May 15,2007

FILED/ACCEPTED

MAY 1 52007

Federal Communications Commission
Office of me Secretary

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington. D.C. 20554

Re: In the Matter of Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act

Petition for Expedited Rulemaking

Dear Ms. Dortch:

Transmitted herewith by the United States Department of Justice, including the Federal Bureau of Investigation, Drug Enforcement Administration, and National Security Division, attached for filing please find an original and four copies of the .Petition for Expedited Rulemaking" in the above-referenced matter.

Thank you for your attention to this matter.

Sincerely,

Elaine N. Lammert
Deputy General Counsel
Investigative Law Branch
Federal Bureau of Investigation

No. of Copies rec'd 0+4
List ABCDE
PA HSB 02-27

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Petition for Expedited Rulemaking to	)	Docket No. 07- _____
Establish Technical Requirements and	)	
Standards Pursuant to Section 107(b) of the	)	
Communications Assistance for Law	)	
Enforcement Act	)	

PETITION FOR EXPEDITED RULEMAKING

Sigal P. Mandelker
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
United States Department of Justice
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Charles M. Steele
Chief of Staff
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Michael L. Ciminelli
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
United States Department of Justice
Washington, D.C. 20537

TABLE OF CONTENTS

SUMMARY

Lawfully authorized electronic surveillance is a critical tool in law enforcement's efforts to combat terrorism, narcotics trafficking, and other crimes. Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA) to ensure that ongoing and future technological changes in the communications industry would not compromise the ability of federal, state, and local law enforcement agencies to engage in lawfully authorized electronic surveillance in order to protect public safety and national security. To that end, CALEA requires that telecommunications carriers ensure that their equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement agencies all call-identifying information and communications content that those agencies lawfully are authorized to access.

CALEA sets forth general requirements, but contemplates that the communications industry, acting in consultation with the Attorney General, will develop technical requirements and standards that meet the assistance capability requirements of the statute. Where an industry standard does not meet CALEA's mandate, CALEA authorizes the Federal Communications Commission ("Commission") to issue rules establishing additional technical requirements and standards.

The United States Department of Justice ("DOJ") requests that the Commission initiate an expedited rulemaking proceeding, pursuant to Section 107(b) and related provisions, with respect to the CALEA standard for CDMA2000 packet data wireless

services published jointly by the Telecommunications Industry Association and the Alliance for Telecommunications Industry Solutions as an American National Standard Institute standard ("J-STD-025-B"). J-STD-025-B is deficient because it fails to include certain assistance capabilities that are required by CALEA Section 103. Specifically, J-STD-025-B does not include capabilities that would provide: **(1)** packet activity reporting; (2) timing information (time stamping); (3) all reasonably available handset location information at the beginning and the end of a communication; and **(4)** adequate security, performance, and reliability requirements. Unless carriers provide these required capabilities, information that is critical to public safety and national security will be lost, and Congress' goal of preserving surveillance capabilities in the face of technological changes will be seriously compromised.

This Petition explains why J-STD-025-B is deficient and what capabilities should be added or modified to carry out CALEA's mandates. DOJ respectfully requests that, pursuant to CALEA Section 107(b), the Commission:

(1) Find that J-STD-025-B is deficient because it does not include certain assistance capabilities that are required by CALEA Section 103;

(2) Establish rules requiring telecommunications carriers to provide the additional and modified assistance capabilities described in this Petition; and

(3) Require telecommunications carriers to provide the additional and modified capabilities within twelve months after the effective date of the Commission's decision in this proceeding.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, **D.C. 20554**

In the Matter of	)	
	)	
Petition for Expedited Rulemaking to	)	Docket No. 07- _____
Establish Technical Requirements and	)	
Standards Pursuant to Section 107(b) of the	)	
Communications Assistance for Law	)	
Enforcement Act	)	

PETITION FOR EXPEDITED RULEMAKING

I. Introduction

The United States Department of Justice ("DOJ"), pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act ("CALEA"),[1] hereby petitions the Federal Communications Commission ("Commission") to initiate an expedited rulemaking proceeding regarding American National Standard Institute ("ANSI")[2]

---

1 **47** U.S.C. § 1006(b).

2 ANSI coordinates the development and use of voluntary consensus standards in the United States. See http://www.ansi.ore;/about ansi/overview/overview.aspx?menuid=1 (last viewed May 14, 2007). J-STD-025-B was developed by the Telecommunications Industry Association ("TIA") and published jointly by the TIA and the Alliance for Telecommunications Industry Solutions ("ATIS) as an ANSI standard. TIA is a contributor of voluntary industry standards that support global trade and commerce in communications products and systems. See http://www.tiaonline.org/ business/about/ (last viewed May 14, 2007). ATIS is a United States-based standards organization that develops and promotes technical and operations standards for the communications and related information technologies industry worldwide. See http://www.atis.org/about.shtml (last viewed May 14,2007).

J-STD-025-B, the CALEA standard for CDMA2000[3] packet data wireless services ("J-STD-025-B").[4]

CALEA Section 103 sets forth assistance capability requirements designed to ensure that law enforcement can conduct lawfully authorized electronic surveillance ("LAES) and directs telecommunications carriers to design, develop, and deploy solutions that meet those requirements.[5] Specifically, Section 103 requires a telecommunications carrier to ensure that its equipment, facilities, or services are

---

3 "CDMA" is the abbreviation for "Code Division Multiple Access." "CDMA2000" is an International Telecommunications Union-approved third generation ("3G") wireless communications standard that provides voice and data capabilities. See QUALCOMM, Inc. website at http://www.qualcomm.com/technology/1x.html (last viewed May 14, 2007). CDMA2000 1x – the world's first operational 3G technology – was launched commercially by wireless carriers in 2000 and is capable of transmitting data faster than most dial-up services. *See* http://www.3gtoday.com (last viewed May 14, 2007). There are currently eight CDMA2000 1x operators in the United States. *Id.*

4 The Commission has authority to act on this Petition on an expedited basis. Expedited consideration of a petition is warranted when a petitioning party demonstrates that it is necessary in order to serve the public interest. *See In the Matter of Omnipoint Corp. v. PECO Energy Co.*, 12 FCC Rcd 24439, 24441 ¶ 3 (1997); *see also In the Matter of Review of the Pioneer's Preference Rules*, First Report and Order, 9 FCC Rcd 605 (1994) (granting request for expedited treatment because it was in the public interest to reach an early decision in the proceeding). Expedited consideration of this Petition is in the public interest because, without the additional and modified capabilities requested herein, information critical to terrorism and other criminal investigations and prosecutions will be lost, risking both public safety and national security. Moreover, if the deficiencies in the standard are not immediately addressed, law enforcement, telecommunications carriers, and equipment manufacturers will be uncertain as to how to proceed, thereby adversely affecting the development and deployment of CALEA solutions for wireless packet data services.

5 47 U.S.C. § 1002.

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.[6]

J-STD-025-B is deficient because it fails to include certain assistance capability requirements mandated by CALEA Section 103. As a result, carriers that rely on J-STD-025-B will not provide federal, state, and local law enforcement agencies[7] with all of the call-identifying information ("CII") and communications content to which, pursuant to lawful authorization, they are entitled under CALEA Section 103. As discussed in more detail below, J-STD-025-B does not include the following capabilities: **(1)** packet activity reporting; (2) timing information (time stamping); **(3)** all reasonably available mobile

---

6 47 U.S.C. § 1002(a).

CALEA Section 107(a) directs the Attorney General, in coordination with other federal, state, and local law enforcement agencies, to consult with standard-setting organizations concerning implementation of the assistance capability requirements of Section 103. See 47 U.S.C. § 1006(a). The Director of the Federal Bureau of Investigation ("FBI") is charged with carrying out the responsibilities conferred upon the Attorney General under CALEA. See 28 C.F.R. § 0.85(o). Pursuant to this delegation of responsibility, the FBI has worked with numerous representatives of federal law enforcement agencies and major state and local law enforcement agencies to develop and coordinate law enforcement's positions on CALEA implementation issues, including standards issues.

handset* location information at the beginning and the end of a communication; and (4) adequate security, performance, and reliability requirements. Without these required capabilities, law enforcement will be unable to carry out LAES fully and effectively. As a result, information that is critical to preserving public safety and national security will be lost, and Congress' goal of preserving law enforcement's electronic surveillance capabilities in the face of technological changes will be seriously compromised

Section 107(b) authorizes the Commission to issue rules establishing additional technical requirements and standards upon petition by a government agency or any other person who believes that an industry-adopted technical requirement or standard is deficient (i.e., does not meet the assistance capability requirements of CALEA Section 103).[9] Accordingly, DOJ respectfully requests that pursuant to CALEA Section 107(b), the Commission:

(1) Find that J-STD-025-B is deficient because it does not include certain assistance capabilities that are required by CALEA Section 103;

(2) Establish rules requiring telecommunications carriers to provide the additional and modified assistance capabilities described in this Petition;[10]

---

8 For purpose of this Petition, the term "mobile handset" refers to any device that a subscriber uses to connect to a wireless carrier's CDMA2000 packet data network, including, but not limited to, a cell phone, smart phone, personal digital assistant, or wireless modem.

9 47 U.S.C. § 1006(b).

10 It should be noted that any rules established by the Commission requiring carriers to provide the additional and/or modified capabilities described herein should also be applicable with respect to other published standards where the same capabilities are at issue.

and

(3) Require telecommunications carriers to provide the .additional and modified capabilities within twelve months after the effective date of the Commission's decision in this proceeding.

II. History of the Development of J-STD-025-B

CALEA Section 107 authorizes telecommunications carriers and manufacturers of telecommunications equipment to meet the requirements of Section 103 by developing and complying with "standards adopted by an industry association or standard-setting organization . . . ."[11] Although industry groups develop and adopt these standards, Congress also clearly established a role for law enforcement in the standard-setting process. Specifically, CALEA Section 103 directs the Attorney General, in coordination with other law enforcement agencies, to consult with appropriate telecommunications industry associations and standard-setting organizations in the development of CALEA standards.[12]

In 2001, TIA began developing J-STD-025-B as a CALEA standard for CDMA2000 packet data wireless services. The wireless packet data services within the scope of J-STD-025-B include, among others, wireless Internet access service, picture mail service, one- and two-way video services, and text messaging services. J-STD-025-

---

11 *Id.* § 1006(a)(2).

12 47 U.S.C. § 1006(a)(1). The Director of the FBI is charged with carrying out the responsibilities conferred upon the Attorney General under CALEA. See 28 C.F.R. § 0.85(o).

B is not intended to apply to voice services.

TIA initially based J-STD-025-B on an existing TIA/ATIS ANSI joint standard called J-STD-025-A,[13] which contains CALEA capabilities for circuit-switched voice wireline and wireless communications services.[14] As work on J-STD-025-B progressed, however, critical capabilities that are included in J-STD-025-A and which have previously been determined by the Commission to be required by CALEA (e.g., timing information capabilities)[15] were eliminated from J-STD-025-B.

In accordance with its consultative role,[16] the FBI actively participated in numerous TIA meetings concerning the development of J-STD-025-B. Throughout the course of J-STD-025-E's development, the FBI suggested possible modifications to the draft standard designed to incorporate critical assistance capabilities that are required

---

13 J-STD-025-A was one of the first CALEA standards developed in the wake of CALEA's enactment. J-STD-025-A defines the interfaces between a telecommunications service provider and a law enforcement agency to assist the law enforcement agency in conducting LAES, including services and features to support LAES and to deliver intercepted communications and CII to law enforcement agencies. See ANSI/J-STD-025-A-2003, § 1.2.

14 J-STD-025-A also contains a very limited set of CALEA capabilities for packet data services not relevant to this Petition. See ANSI/J-STD-025–A-2003, §§ 4.6.3, 5.4.3, 5.4.2, & 5.4.11.

15 *See In the Matter of Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, 16835 ¶ 95 (1999) *("Third R&O"), aff'd in part and vacated in part* by *United States Telecom. Ass'n v. F.C.C.*, 227 F.3d 450,465 (D.C. Cir. 2000).

16 *See* 47 U.S.C. § 1006(a)(1).

by Section 103 but were missing from the standard.[17] The majority of the FBI's proposed changes, however, were not included in TIA's final version of J-STD-025-B. Accordingly, DOJ files this petition requesting that the Commission issue rules establishing additional technical requirements in order to address the deficiencies in the standard.[18]

III. Overview of the Capabilities Not Provided for in J-STD-025-B

As more fully explained below, J-STD-025-B does not include capabilities that would provide: (1) packet activity reporting; (2) timing information (time stamping);

---

[17] The FBI provided TIA with several contributions to J-STD-025-B during the drafting stage. See, *e.g.,* Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) Capabilities for Packet-based Communications Pursuant to the Communications Assistance for Law Enforcement Act (CALEA) (Jan. 21, 2002) (copy attached as Appendix A); CALEA Implementation Unit (CIU) Vote on Letter Ballot **1174,** at 1 (submitted Sept. **17,** 2003) (listing the various contributions submitted by CIU during the development of J-STD-025-B) (copy attached as Appendix B). The FBI also provided fifteen specific comments on the proposed standard after it was balloted for approval by TIA members, in an effort to cure the standard's deficiencies. See CALEA Implementation Unit Vote on Letter Ballot 1174 (submitted Sept. 17,2003) (submitting a "no" vote on the proposed J-STD-025-B standard and identifying numerous deficiencies contained in the proposed standard) (see Appendix B). These comments were later reiterated in the FBI's reply to a call for comments on J-STD-025-B as a trial use standard. See Letter from Gregory Milonovich, Supervisory Special Agent, CALEA Implementation Unit, FBI, to Susan Carioti, ATIS (Apr. 16, 2004) (copy attached as Appendix C).

[18] TIA published the final version of J-STD-025-B as a TIA "trial use" standard in January 2004. In March 2004, the "trial use" version of J-STD-025-8 was submitted for ballot to both TIA and ATIS as a proposed ANSI standard. Because "trial use" standards are superseded by the publication of an ANSI standard, DOJ waited to file this Petition until after the publication of the ANSI version of the standard, which occurred in August 2006.

(3) all reasonably available mobile handset location information at the beginning and the end of a communication; and (4) adequate security, performance, and reliability requirements.

Three of these capabilities – packet activity reporting, timing information, and all reasonably available mobile handset location information – are CII-related capabilities that are necessary to ensure that carriers can isolate and deliver CII, as required by CALEA Section 103.[19] A packet activity reporting capability, which identifies Internet protocol ("IP") addresses, port numbers, and transport layer protocol information for the source and destination of an IP packet, would ensure that law enforcement agencies receive information that is critical to identifying the parties to a packet data communications session and the locations between which the data is sent. A timing information (time stamping) capability, which prescribes the timing and procedures for delivery of CII messages to law enforcement agencies, would enable law enforcement agencies accurately to correlate CII with communications content. **A** capability that provides all reasonably available mobile handset location information at the beginning and the end of a communication would allow isolation and delivery of the most

---

[19] The Commission held in the *Third RDO* that call-identifying information that is "present at a carrier's [intercept access point] and can be made available without the carrier being unduly burdened with network modifications . . ." is reasonably available. *Third RDO* at 16809 ¶ 28. The CII that would be provided via the above-described capabilities is present at a carrier's intercept access point ("IAP") because the same CII is already used by carriers for purposes of their normal commercial (business) operations. Therefore, DOJ expects that this CII can be made available without the carrier being unduly burdened with network modifications.

accurate location CII that is reasonably available to a CDMA2000-based wireless carrier where lawfully authorized. In many cases, such CII will be the more accurate longitude and latitude location information for the subscriber's mobile handset – information that carriers already use for E-911 compliance, delivery of location-based services, and other business purposes.

J-STD-025-B also fails adequately to address the security, performance, and reliability requirements mandated by Section 103.[20] CALEA's security requirement mandates, among other things, that carriers ensure that electronic surveillance is not detectable by the subject; use procedural safeguards to protect the controls used for LAES and intercepted CII and communications content; and protect the delivery of CII and communications content to law enforcement. The performance and reliability requirement mandates that carriers ensure the completeness and quality of service for the electronic surveillance intercept (e.g., packet loss, bit error rate, etc.) and ensure the reliability of the electronic surveillance information delivered to law enforcement.

IV. Packet Activity Reporting, Time Stamping of Packet Data, and Longitude/Latitude Information Are Required Call-Identifying Information Capabilities That Should Be Included in J-STD-025-B

CALEA requires that a carrier "expeditiously isolat[e] and enabl[e] the government . . . to access the call-identifying information that is reasonably available to

[20] 47 U.S.C. §§ 1002(a)(2)-(4), 1004.

the carrier."[21] CALEA defines the term "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."[22] As both the United States Court of Appeals for the D.C. Circuit ("D.C. Circuit") and the Commission have recognized, "call identifying information" is not limited merely to telephone numbers; it also includes signaling information.[23] In holding that CII "must identify the origin, termination, direction, or destination of each communication," the Commission defined these terms as follows:

> [O]rigin 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).[24]

---

21 *See id.* § 1002(a)(1)-(2).

22 *Id.* § 1001(2).

23 *United States Telecom. Ass'n*, 227 F.3d at 458 ("CALEA's definition of 'call identifying information,' moreover, refers not just to 'dialing...information,' but also to 'signaling information,' leading us to believe that Congress may well have intended the definition to cover something more than...telephone numbers."); *In the Matter of Communications Assistance for Law Enforcement Act,* Order on Remand, 17 FCC Rcd 6896, 6911 ¶ 47 (2002) *("Order on Remand")* (stating that CII consists of dialing and signaling information that is not limited to telephone numbers).

24 *Order on Remand* at 6911 ¶ 47.

As the Commission makes clear in its *Order on Remand,* these definitions are intended to "accommodate CALEA's intent to preserve the ability of law enforcement to conduct electronic surveillance effectively and efficiently in the face of rapid advances in telecommunications technology."[25] A carrier that provides CDMA2000 packet data services, therefore, must be capable of isolating and delivering CII that identifies the "origin, destination, direction, and termination" of a communication. As described below, packet activity, time stamping, and all reasonably available mobile handset location information at the beginning and the end of a communication are CII that is reasonably available to carriers. Accordingly, to meet CALEA's requirements, any standard must ensure that carriers have the capability of isolating and delivering these types of CII.

A. Packet Activity Reporting

1. Packet Activity Reporting Is a Required CII Capability

Packet activity reporting refers to a carrier's ability to isolate and deliver the CII contained in IP communications packets that are sent by or to an intercept subject. This capability permits the carrier to report the CII associated with the origin, destination, or termination of a particular packet. It includes the ability to **(1)** detect packets being sent by or to the subject, (2) retrieve CII from those packets, and (3) deliver it to law enforcement. The packet activity that would be reported pursuant to this capability

---

[25] *Id.* at 6911 ¶ 48.

consists of the IP addresses, port numbers, and transport layer protocol information for the source and destination of an IP packet. Each of these forms of packet activity falls squarely within the CALEA definition of CII because each constitutes "signaling information that identifies the origin . . . destination, or termination of [a] communication generated or received by a subscriber" of the carrier's service.[26] Moreover, the packet activity CII that would be provided pursuant to this capability in a packet-mode communications context is analogous to the CII provided pursuant to J-STD-025-A that permits law enforcement to identify the origin and destination of communications transmitted by or to an intercept subject in a circuit-switched network – e.g., called and calling party information.[27]

First, IP addresses are network addresses; they identify computers and devices connected to a network so that data packets transmitted from other computers and devices can reach them. They are akin to telephone numbers in that they provide a device-specific number that allows one person using a computer or other device to reach another on the Internet, just as a telephone number allows a telephone to reach

---

[26] 47 U.S.C. § 1001(2).

[27] The Commission held in the *Order on Remand* that it is proper to view "call identifying information" as consisting of dialing or signaling information not limited to telephone numbers, provided such information identifies the origin, termination, direction, or destination of each communication. *Order on Remand* at *6911* ¶ 47. The Commission defined the term "origin" to include "a party initiating a call . . . or a place from which the call is initiated," and the term "destination" to include "a party or place to which a call is being made." *Id.*

another telephone connected to the public switched telephone network.[28] As such, the IP address of the subject is CII that identifies the "origin" of the communication when the subject initiates a communication, or the "destination" or "termination" of a communication when the subject receives a packet communication from an associate or the network.[29] Conversely, the IP address of the associate is CII that identifies the "destination" or "termination" when the subject transmits a packet communication to an associate, or the "origin" when the associate transmits the packet communication to the subject. Another field called "version" states the IP version used – e.g., IPv4 or IPv6. The "version" field facilitates the identification of the format of the other fields contained in the IP header.

Second, ports are used to identify the ends of logical connections that carry conversations, which typically consist of multiple packets exchanged between endpoints.[30] Port numbers are addresses at the transport layer of the packet protocol (one layer above the IP layer). **A** port number represents an origin or destination, or

---

[28] *See Computer Networking FAQ #12: What is a port number?, available at* http://compnetworking.about.com/od/tcpip/1/blfaq012.htm (last viewed Dec. 28, 2006). The Commission has already found that telephone numbers are CII under CALEA. See *Order on Remand* at 6909 ¶ 39. CII includes, but is not limited to, a caller's telephone number. ***Id.*** at 6909 ¶ 39,6911 ¶ **47.**

[29] *Order on Remand* at 6911 ¶ 47. Moreover, carriers already utilize IP addresses and port numbers – which are packet activity CII – to route traffic in their networks, and some carriers also log such CII for security purposes.

[30] *See* IETF RFC 1700, Reynolds and Postel, at 15 (Oct. 1994) ("WELL KNOWN PORT NUMBERS), 38 ("REGISTERED PORT NUMBERS").

alternatively an endpoint for network communications,[31] and often identifies the application type understood to be using that port.[32] A contact or "well-known" port can also be used to provide services to unknown callers.[33] Taken together with an IP address, a port number identifies both a computer and a "channel" within that computer where the network communication will take place.[34] Destination and origination transport ports also qualify as CII under CALEA because they can help identify the destination, termination, or origination points of packet data communications sessions, thus enabling law enforcement to determine to, and/or from, where data was sent.[35] Port numbers also help refine and narrow endpoints of particular types of communications, assisting law enforcement in focusing on specific

---

31 *See Definition of Port Number, available at* http://compnetworking.about.com/od/basicnetworkingconcepts/l/bldef_port.htm (last viewed May 14,2007).

32 *See* a commonly-used definition of the term "port," *available at* http://www.webopedia.com/TERM/p/port.html (last viewed Dec. 28, 2006). For example, Port 80 is used for HyperText Transfer Protocol (HTTP) traffic, which is an underlying protocol used by the World Wide Web, and Port 25 is used for Simple Mail Transfer Protocol (SMTP) traffic – i.e., transport of e-mail.

33 *See* IETF RFC 1700, Reynolds and Postel, at 15 (Oct. 1994).

34 *See Computer Networking FAQ #12: What is a port number?, available at* http://compnetworking.about.com/od/tcpip/1/blfaq012.htm (last viewed Dec. 28, 2006).

35 Delivery of port numbers in the packet-mode context is analogous to the delivery of "sub-addresses" in the circuit-switched context. Sub-addresses operate similarly to port numbers, in that they are generally passed by the network between calling and called endpoint where the network is the actual termination point for the information. J-STD-025-A specifies the delivery of sub-addresses if they are available to the carrier. Given that port numbers function similarly to sub-addresses, port numbers should be provided.

communications of a subject. Transport addresses may also be termed "port numbers."[36]

Third, transport layer protocol ensures reliable data delivery and end-to-end data integrity by providing connection-oriented services between two end systems.[37] A port number alone may not fully identify the destination, termination, or origination points of packet data communications sessions. In addition, the header on an IP packet contains a field identifying the next level protocol used in the data portion of the Internet datagram. The transport layer creates a transport address by combining the network layer address and a transport layer service access point ("SAP") number.[38]

2. The Commission Should Require Carriers to Provide a Packet Activity Reporting Capability

The Commission should establish a rule requiring carriers to provide a packet activity reporting capability. As discussed above, packet activity (i.e., IP addresses, port numbers, and transport layer protocols) is a form of CII that CALEA Section 103 requires carriers to be capable of isolating and delivering to law enforcement.[39] Because J-STD-025-B does not contain a packet activity reporting capability, carriers should not be allowed to rely on it to meet the capability requirements of Sections 103(a)(2) and

---

36 *See General* Glossary *Terms*, The Conference Zone Resource Center, *available* at *http://www.conferzone.com/resource/glossary.html* (last viewed May 14, 2007).

37 *Id.*

38 *Id.*

39 47 U.S.C. § 1002(a)(2)-(3).

(3).[40]

CALEA requires that telecommunications carriers ensure that their equipment, facilities, or services include these capabilities for good reason. The lack of a capability to isolate and deliver this most basic CII could seriously impede or compromise an investigation. Indeed, the most valuable CII generated during a packet data session is the "identities" (i.e., network addresses) of the communicating parties and port information relating to the other devices with which a subject is communicating.[41] Without a packet activity reporting capability, the only CII that law enforcement would receive for a subject's entire communications session (which could run for minutes or hours) is that the subject's session has started. By itself, this information provides, at best, an incomplete picture. The subject could be communicating with numerous other people or services during the course of the session, but law enforcement would not receive any of the associated network and transport layer CII (i.e., IP address(es), port number(s) or transport layer protocol(s)) that would allow law enforcement to interpret the communications session and/or correlate the communications content.[42] This would be akin to having a pen register/trap and trace ("PR/TT") in place that is unable either to

---

40 *Id.* § 1002(a)(1)-(3).

41 This information is analogous to the phone numbers received in a pen register/trap and trace context.

42 In the case of a single intercept, this would be correlating the communications content of the intercepted communication with other information, including CII; in the case of multiple simultaneous intercepts, it would be correlating both the content of each specific intercept with other information, including CII, *and* correlating the content

receive a single phone number for any calls made or to provide any information other than that the subject is using his telephone. Simply put, in the absence of a packet activity reporting capability, law enforcement will not receive the CII that identifies the endpoints of the communication, which is information critical to interpreting the communications session and/or correlating the communications content.

For privacy and other reasons, CALEA intentionally places the burden of isolating CII on carriers.[43] But the failure to provide a packet activity reporting capability results in a shift of the Section 103(a)(2) mandate from carriers to law enforcement because it requires law enforcement agencies to implement methods to extract the CII information themselves, and separate it from the contents of any wire or electronic communication. It is no answer for industry to argue that law enforcement could itself extract the required packet information from a broader packet stream. Shifting the task of extracting and reporting packet activity to law enforcement would create significant and potentially prohibitive costs and technical difficulties for law enforcement agencies – difficulties that would be particularly burdensome for state and local law enforcement agencies. This would conflict with both the language and the purpose of CALEA. Requiring carriers to provide this capability, however, would not only enable carriers to isolate CII from other information and deliver only the isolated CII to law enforcement, but also would harmonize CALEA's goal of protecting the

---

as among each of the multiple simultaneous intercepts.

[43] 47 U.S.C. § 1002(a)(1)-(2).