, the following information:

(i) The telephone number(s) and/or circuit identification numbers involved;

(ii) The start date and time that the carrier enables the interception of communications or access to call identifying information;

(iii) The identity of the law enforcement officer presenting the authorization;

(iv) The name of the person signing the appropriate legal authorization;

(v) The type of interception of communications or access to call-identifying information (e.g., pen register, trap and trace, Title III, FISA); and

(vi) The name of the telecommunications carriers' personnel who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under Sec. 64.2103.

(2) This certification must be signed by the individual who is responsible for overseeing the interception of communications or access to call-identifying information and who is acting in accordance with the telecommunications carrier's policies established under Sec. 64.2103. This individual will, by his/her signature, certify that the record is complete and accurate.

(3) This certification must be compiled either contemporaneously with, or within a reasonable period of time after the initiation of the interception of the communications or access to call-identifying information.

(4) A telecommunications carrier may satisfy the obligations of paragraph (a) of this section by requiring the individual who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under Sec. 64.2103 to sign the certification and append the appropriate legal authorization and any extensions that have been granted. This form of certification must at a minimum include all of the information listed in paragraph (a) of this section.

(b) A telecommunications carrier shall maintain the secure and accurate records set forth in paragraph (a) for a reasonable period of time as determined by the carrier.

(c) It is the telecommunications carrier's responsibility to ensure its records are complete and accurate.

(d) Violation of this rule is subject to the penalties of Sec. 64.2106.

Sec. 64.**2105** Submission of policies and procedures and commission review.

(a) Each telecommunications carrier shall file with the Commission the policies and procedures it uses to comply with the requirements of this subchapter. These policies and

procedures shall be filed with the Federal Communications Commission within 90 days of the effective date of these rules, and thereafter, within 90 days of a carrier's merger or divestiture or a carrier's amendment of its existing policies and procedures.

(b) The Commission shall review each telecommunications carrier's policies and procedures to determine whether they comply with the requirements of Sec. 64.2103 and Sec. 64.2104.

(1) If, upon review, the Commission determines that a telecommunications carrier's policies and procedures do not comply with the requirements established under Sec. 64.2103 and Sec. 64.2104, the telecommunications carrier shall modify its policies and procedures in accordance with an order released by the Commission.

(2) The Commission shall review and order modification of a telecommunications carrier's policies and procedures as may be necessary to insure compliance by telecommunications carriers with the requirements of the regulations prescribed under Sec. 64.2103 and Sec. 64.2104.

Sec. 64.**2106** Penalties.

In the event of a telecommunications carrier's violation of Sec. 64.2103 or Sec. 64.2104 of this subchapter, the Commission shall enforce the penalties articulated in 47 U.S.C. 503(b) of the Communications Act of 1934 and 47 CFR 1.8.