DOCKET FILE COPY DUPLICATE

May 15, 2007

FILED/ACCEPTED

MAY 15 2007

Federal Communications Commission
Office of the 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

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.org/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).

7 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[8] 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-B'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-B 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 R&O* 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 R&O* 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).

privacy and security of communications not authorized to be intercepted[44] with the government's authority to collect CII.[45]

B. Timing Information (Time Stamping)

1. Timing Information Is a Required CII Capability

Timing information is information that distinguishes and properly associates CII with the content of several communications that occur at approximately the same time. A timing information capability would require a carrier to time stamp each CII message within a specific amount of time from when the event triggering the message occurred, and send the CII message to law enforcement within a defined amount of time after the triggering event. Together, this allows law enforcement to associate the CII message with the communication content information (i.e., the communication) and associate the party contacted by the subject with the communication.

The Commission already has held in the *Third R&O* that a timing information requirement is a CII capability required by CALEA Sections 102(2) and 103(a)(2).[46] Specifically, the Commission stated:

> We will adopt a timing information requirement as an assistance capability requirement of section 103 of CALEA.

---

[44] *See id.* §§ 1002(a)(4)(A), 1006(b)(2).

[45] *See id.* § 1002(a)(2). Although Federal law does not prohibit law enforcement agencies from filtering a broader packet stream and extracting the authorized CII from that stream, implementing a packet activity capability would help alleviate the burden on law enforcement agencies, and at the same time complement CALEA's privacy requirements.

[46] *Third R&O* at 16835 ¶ 95.

> First, we find that time stamping is call-identifying information as defined in section 102(2) of CALEA. This information is needed to distinguish and properly associate the call identifying information with the content of several calls occurring at approximately the same time. In other words, time stamp information is needed to identify "the origin, direction, destination, or termination" of any given call and, thus, fits within the statutory definition of section 102(2). Second, we find that delivery of call identifying information, including time stamp information, to the [law enforcement agency] must, pursuant to section 103(a)(2), be provided in such a timely manner to allow that information "to be associated with the communication to which it pertains."[47]

In adopting a timing information requirement, the Commission also adopted specific parameters for delivery of the required timing information. Specifically, a CII message must be transmitted to the law enforcement agency's Collection Function within eight seconds of its receipt by the intercept access point ("IAP") 95% of the time, and with an accuracy within 200 milliseconds.[48] The timing information requirement – including the specific parameters for delivery of the required timing information – was codified in the Commission's rules[49] and remains in force today. As a result of the Commission's conclusions in the *Third R&O* and the adoption of a rule requiring a timing information capability, the timing information (time stamping) capability was

---

47 *Id.*

48 *Id.* at 16835 ¶ 96.

49 47 C.F.R. §§ 64.2202, 64.2203(c) (now contained in 47 C.F.R. §§ 1.20007(a)(14), (b)(5)).

added by industry to J-STD-025-A.[50] As more fully discussed below, there is no reason why this capability should not have been included in J-STD-025-B.

2. The Commission Should Reaffirm That Timing Information (Time Stamping) Is a Required Capability

Despite the requirements of CALEA Section 103(a)(2) and the Commission's directive in the *Third R&O*, J-STD-025-B does not contain language that establishes specific parameters for delivery of the required timing information (time stamping). As a result, unlike its predecessor J-STD-025-A, J-STD-025-B is ambiguous as to whether the Commission's timing requirements for accuracy and delivery of CII apply to packet data services.

J-STD-025-B's ambiguity over the timing information (time stamping) capability arises from a footnote added to a June 2004 version of J-STD-025-B at the request of an industry representative. The footnote stated that the *Third R&O's* timing "requirement is established by the [Commission] for *circuit-mode only*."[51] Notwithstanding that the Commission's *Third R&O* clearly addressed both circuit-mode and packet-mode communications,[52] certain TIA members took the position – based on the addition of the footnote – that the Commission's time stamping requirement does not apply to any packet data services. Although the footnote subsequently was removed from J-STD-

---

50 *See* ANSI/J-STD-025-A-2003, § 4.7.

51 Ballot Version of ANSI J-STD-025-B, §§ 3, 4.7 n.2 (June 2004) (emphasis added).

52 *Third R&O* at 16795 ¶ 1.

025-B, that standard is silent as to whether timing information (time stamping) must be provided, and several TIA members continue to this day to dispute whether the timing requirements set forth in the *Third R&O* apply to packet data services.

The Commission held in the *Third R&O* that circuit- and packet-mode communications services are each subject to CALEA, and adopted capabilities in the *Third R&O* that apply to *both* circuit- and packet-mode services.[53] Given the Commission's holding, it is entirely unclear why certain TIA members continue to maintain that the time stamping requirement does not apply to packet data services. The Commission should make clear that, irrespective of what the standard states, carriers nonetheless must comply with the letter and spirit of the Commission's timing information capability rule.

Although the Commission concluded in the *Third R&O* that J-STD-025 (later J-STD-025-A) was not a sufficient CALEA solution for packet-mode services,[54] the Commission set a September 2001 deadline for packet-mode compliance,[55] and specifically requested that TIA "study CALEA solutions for packet-mode technology and report to the Commission [by September 2000] on steps that can be taken, *including*

---

53 *Id.*

54 *Third R&O* at 19819 ¶ 55. The Commission's conclusion was rooted in its concerns about the technical mechanisms for providing the required capabilities to law enforcement, rather than the required capabilities themselves. *See id.* at 16795 ¶ 1, 16819-20 ¶¶ 55-56.

55 *Id.* at 16819 ¶ 55.

particular amendments to J-STD-025."[56] It is clear from the Commission's statements that such packet-mode compliance would include providing the capabilities adopted in the *Third R&O* via amendments to J-STD-025 – i.e., in J-STD-025-B. Therefore, there is nothing in the *Third R&O* that suggests that the capabilities adopted therein – including the timing information (time stamping) requirement – do not apply to packet-mode (data) services.[57]

Nor is there anything in the *Third R&O* that would preclude the application of the timing information requirements specified therein to packet-mode (data) services. In fact, the Commission's rules contain no distinction about the type of communications (i.e., circuit-mode vs. packet-mode) to which the timing capability applies; the rules state only that "wireline, cellular, and PCS telecommunications carriers shall provide to a [law enforcement agency] [a timing information capability]."[58]

Highly accurate timing information is critical for a number of important reasons. First, as the Commission recognized, time stamping is critical to proper correlation of the CII events to the associated intercepted communications content stream.[59] The less accurate the time stamp, the greater the possibility that multiple events occurring in the

---

[56] *Id.* (emphasis added); *see also id.* at 16820 ¶ 56. TIA commenced work on the J-STD-025-B packet data standard in direct response to the Commission's directive in the *Third R&O.*

[57] *Third R&O* at 16795 ¶ 1, 16819-20 ¶¶ 55-56.

[58] 47 C.F.R. § 1.20007(b)(5).

[59] *Third R&O* at 16835 ¶ 95.

same time frame will lead to a misinterpretation of the sequence of CII events.

Second, unlike traditional circuit-switched networks, electronic intercepts in packet data sessions may occur at multiple points (nodes) within a carrier's network. In fact, because of the diffuse nature of packet-based technologies (i.e., that packet data sessions can occur at multiple nodes in a carrier's network and involve multiple IAPs), time stamping is even more critical in the packet-mode communications context than the circuit-mode context. Thus, it is critically important that time stamping occur so that the CII events between these multiple network nodes can be properly correlated with the communications content.

Third, multiple simultaneous packet data sessions can be established by a user of packet-mode services. A time stamp capability is needed to correlate the CII events and communications content on a timeline for each session, and to permit law enforcement to distinguish between CII events for each different session. Moreover, to the extent that two communications sessions may be related, this level of accuracy will allow law enforcement to correlate, where necessary, the two sessions.

Finally, accurate time stamping for packet data intercepts – regardless of the format used to deliver the intercepted communications to law enforcement – is crucial to law enforcement's reconstruction of the sequence of events contained in the interception.

The lack of accurate timing information (time stamping) requirements frustrates CALEA's purpose because it impedes law enforcement's ability accurately to associate

CII with communications content. Indeed, as a practical matter, without accurate time stamping, law enforcement may not be able to correctly determine when the CII events occurred or correlate them with the communications content. As a result, a court order can be frustrated as much as if the information were not delivered to law enforcement at all.

Given that packet mode communications are subject to CALEA,[60] and in light of the Commission's conclusion in the *Third R&O* that timing information is CII under Section 102(2),[61] there is no rational basis for omitting a timing information (time stamping) assistance capability from a packet mode standard such as J-STD-025-B. Indeed, the fact that a time stamping capability is more significant with respect to packet-mode communications should compel its inclusion in such standards.

Therefore, in order to resolve any ambiguity, DOJ requests that the Commission reaffirm that a timing information (time stamping) requirement is applicable to packet data services, regardless of the technology used by the carrier to provide the service. In addition, DOJ asks the Commission to require that carriers provide, at a minimum, a timing information (time stamping) capability that meets the requirements prescribed in the *Third R&O* and codified in the Commission's rules – including the specific

---

60 *Id.* at 16795 ¶ 1.

61 *Id.* at 16835 ¶ 95.

parameters for delivery of the required timing information.[62, 63]

C. Capability to Provide All Reasonably Available Location Information for a Mobile Handset at the Beginning and the End of a Communication[64]

1. Signaling Information That Reveals the Location of a Mobile Handset Is Call-Identifying Information That Is Required to Be Provided Pursuant to Lawful Authorization When It Is Reasonably Available to a Carrier

J-STD-025-B also fails to provide all of the reasonably available CII regarding the location of a mobile handset at the beginning and the end of a communication. The location information capability in J-STD-025-B provides law enforcement only with "cell site" information – i.e., the location of the cellular tower with which a subject's mobile handset is connected – at the beginning and the end of a communication. As a practical

---

[62] The 200 millisecond time stamp requirement prescribed in the *Third R&O* (*see Third R&O* at 16835-36 ¶¶ 95-96) is reasonable for industry with respect to packet-mode services because it already is included in various CALEA packet data standards (e.g., ANSI standard T1.678; ANSI standard T1.724; TIA Trial Use Version of J-STD-025-B) and has been deployed by vendors and carriers. Moreover, several equipment manufacturers have stated publicly that the 200 millisecond time stamp requirement is feasible and provided by their equipment. There are also a number of protocols that support time synchronization of up to one (1) millisecond, including the Network Time Protocol (*see* IETF RFC 1305), Simple Network Time Protocol (*see* IETF RFC 2030), and the Precise Time Protocol (PTP) (*see* IEEE 1588).

[63] Since a time stamp indicates the date and time that an event is detected in the network, the time stamp also should include the time zone offset from universal coordinated time (UTC). A number of vendors already provide this feature as part of the time stamp capability.

[64] The discussion of, and positions regarding, a location information capability for wireless packet data services contained herein relates only to terrestrial use of such services, and does not relate to any potential separate use of such services on board aircraft in an air-to-ground communications services context.

matter, this capability frequently does not provide law enforcement with the information required and intended by CALEA, in terms of both type and accuracy. Many carriers today, moreover, have reasonably available to them additional signaling information that more accurately identifies the location of the mobile handset itself.

CALEA Section 103(a) requires, among other things, that a telecommunications carrier enable law enforcement agencies operating with proper legal authority to (1) intercept wire or electronic communications, and (2) access CII that is reasonably available to the carrier before, during, and immediately after the transmission of wire or electronic communications and in a manner that allows it to be associated with the communication to which it pertains.[65] Thus, Section 103 makes clear that law enforcement agencies are entitled, pursuant to lawful authorization, to receive all CII that is reasonably available to the carrier.

In evaluating the propriety of the particular location capability included in the original J-STD-025 CALEA standard, both the Commission and the D.C. Circuit held that cell site information concerning the location of a mobile handset at the beginning and the end of a communication is CII under CALEA.[66] As both the Commission and

---

[65] *See* 47 U.S.C. §§ 1002(a)(1) and (2).

[66] *See Third R&O* at 16815 ¶ 44 (finding that "a subject's cell site location at the beginning and end of a call is call-identifying information under CALEA"); *United States Telecom. Ass'n*, 227 F.3d at 463-64. The fact that information indicating the mobile handset location for mobile calls is signaling information that falls within the statutory definition of CII provided further support for the D.C. Circuit's conclusion. *See United States Telecom. Ass'n*, 227 F.3d at 463-64 (holding that the mobile phone signals at the

the D.C. Circuit found, location information at the beginning and the end of a communication identifies the origin or destination of the communication.[67] And as both the Commission and D.C. Circuit recognized, signaling that reveals the location of a mobile handset is CII that CALEA requires carriers to be "capable of . . . expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access" when reasonably available to the carrier.[68]

Signaling information that reveals the location of a mobile handset is indisputably CII. Accordingly, such information is required to be provided to law enforcement agencies pursuant to lawful authorization, where it is reasonably available to a carrier.

2. All Reasonably Available Signaling Information That Reveals the Location of a Mobile Handset Should Be Provided to Law Enforcement Pursuant to Lawful Authorization

CALEA Section 103(a)(2) requires carriers to isolate and enable law enforcement to access pursuant to lawful authorization CII that is reasonably available to the

---

beginning and end of a call necessary to achieve communications between the caller and the called party are signaling information that is call identifying information).

[67] *United States Telecom. Ass'n*, 227 F.3d at 463. Moreover, the Commission found in the *Third R&O* that at least cell site location information is reasonably available to wireless carriers. *Third R&O* at 16816 ¶ 45 (stating that "location information is reasonably available to cellular and broadband PCS carriers").

[68] *See Third R&O* at 16815-16 ¶¶ 44-45. Consistent with the statute, this Petition requests only capabilities to provide information that is reasonably available in carrier's networks.

carrier,[69] and contains only one restriction with respect to the provision of location information to law enforcement: it precludes a carrier from providing – "solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code)" ("PR/TT order") – information that may disclose the physical location of the subscriber, except where location may be determined from the telephone number.[70] The Commission stated in the *Third R&O* that the language in Section 103(a)(2)(B) ". . . does not exclude location information from the category of 'call-identifying information,' but simply imposes on law enforcement an authorization requirement different from that minimally necessary for the use of pen registers and trap and trace devices."[71] The Commission went on to state that its conclusion was justified because ". . . interpreting [Section 103(a)(2)(B)] to exclude location information from the technical requirements for CALEA would render the provision 'mere surplusage' and would thus conflict with the usual rules of statutory construction."[72] In upholding the Commission's conclusions concerning location information,[73] the D.C. Circuit agreed that such a reading was required by the "well-accepted principle of statutory construction that requires every provision of a

---

69 *See* 47 U.S.C. § 1002(a)(2).

70 *See id.* § 1002(a)(2)(B).

71 *Third R&O* at 16815 ¶ 44.

72 *Third R&O* at 16815 n.95.

73 *See United States Telecom. Ass'n*, 227 F.3d at 463.

statute to be given effect."[74] Accordingly, CALEA requires that carriers will provide law enforcement access to location information pursuant to Section 103(a)(2) and proper legal authorization *except* where the government acts "solely pursuant" to a PR/TT order.

Moreover, CALEA does not specifically delineate the type(s) of location information to be provided. Rather, the inclusion of the phrase "reasonably available to the carrier" in Section 103(a)(2) recognizes that different carriers could and would provide different location information based on availability in their respective networks. This supports the conclusion that CALEA does not otherwise limit or restrict the type of location information and related location information assistance capabilities that could and should be provided to law enforcement pursuant to lawful authorization. Thus, any reading of the statute that would preclude access to this information must be rejected.

3. The Commission Should Require Carriers to Provide All Signaling Information That Reveals the Location of a Mobile Handset That Is Reasonably Available to the Carrier Pursuant to Lawful Authorization

J-STD-025-B is deficient because it fails to specify that carriers provide all reasonably available signaling information that reveals mobile handset location information at the beginning and end of a communication that law enforcement is

---

[74] *Id.*

legally authorized to receive.[75] J-STD-025-B contemplates the delivery to law enforcement of cell site location information only, regardless of the availability of more precise signaling information in a carrier's network, and more importantly, the presence of a court order authorizing law enforcement to receive more than just the cell site identifier. Thus, a carrier that employs J-STD-025-B will not have the capability to provision a CALEA-based intercept for any court order that authorizes law enforcement to receive something beyond cell site location information (i.e., longitude- and latitude-based location information).

When the Commission evaluated the location information capability in the original J-STD-025 standard, it considered whether carriers should be required to provide more precise location information for the subject's mobile handset based on the facts as they then existed.[76] At that time, the Commission declined to require carriers to

---

[75] For example, J-STD-025-B misleadingly states that location information will be "provided for established packet data sessions, when authorized, to identify location information *for* the intercept Mobile Station (MS)." *See* J-STD-025-B, Tables 18 and 20 (emphasis added). The use of the word "for" would allow the location information capability to be satisfied by providing the Base Station identification (i.e., the mobile cell site or tower identification), rather than the actual location of the mobile handset, even where the more accurate information is available in the carrier's network. MS or mobile handset longitude/latitude information is far more useful, and should therefore be provided pursuant to lawful authorization when reasonably available to a carrier.

[76] *See id.* at 16815 ¶ 43. *See also* Comments of the New York City Police Department, CC Docket No. 97-213, at 7-8 (filed Dec. 18, 1998) (commenting that the location information that carriers should be required to provide is only that which is reasonably available to the carrier, and advocating that information used and/or available in a carrier's for purposes of providing overall service, maintenance, administration functionality, and call processing of individual calls should be considered to be

provide more precise location information, concluding that a more generalized location capability "[would] give [law enforcement agencies] adequate information."[77] The Commission went on to acknowledge, however, that its decision not to *require* the capability "does not preclude law enforcement agencies from requesting legal authority to acquire more specific location information in particular circumstances."[78]

Location identification technology has greatly advanced in its ability to precisely locate a wireless handset subscriber in the more than seven years since the Commission's *Third R&O* was issued. As a result of these advances, the types of signaling information reasonably available to carriers regarding handset location have changed dramatically. In particular, some carriers now use location technologies that result in more precise location information being generated by and reasonably available in their networks. These new technologies result in locations for the actual handsets that are more precise than those provided by older technologies – i.e., cell sites that would only allow extrapolation to general locations within a radius of miles.

These advances were spurred in part by the Commission's E-911 Phase II wireless services mandate, which requires wireless carriers to be capable of providing the precise latitude, longitude, and altitude location information for wireless

---

reasonably available).

[77] *See Third R&O* at 16816 ¶ 46. As discussed below, this has not generally been the case.

[78] *Id.*

subscribers' handsets. Many, if not most, carriers have deployed the E-911 Phase II location capability in their networks in response to the Commission's mandate.[79] Several carriers have leveraged this investment in better location information capabilities and routinely use their E-911 Phase II location information capability to assist them in other business and commercial operations, such as call completion and network management.[80] Carriers also have introduced new and improved wireless location service offerings to their subscribers.[81] CDMA2000 carriers and TIA already have developed and deployed a standard that enables wireless carriers to search for a subject's mobile handset location for commercial applications.[82] Thus, as a result of the

---

[79] 47 C.F.R. §§ 20.18(e), (g)(1)(v), (h). A list of the Commission's E-911 wireless decisions can be found at the Commission's website at http://www.fcc.gov/911/enhanced/releases.html#ro (last viewed May 14, 2007).

[80] Indeed, carriers use longitude and latitude location information for the purpose of identifying the "origin" (i.e., geographic location) of the subscriber's handset not only for E-911, but also for network management and efficiency purposes. For example, carriers often use the more precise information to route calls through an alternate cell tower – rather than the "default" tower or one to which the call would ordinarily have been routed based on its proximity to the caller – in order to reduce the burden on a particular tower for network efficiency.

[81] *See, e.g.*, http://www.nextel.com/en/services/gps/mobile_locator.shtml (describing Sprint's wireless location-based services, including the ability to track individual users) (last viewed May 14, 2007). In addition, wireless carriers, in cooperation with state and local governments, are already testing traffic monitoring systems that utilize the wireless carriers' handset location information in order to reduce congestion. Matt Richtel, *Tracking Phones for Traffic Reports*, INT'L HERALD TRIB., Nov. 11, 2005, at Finance, Pg. 19.

[82] TIA published a standard in early 2004 called TIA-881, which "enable[s] a wireless system to provide enhanced location services." *See* TIA, *TIA Publishes New Standard TIA-881,* Press Release, *available at*

E-911 mandate and consumer expectations and demand for new and better location-based wireless services, existing technology now routinely makes highly accurate geographical (latitude/longitude) wireless subscriber mobile handset location information "reasonably available" to carriers.[83]

In addition, although it is not relevant to whether Section 103 requires the location capability requested in this Petition, the Commission's conclusion in the *Third R&O* that a more generalized location capability would "give [law enforcement agencies] adequate information"[84] has not been borne out by subsequent experience. In

---

http://www.tiaonline.org/business/media/press_releases/legacy.cfm?parelease=04-65 (last viewed May 14, 2007).

[83] DOJ seeks to obtain, pursuant to proper legal authorization, all forms of signaling information that reveal the location of the subject's mobile handset at the beginning and the end of the communication only, and only when such location information is reasonably available to the carrier. DOJ's request that the Commission require carriers to be capable of providing more precise mobile handset location information (i.e., longitude/latitude) at the beginning and the end of each communication should in no way be construed as a request for a real-time tracking capability that would provide such information throughout the duration of the communication.

Such information will be "reasonably available" in many, if not most, carriers' networks by virtue of their compliance with the Commission's E-911 Phase II mandate. Given that other regulatory mandates already have directed carriers to deploy longitude/latitude-based mobile handset location capabilities, there would appear to be no reason not to leverage the existing presence of such capabilities with respect to CALEA. Such an approach would be consistent with CALEA's statutory purpose. In addition, just as the Commission's E-911 mandate calls for a phased-in approach whereby over time carriers would continue to improve the accuracy of the user information provided, so too should the accuracy of the location information provided to law enforcement pursuant to the requirements in Section 103 continue to improve over time as the result of technological advances and availability.

[84] *See Third R&O* at 16816 ¶ 46.

most cases, the more generalized cell site location information does not in fact provide law enforcement with "adequate" information, because it is frequently not usable in the manner in which the Commission anticipated. Both the operational challenges for law enforcement associated with the capability as adopted in the *Third R&O* and the technological advancements with respect to location identification in the last several years suggest that modifying the current location information capability as requested in this Petition is necessary and warranted in order to ensure that the location information capability's intended purpose is retained. Under the more generalized location information capability, carriers identify by cell site identifier the location of the cellular tower to which the handset is connected at the beginning and the end of a call. However, cell site information indicates only the general area in which a subject's mobile handset is located and cell sites often covers areas that are dozens or even hundreds of square miles, making it difficult for law enforcement to determine anything more than just the general vicinity of the handset.[85] Even worse, in some cases, the cell site location information that carriers provide to law enforcement is

---

[85] While many cell sites have a radius of one to three miles, some have a radius of as many as ten miles. Although a cell site with a one-mile radius will cover only approximately three square miles, a cell site with a three-mile radius will cover approximately 28 square miles, and a cell site with a ten-mile radius will cover approximately 314 square miles. While the combination of cell site plus sector identification serves to reduce the coverage area by approximately one-third, the coverage area would nonetheless remain quite large in many cases.

outdated and/or otherwise inaccurate.[86] Moreover, law enforcement has experienced problems with quickly and effectively correlating the cell site location information received from carriers to the physical location because there is no uniform carrier reporting mechanism for this information.

The Commission's conclusions in the original J-STD-025 deficiency proceeding should be read in light of their context. They do not preclude modifying the existing location information capability to require carriers to ensure access to all forms of signaling that reveal mobile handset location information that are now reasonably available to carriers. Moreover, a decision to adopt a rule requiring that all reasonably available signaling that reveals mobile handset location information be provided to law enforcement when authorized would not be inconsistent with the Commission's earlier position, given the technological advances and the operation of the capability in the years since the *Third R&O* was released. As discussed in this Petition, carriers' networks and services have evolved beyond their status at the time of the Commission's earlier decision. DOJ requests that the Commission require carriers to ensure law enforcement's ability to access all forms of signaling that reveal mobile handset location information pursuant to lawful authorization, when reasonably available to the carrier.

---

[86] The ability to accurately determine a subject's location is inherently tied to the quality of the mobile handset location information provided by the carrier. For the location information capability to work properly, carriers must regularly update tower site address location information and provide it to law enforcement. There have been times in the past, however, when carriers have not given law enforcement accurate location information for their cellular towers, rendering the cell site location

This will be the same signaling information that is already being made available by a number of carriers in connection with E-911 emergency services.[87]

In addition, in the original J-STD-025 deficiency proceeding, DOJ took the position in discussing the standard's location information capability that carriers need not have the capability to deliver more detailed location information in order to satisfy their obligations under CALEA.[88] DOJ also took the position that CALEA does not obligate carriers to design their networks to provide more extensive location information than what the standard itself specified.[89] These positions have not changed. DOJ's current request is that all signaling that reveals location information for a mobile handset at the beginning and the end of a communication be provided to law enforcement pursuant to lawful authorization *where such information is "reasonably*

---

information provided as part of the intercept solution useless.

[87] To the extent that the existence of such a capability may appear to the Commission to raise privacy concerns, the Commission may, as it has done previously, rely on the courts to regulate access to this information by law enforcement's proper showing of cause and need for such information in a particular case. *See Order on Remand* at 6927-28 ¶¶ 81-83 (concluding that whether a law enforcement agency is entitled to receive post-cut-through dialed digits under a particular type of legal authority is a legal question that should be left to the court that is considering a specific surveillance request).

[88] *See* Comments of the Department of Justice and the Federal Bureau of Investigation, CC Docket No. 97-213, at 74 (filed Dec. 18, 1998). DOJ did note, however, that although CALEA does not *require* carriers to deliver more extensive location information than cell site information, CALEA does not *prohibit* carriers from doing so where carriers have designed their networks to generate such information, and law enforcement has been legally authorized to obtain such information. *Id.*

[89] *See id.*

available" to a carrier. As discussed above, more accurate location information is now routinely generated by, and reasonably available in, many carriers' networks. Thus, carriers would not have to design (or redesign) their networks so as to create this information for the express purpose of complying with CALEA and providing it to law enforcement. Such information is already in carriers' networks and is being used by carriers and their customers. DOJ requests only that carriers be capable of providing this same reasonably available information when law enforcement is lawfully authorized in a specific matter to receive it.[90] Accordingly, DOJ requests that the Commission adopt a rule requiring carriers to be capable of providing all lawfully authorized mobile handset location information at the beginning and the end of a communication when such information is "reasonably available" to the carrier.

In addition, DOJ requests that the Commission require that a "toggle feature" be

---

[90] The Commission need only consider in the context of this proceeding whether the more precise/accurate mobile handset location information that would be provided by the modified capability is CII that should be provided to law enforcement pursuant to proper legal authorization where such information is reasonably available to the carrier. The Commission need not address – nor would it be appropriate for the Commission to address – the separate issue of what type of legal authorization law enforcement must obtain to be entitled to all forms of signaling information that reveals the location of a subject's mobile handset. For purposes of the Commission's analysis, the Commission can and should presume that law enforcement will have obtained the requisite legal authorization to enable it to request and receive such information from carriers. The Commission likewise should not fear that it will be opening the door to unauthorized collection of such information by requiring carriers to be capable of delivering it to law enforcement. J-STD-025-B itself makes the presentation of legal authorization by a law enforcement agency a precondition for a carrier's assistance with LAES. *See* J-STD-025-B § 1.1 (providing that "[a]s a precondition for a TSP's assistance with Lawfully Authorized Electronic Surveillance (LAES), [a law enforcement agency]

incorporated into this more precise location information capability to allow it to be turned "on" or "off" on a per-intercept basis consistent with the authority granted by a given court order.[91, 92] In order to avoid any confusion, DOJ recommends that the toggle

---

must serve a TSP with the necessary legal authorization").

[91] The Commission previously found – in the context of the dialed-digit extraction capability – that a toggle feature was a reasonable and appropriate way to address the issue of the differing types of legal authority for LAES that might be presented to carriers. *See Order on Remand* at 6930-31 ¶ 90. A similar "toggle" feature was adopted by the Commission and is included in J-STD-025-A for dialed-digit extraction. *See* 47 C.F.R. § 64.2203(c)(6) (now contained in 47 C.F.R. § 1.20007(b)(6)); ANSI/J-STD-025-A-2003, § 5.4.8.

[92] The current "location" capability in J-STD-025-B identifies the "cell site" of the subject's mobile handset at the beginning and the end of a communication. The "Message Descriptions" section of J-STD-025-B describes the various event messages that are relayed to law enforcement in connection with call/communication events. The event messages provided to law enforcement consist of a set of parameters, each of which is either "Mandatory," "Conditional," or "Optional." The event message parameter in J-STD-025-B for the delivery of location information is "Conditional," which means that location information is required to be provided only in situations where a condition (as defined in the standard) is met. Thus, J-STD-025-B currently requires the location information message field to be populated only where the delivery of location information is lawfully authorized and such information is reasonably available to the carrier. The standard contains a per-intercept toggle capability requirement to ensure the provision, or non-provision, of location information consistent with the type of lawful authority granted.

DOJ's request is not intended to replace the existing capability in the standard. Rather, it is intended to be a supplemental capability that would enable carriers to *also* provide this type of location information in addition to cell site where authorized and reasonably available. This would be accomplished by adding another "Conditional" location information message field that would be populated with the additional location information (i.e., longitude and latitude) where such information is lawfully authorized and is reasonably available to the carrier. Like the toggle feature already present in the standard to control the delivery or non-delivery of location information, including a per-intercept toggle capability for the additional location information message parameter would ensure the provision or non-provision of longitude and

feature for the more precise location information capability have a default setting of "off." Such a feature would help to better control delivery of the more precise and accurate location information to law enforcement by making the technical capability available and allowing the court to authorize, or not authorize, the delivery of such information on a case-by-case basis. This feature also would protect the privacy of communications not authorized to be intercepted by ensuring that law enforcement receives only the location information to which it is entitled by law.

V. The Security, Performance, and Reliability Capabilities Missing from J-STD-025-B Are Required by CALEA and Critical to Complying with Its Mandate

Security, performance, and reliability capabilities ensure the protection, completeness, and integrity of communications intercepts. Security-related capabilities measure and ensure the overall protection of a given interception. Performance- and reliability-related capabilities address the completeness and quality of the information delivered by a telecommunications carrier. J-STD-025-B lacks capabilities that adequately address these important CALEA-mandated requirements.[93]

---

latitude location information consistent with the type of authority granted. The inclusion of the additional field would enable a carrier to be capable of providing, on a per-intercept basis, whatever location information is lawfully-authorized and reasonably available to the carrier (i.e., no location information at all, cell site location information only, or both cell site and longitude/latitude location information).

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

A. Security, Performance, and Reliability Capabilities Are Required by CALEA Section 103

1. Security

CALEA Section 103 requires telecommunications carriers to be capable of:

> 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.[94]

Generally, this requires carriers to ensure that LAES can be implemented in a way that is transparent to (i.e., not detectable by) the intercept subject or other parties to the communication, and protect the fact of an interception and information related thereto. It also requires carriers to safeguard the assistance capabilities used to facilitate interception/LAES, and protect the packet data streams as they are delivered to law enforcement.[95]

It is also noteworthy that CALEA Section 105 and the Commission's security rules implementing that section require carriers to adopt internal security procedures regarding employee supervision, control, and access to communications content and CII

---

[94] *See id.* § 1002(a)(4).

[95] A capability that ensures the packet data streams are protected as they are delivered to law enforcement is critical because, to the extent that the CII is altered, mutilated, or manipulated, it would be rendered unusable, and law enforcement's access to call identifying information clearly would not be protected as required by Section 103(a).

obtained through LAES.[96] Together, Sections 103 and 105 prohibit improper carrier disclosure of LAES, and require carriers to protect LAES controls/assistance capabilities and the delivery of communications content and CII to law enforcement.[97]

2. Performance and Reliability

CALEA Sections 103(a)(2) and 103(a)(3) requires telecommunications carriers to be capable of:

> [E]xpeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to

---

[96] *See* 47 U.S.C. § 1004; 47 C.F.R. § 1.20003 (formerly 47 C.F.R. § 64.2103); *In the Matter of Communications Assistance for Law Enforcement Act*, Report and Order, 14 FCC Rcd 4151 (1999).

[97] Section 105 and the Commission's security rules implementing that section require carriers to adopt internal system security and integrity policies and procedures for provisioning LAES. But the absence of Section 103 capabilities resident in the equipment that effectuate LAES pursuant to such carrier-adopted policies and procedures would render these policies and procedures useless. J-STD-025-A recognizes this very point in discussing both the Access Function and the Delivery Function, stating that each function typically includes "the ability . . . to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information *consistent with [telecommunications service provider] security policies and practices.*" *See* ANSI/J-STD-025-A-2003, §§ 5.3.1.1 and 5.3.1.2 (emphasis added).

In terms of safeguarding delivery of communications content and call identifying information to law enforcement, ensuring both the security of intercepted information sent from the Intercept Access Point ("IAP") to the Delivery Function ("DF"), and the security of intercepted information from the DF to the Collection Function ("CF") (in the case of carrier-provided buffering), is critical. To minimize the risk that such intercepted information might be improperly accessed or altered by unauthorized parties, the information provided via these delivery links should be kept physically or logically separate from other communications through the use of, for example, secure tunnels/virtual private networks ("VPN") – in order to protect communications content and CII delivered to law enforcement via the Internet.

> access call-identifying information that is reasonably available to the carrier. . . .;[98] and
>
> [D]elivering 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. . . .[99]

CALEA obligates carriers to address quality of service concerns specifically for both the interception and the delivery of CII and communications content packets.[100] By explicitly including in CALEA an obligation as to the delivery of intercepted information to law enforcement, Congress unambiguously expressed its expectation that CALEA compliance would include addressing both the mechanisms for intercepting CII and communications content *and* the method by which such information is transmitted from the carrier to law enforcement.[101]

---

98 47 U.S.C. § 1002(a)(2).

99 *Id.* § 1002(a)(3).

100 *Id.* § 1002(a)(2)-(3).

101 DOJ's request that the security, performance and reliability of the delivery function be addressed should not be interpreted as a request for adoption of a standardized delivery interface. DOJ asks only that the Commission require that a carrier adequately address the security, performance, and reliability capability requirements in Section 103, which would include addressing the delivery of communications content and CII to law enforcement. The Commission has the authority to direct a standards-setting organization to adopt provisions that address the assistance capability requirements of Section 103 (e.g., security, performance, and reliability capabilities) without mandating a particular way of implementing the requirement.

Sections 103(a)(2) and (3) also require reliability with respect to LAES.[102] If a carrier has not implemented measures to assess and confirm the reliability of a packet data intercept and its delivery to law enforcement, the carrier will have no way to assure law enforcement that it has reliably isolated, and reliably provided law enforcement with access to, CII and/or communications content.[103] Without such assurances, law enforcement will not be able to rely on the intercepted information. Moreover, given the delivery requirement in Section 103(a)(3), intercepted information that is not reliably delivered to law enforcement cannot be considered to be truly "delivered."

B. The Commission Should Make Clear That Carriers Are Required to Provide Capabilities That Adequately Address Security, Performance, and Reliability

As discussed above, CALEA Section 103 requires carriers to implement capabilities that address security, performance, and reliability with respect to LAES. Indeed, industry has acknowledged this very requirement by including such capabilities in J-STD-025-B. But while J-STD-025-B includes security, performance, and reliability capability provisions, it merely imports the same limited provisions contained in J-STD-025-A, without taking into account the nature of the services to which J-STD-025-B is intended to apply.

Put simply, J-STD-025-B's security, performance, and reliability provisions are

---

102 47 U.S.C. § 1002(a)(2)-(3).

insufficient because they address the capability requirements from a circuit-mode – rather than a packet-mode – perspective and, therefore, will not ensure the security, performance, and reliability of packet data service intercepts. It is important to differentiate between the circuit-mode services that fall within the scope of J-STD-025-A and the packet-mode services that fall within the scope of J-STD-025-B. For circuit-switched services, the loss of some small amount of an intercepted communication, e.g., a millisecond of communications time, is imperceptible to the user as well as to law enforcement. For packet-based services, however, the loss of one or more packets may render the collection of an entire communication worthless if the packets lost are vital to the reconstruction of the communication. In other words, the nature of packet-mode services raises the bar for both the carrier and law enforcement. Completeness and reliability are critical; thus, reliance on the limited and vague provisions in J-STD-025-A to ensure the security, performance, and reliability of packet-based services is not adequate to meet the requirements and obligations in CALEA Section 103.

To be deemed to have met the requirements of Section 103, a standard must, at a minimum, include security, performance, and reliability capabilities for electronic surveillance that are at least equivalent to those used to determine and ensure the security, performance, and reliability of the carrier's network. Accordingly, DOJ requests that the Commission establish rules requiring carriers to (1) provide capabilities that address security, performance, and reliability with respect to LAES,

---

[103] *Id.* § 1002(a)(1)-(2).

and (2) take into account the adequacy of such security, performance, and reliability capabilities with respect to the service involved.

1. Security

J-STD-025-B is deficient because it fails to include security-related provisions that would, in the context of packet data services, ensure that LAES is undetectable to the subject and protect the fact of and access to an interception and information related thereto. Among the specific security capabilities that should be – but are not – included in J-STD-025-B are:

- The capability to ensure that LAES is unobtrusive – i.e., transparent to and not detectable by the intercept subject, the associates, and other parties to the communication;
- The capability to prevent unauthorized communications and CII from being intercepted;
- The capability to protect the assistance capabilities used to facilitate LAES;
- Capabilities to protect the confidentiality of LAES activities (e.g., preventing knowledge of the fact that LAES is being conducted; technical security mechanisms for activating/deactivating LAES or accessing captured CII or communications content; preventing LAES subjects from being notified of service changes caused by LAES);
- The capability to protect information regarding the government's interception of communications and access to CII; and
- The capability to protect (securely deliver) the packet data streams as they are delivered to law enforcement.[104]

---

[104] CALEA Section 103(a) requires this insofar as it provides that carriers must "facilitat[e] authorized communications interceptions and access to call-identifying information unobtrusively" and "in a manner that protects . . . the government's interception of communications and *access to call-identifying information*." 47 U.S.C.

The security capability requirements in Section 103 can only be satisfied by requiring security-related capabilities, with quantitative measures that assess and ensure the overall security of a given interception. J-STD-025-B's lack of adequate security-related capabilities not only fails to meet Section 103's security requirements, but threatens to compromise law enforcement's investigations. For example, a subject could become aware of an interception or be inadvertently notified of a change in service, or an unauthorized interception of communications content or CII could be conducted.

Thus, a carrier that fails to deploy capabilities that adequately address the security requirements in Section 103 – or relies on a standard that does not adequately address the security requirements in Section 103 in the context of the services to which that standard is intended to apply – cannot be deemed to have complied with its statutory obligations under CALEA. Accordingly, DOJ requests that the Commission require carriers to provide security-related capabilities that address the requirements of Section 103 in the context of the service(s) involved.

2. Performance and Reliability

As discussed above, CALEA Sections 103(a)(2) and (3) require carriers to isolate and deliver intercepted communications content and CII to law enforcement.[105] Complete, accurate, and reliable collection and delivery of the intercepted information

---

§ 1002(a)(4) (emphasis added).

[105] 47 U.S.C. § 1002(a)(2)-(3).

is implicit in this requirement. CALEA requires that carriers isolate and enable the government to intercept "*all* wire and electronic communications carried by the carrier . . . to or from equipment, facilities, or services of a subscriber"[106] and deliver such intercepted communications to the government.[107] As noted previously, this is particularly true in the case of packet data services, where even tiny inaccuracies in delivery can render a communication unusable by law enforcement. These provisions necessarily require that carriers use quantitative performance and reliability measures to assess and confirm the completeness and reliability of both the interception *and* the delivery of the intercepted communications to law enforcement.[108]

Notwithstanding these requirements, J-STD-025-B does not contain any quantitative performance and reliability measures, such as packet loss or bit error rate, which are designed to assess and ensure the completeness and reliability of intercepts. For example, J-STD-025-B fails to include any measures that address packet loss of communications content after an interception (i.e., the loss or omission of packets from the communications stream). Lost or omitted packets present significant technical problems in reassembling packet data communications. Effectively and accurately

---

106 47 U.S.C. § 1002(a)(1) (emphasis added).

107 *Id.* § 1002(a)(3).

108 With respect to delivery, if the completeness and reliability of the intercepted information being delivered to law enforcement cannot be confirmed by the carrier, the carrier cannot be said to have actually "delivered" the intercepted communications content and CII to law enforcement as required by Section 103(a)(3).

reassembling a subject's broadband communication stream into the associated individual applications (e.g., web browsing, e-mail, instant messaging) requires access to the subject's complete packet stream; the loss, omission, or corruption of key packets within the subject's communication stream during transmission from the carrier makes it difficult, if not impossible, for law enforcement to reassemble the associated application-level communications.[109] This loss would severely damage law enforcement's ability to conduct LAES. Without performance and reliability measures in place to help it determine whether or not a packet has been lost, dropped, or corrupted, law enforcement will not be able to ensure that it has received all of the intercepted communications and CII to which it is legally entitled.[110]

---

[109] DOJ is not requesting that carriers be responsible for *any* application level processing, but rather that the delivery solution to law enforcement ensure that packet loss is avoided so that law enforcement can successfully perform such processing.

[110] Two cost-effective performance and reliability methods that would solve this problem are near-real-time delivery of communications content to a law enforcement co-located collection device, or carrier-provided buffering and retrieval of LAES over a secure VPN. DOJ urges the Commission to direct that the performance and reliability deficiencies in the standard be addressed via one of these methods. Mandating that law enforcement agencies procure a dedicated, high-bandwidth facility from the carrier to law enforcement would be neither a cost-effective nor a time-efficient solution to the problem. For example, VPNs can be set up within hours, while dedicated high-bandwidth facilities take a substantial amount of time to install (typically 30 days or more). The timeliness and completeness of delivery of lawfully authorized target communications to law enforcement is not only required by CALEA, but is also critical to law enforcement's ability to accomplish its mission. Delays in the delivery of lawfully authorized target communications to law enforcement could render the communications unusable by law enforcement, and would amount to a waste of time and resources for all concerned. DOJ notes, however, that to the extent a buffering solution is utilized, carriers may need to examine the impact of this solution on the

Quantitative performance and reliability measures such as packet loss and bit error rate are routinely used by carriers to assess and confirm the completeness, quality, and reliability of communications transmitted on and over their networks. Because law enforcement has a similar need to confirm the completeness, quality, and reliability of the information provided to it, the Commission should require carriers to use these measures for purposes of satisfying the requirements of Section 103. Such measures will help to assure law enforcement that the CII and communications content has been collected by the carrier and delivered to law enforcement in a reliable, secure, and error-free manner that protects the integrity of the intercepted communications. Moreover, Sections 103(a)(2) and (3) necessarily require the use of such measures because omissions and errors cannot be identified and addressed without them.

As a general principle, the measures used by a carrier to assess the quality of the transmission of CII and communications content to law enforcement pursuant to CALEA Section 103 should be comparable – if not equivalent to – those it uses to measure the quality of transmissions on/over its own network. The reliability of the LAES intercept should likewise be at least equal to the highest level of reliability for the carrier's underlying service.[111] Satisfaction of the performance and reliability capability requirements in Section 103 can be assured only by requiring carriers to implement

---

timing capability (i.e., delivery of intercepted communications to law enforcement within 8 seconds).

[111] Typically, carriers' service level agreements dictate the level of reliability offered to a customer.

adequate performance and reliability-related capabilities in connection with LAES. Moreover, without such capabilities, law enforcement investigations may be significantly compromised.

Thus, a carrier that fails to provide capabilities that address the performance and reliability requirements in Section 103 – or relies on a standard that does not adequately address the performance and reliability requirements in Section 103 in the context of the services to which that standard is intended to apply – cannot be deemed to have complied with its statutory obligations under CALEA. Accordingly, DOJ requests that the Commission require carriers to provide performance- and reliability-related capabilities that address the requirements of Section 103 in the context of the services involved.

VI. The Commission Should Establish Rules Requiring Carriers to Provide the Additional and Modified Capabilities Identified in This Petition in Order To Meet the Assistance Capability Requirements of CALEA

CALEA Section 107(b) provides that if a standard-setting organization's "requirements or standards are deficient," the Commission "may establish, by rule, technical requirements or standards" that:

> (1) meet the assistance capability requirements of Section 103 by cost-effective methods; (2) protect the privacy and security of communications not authorized to be intercepted; (3) minimize the cost of such compliance on residential ratepayers; (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and (5) provide a reasonable time and conditions for compliance with and the transition to any new standard,

> including defining the obligations of telecommunications carriers under section 103 during any transition period.[112]

The requested capabilities are necessary to meet CALEA's assistance requirements, which are in turn vital to protecting public safety and national security.[113] Accordingly, for the reasons described below, the adoption of Commission rules requiring the additional and modified capabilities described in this Petition is warranted under CALEA Section 107(b).

A. Adopting the Capabilities Identified in this Petition Will Meet the Assistance Capability Requirements of CALEA Section 103 by Cost-Effective Methods

Although CALEA does not define the term "cost effective,"[114] the Commission established in its *Order on Remand* a process by which to evaluate whether a given capability is "cost-effective":

> [W]e first inquire whether we have in the record an alternative means to accomplish each of the punch list capabilities. . . . If we cannot make a cost comparison, we will consider other ways of determining whether a punch list capability is "cost-effective." . . . In general, something is "effective" if it accomplishes a task in an efficient manner.[115]

The Commission further noted in the *Order on Remand* that it would not "adopt or reject a capability solely on the basis of a cost-benefit analysis because Congress already has

---

112 47 U.S.C. § 1006(b).

113 *Id.* § 1002.

114 *Order on Remand* at 6914 ¶ 57.

115 *Id.* at 6914-16 ¶¶ 57-58.

made such a calculation when it determined the assistance capability requirements of CALEA."[116]

No reasonable alternatives for providing these capabilities to law enforcement were presented by the TIA membership during J-STD-025-B's development. But even if alternative proposals are advanced by industry with respect to providing the additional and modified capabilities, the Commission should nonetheless – consistent with its previously established evaluation process – consider simply whether these capabilities provide law enforcement with required CII in an efficient manner.

Commercial "off-the-shelf" hardware and software is already readily available that could be adapted to enable carriers to provide the CII-related capabilities requested in this Petition. In fact, numerous companies (e.g., trusted third party service bureaus, CALEA solution vendors, equipment manufacturers) have emerged over the past several years that specialize in providing telecommunications carriers with CALEA solutions for their packet-mode services. As a result, CALEA solutions often are now much less costly and burdensome to install than in the past. Thus, satisfying the requirements of CALEA by providing the capabilities requested in this Petition can be accomplished efficiently and by cost-effective methods.

---

[116] *Id.* at 6916 ¶ 58. Noting that there are costs associated with CALEA that Congress clearly anticipated carriers would bear, the Commission refused to "reject the punch list capabilities solely because they would be costly to implement. . . ." *Id.* at 6916 ¶ 59.

B. The Capabilities Identified in This Petition Will Help Protect the Privacy and Security of Communications

Each of the requested capabilities will help protect the privacy and security of communications not authorized to be intercepted.

1. Packet Activity Reporting

Packet activity reporting CII enables law enforcement to identify the parties involved in a communication and the types of services used by the subject. In the absence of a packet activity reporting capability, carriers have no means by which to isolate certain CII from other information, including communications content, and deliver only the isolated CII to law enforcement.[117] As a result, law enforcement will have no other practical alternative than to attempt to do the separation itself in order to ensure compliance with court orders and other authorizations. This situation is exactly the kind that CALEA sought to avoid. Thus, as more fully discussed above,[118] requiring a packet activity reporting capability helps protect the privacy and security of communications by harmonizing CALEA's goal of protecting the privacy of communications not authorized to be intercepted with the government's authority to collect CII.[119]

---

117 47 U.S.C. § 1002(a)(1)-(2).

118 *See supra* Section IV.A.

119 *See* 47 U.S.C. §§ 1002(a)(2), (a)(4)(A), 1006(b)(2).

2. Timing Information (Time Stamping)

The Commission already has concluded, without raising any privacy concerns, that a timing information (time stamping) capability is necessary to implement CALEA.[120] Likewise, there are no privacy concerns with requiring a timing information (time stamping) capability for CDMA2000 data services.

3. Location Information

The location information capability also does not impact any legitimate privacy interest because it would not provide any information that law enforcement is not authorized to receive. CALEA directs the Commission to adopt rules that "protect the privacy and security of communications *not authorized to be intercepted* . . . ."[121] DOJ asks the Commission to require that carriers deliver to law enforcement all signaling that reveals mobile handset location information only when (1) law enforcement has obtained the appropriate legal authorization to receive such information, and (2) such information is "reasonably available" to the carrier. DOJ's request satisfies CALEA Section 107(b)(2)'s privacy prong because the requested capability would not allow law enforcement to access any information that it is not lawfully authorized to receive. To the extent the Commission chooses to evaluate the privacy impact of the location

---

120 *See Third R&O* at 16835-36 ¶¶ 95-96.

121 47 U.S.C. § 1006(b)(2) (emphasis added).

capability requested in this Petition,[122] however, the conclusion that the requested capability would not unduly intrude on any privacy interest remains the same.

When it crafted Section 103(a)(2), Congress considered the effect on privacy of enabling law enforcement to access location information. In that Section, Congress specified one situation in which location information *cannot* be provided to law enforcement: when law enforcement has only a pen register or trap and trace order.[123] This is a unique provision in a statute that otherwise does not address legal authority at all. By foreclosing only one means for obtaining access to location information, Congress implicitly expressed an expectation that other legal authorities *could* authorize law enforcement to obtain a subscriber's mobile handset location information. In addition, both the Commission and the D.C. Circuit have confirmed that location information is CII under CALEA.[124]

As discussed above, DOJ's request for access to signaling that reveals mobile handset location information is consistent with CALEA and with the Commission's prior approach to location information capabilities. First, regardless of a requirement to provide law enforcement with more precise location information when it is reasonably available to the carrier, law enforcement still must have appropriate legal authorization

---

122 Should the Commission decide to conduct a privacy analysis of this capability, the Commission should describe the factors it will use in reaching its conclusion.

123 47 U.S.C. § 1002(a)(2)(B).

124 *Third R&O* at 16815 ¶ 44; *United States Telecom. Ass'n*, 227 F.3d at 463-64.

before it may access any such information. Second, law enforcement still will be able to access such mobile handset location information only at the beginning and the end of each communication. The only difference between the capability requested in this Petition and that adopted in the *Third R&O* and currently provided in J-STD-025-B is that the former would provide law enforcement with a *more* accurate and precise version of the location information at the beginning and the end of a communication (i.e., latitude/longitude information, versus a mobile cell site identifier). Accordingly, the distinction is not the identification of the location of a mobile handset *per se*, but the *more accurate and precise* identification of that mobile handset's location.

Wireless subscribers' privacy will be protected even if carriers provide law enforcement with more accurate location-based CII, since a location information capability is already included in J-STD-025-B. But even assuming *arguendo* that the more precise location information capability raises more significant privacy concerns than the existing capability, the inclusion of the requested toggle feature – with a default setting of "off" – will reasonably ensure the privacy of information not authorized to be intercepted by ensuring that carriers provide to law enforcement only the information authorized to be accessed.

4. Security, Performance and Reliability Capabilities

The modified security capabilities that DOJ seeks will "protect the security and privacy of communications not authorized to be intercepted."[125] As described above, the requested capabilities include controls that ensure that LAES is undetectable to the subject, and that protect the fact of, and access to, an interception and information related thereto. Moreover, these capabilities safeguard the equipment and mechanisms used to perform intercepts, and protect the packet data streams as they are delivered to law enforcement.[126] Indeed, the very purpose of such capabilities is to protect the security and privacy of communications not authorized to be intercepted. Accordingly, the security capabilities sought would advance CALEA's goal of protecting the security and privacy of such communications.

C. The Additional and Modified Capabilities Minimize the Cost of Compliance on Residential Ratepayers

The additional and modified capabilities requested by DOJ can be implemented cost-effectively and in a manner that minimizes the costs of compliance on residential ratepayers, as many of the capabilities described already exist in carriers' networks, or

---

125 47 U.S.C. § 1006(b)(2). The modified performance and reliability capabilities sought by DOJ have no impact on the security or privacy of communications *per se*, as they are designed to ensure that the intercepted communications are actually and accurately delivered to law enforcement. To the extent that these performance and reliability capabilities ensure that intercepts are performed in accordance with the legal authorization, then these capabilities also protect the security and privacy of communications from inadvertent or mistaken collection.

126 *See* Section V *supra*.

can be implemented with relatively minimal cost.

Many of the capabilities described in this Petition exist in carriers' networks and have already been paid for by the affected carriers. For example, wireless carriers have paid for the E-911 Phase II location information capability that has been deployed in their networks.[127] Providing this same capability for CALEA purposes should add very little, if any, to carriers' E-911 Phase II development costs, and should therefore minimize the cost of compliance on residential ratepayers. The cost of providing a timing information (time stamping) capability to law enforcement also would be minimal, at most, because the same capability already is present and available in the affected carriers' networks. Similarly, because performance and reliability measures (e.g., packet loss, bit error rate) are currently present in, and routinely used by carriers to assess the completeness, quality, and accuracy of communications transmitted on their networks, there should be little or no additional costs associated with providing these capabilities for purposes of CALEA.

Moreover, the cost of implementing the requested capabilities in a packet-based network is likely to be significantly less than in traditional circuit-switched networks, because large switches need not be replaced and many third party providers offer these

---

[127] Some carriers chose to incur these costs themselves while others included a small monthly customer surcharge passed through on customer bills to recover the costs of such upgrades.

capabilities to industry at competitive prices.[128]

Finally, even assuming the carrier must incur some costs to provide such capabilities, just as with the additional capabilities that were adopted by the Commission in the original J-STD-025 proceeding and later added to the standard, the cost of carrier compliance should have minimal impact on residential ratepayers. As the Commission recognized in the *Order on Remand*:

> [I]t is likely that the cost would be shared by all ratepayers and, therefore, would be significantly diluted on an individual residential ratepayer basis. The fact that costs are spread across such a large base in itself suggests another means by which provision of these capabilities will minimize the effect on residential ratepayers – that the cost of CALEA compliance for any particular ratepayer will be

---

[128] *See In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 15011 n.127 (2005) (*"First R&O"*) (finding that industry solutions appear to be readily available); *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360, 5372 ¶ 26 (2006). Furthermore, many broadband carriers have utilized network monitoring capabilities, such as packet inspection and packet capture (PCAP), to identify unauthorized and inappropriate use of their network (e.g., SPAM; Denial of Service (DoS) attacks, etc.). (See http://www.winpcap.org/ and http://www.tcpdump.org/ for more information on PCAP). Capabilities such as Multiprotocol Label Switching (MPLS) give network operators a great deal of flexibility in implementing Quality of Service (QoS) capabilities and assuring reliable transport of communications within their networks. The wide-scale adoption of Network Time Protocol (NTP) in IP networks provides a means of accurately synchronizing the internal clocks of IP-based network equipment. (For more information, see Network Time Protocol (NTP), IETF RFC 958, Sept. 1985; NTP.ORG, Home of the Network Time Protocol Project, viewable at http://www.ntp.org/). All of these capabilities – which are already implemented in many carrier networks – could be leveraged in order to address the capabilities described in this Petition.

minimal.[129]

Accordingly, DOJ believes the requested capabilities can be provided at a minimal incremental cost to carriers, resulting in little or no cost to residential ratepayers.

D. The Additional and Modified Capabilities Are Consistent With the Commission's Policy of Encouraging the Provision of New Technologies and Services to the Public

The additional and modified capabilities described in this Petition are consistent with CALEA Section 107(b)(4) in that they "encourage the provision of new technologies and services to the public."[130] DOJ does not seek to delay or stop the deployment of any service to which J-STD-025-B would apply. DOJ does not believe that requiring the requested capabilities would have that effect. Nor was any evidence presented during the J-STD-025-B development process that requiring the additional and modified capabilities discussed in this Petition would discourage the provision of packet- mode (data) services. In fact, over the past several years, the FBI has worked actively with vendors and their carrier clients in an effort to facilitate the development of complete packet-based CALEA solutions for the marketplace that could be deployed simultaneously with the launch of CDMA2000 technologies and services. Indeed, based on these efforts, DOJ understands that several vendors have developed new CALEA solutions intended for CDMA2000 packet data services that can be deployed in a

---

[129] *Order on Remand* at 6919-20 ¶ 65.

carrier's network when service is launched.

E. Twelve Months Is a Reasonable Transition Period Within Which to Incorporate the Capabilities Described in this Petition

Consistent with its comments on the *CALEA NPRM*,[131] DOJ believes that twelve months after the effective date of the Commission's decision in this proceeding is an appropriate compliance period.[132,133] The carriers that will be affected by the Commission's decision in the instant deficiency petition proceeding are already covered by CALEA and have been aware of CALEA's packet data compliance obligations since August 1999.[134] Moreover, TIA and industry have been aware of the additional and

---

130 47 U.S.C. § 1006(b)(4).

131 *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd 15676 (2004) ("*CALEA NPRM*").

132 DOJ Comments on *CALEA NPRM*, at 57 (filed Nov. 8, 2004); DOJ Reply Comments on *CALEA NPRM*, at 46-47 (filed Dec. 21, 2004). Although the Commission ultimately concluded in the CALEA rulemaking proceeding that eighteen months was a reasonable time period for CALEA compliance by newly covered entities, *see First R&O* at 14990 ¶ 3, that decision should not be controlling here, because the requirement in the *First R&O* is applicable to entities that are *newly covered* by CALEA. A compliance time period adopted with respect to the application of CALEA to a given group of carriers or other entities pursuant to CALEA Section 102 should not apply to a deficiency petition filed under Section 107(b).

133 DOJ notes, however, that there are limited circumstances in which a twelve-month compliance period may not be appropriate. For example, where air-to-ground wireless or broadband Internet access services have been deployed on commercial aircraft, a twelve-month gap in compliance would be excessive given the risk that terrorists or other criminals might use such services to communicate before or after taking control of an aircraft.

134 *Third R&O* at 16795 ¶ 1.

modified capabilities requested in this Petition since at least 2001, when the FBI raised them at the outset of the J-STD-025-B standard development process. Given the facts and circumstances involved, a twelve-month compliance schedule is both reasonable and appropriate.[135] In addition, based upon DOJ's significant prior experience in working with wireless carriers deploying packet data CALEA solutions, twelve months has proven to be an adequate amount of time for carriers and their vendors to deploy such packet data solutions.

In the *Order on Remand*, the Commission clearly recognized that separate and unique CALEA compliance periods under CALEA Section 107(b)(5) are appropriate.[136] There, the Commission required – based on the particular facts, circumstances, and record in that proceeding – that carriers deploy the additional punch list capabilities for

---

[135] The text in Section 107(b)(5) clearly shows that Congress expected the Commission to adopt a unique time frame for carrier compliance as part of the deficiency petition process on the basis of the particular facts and circumstances presented. *See* 47 U.S.C. § 1006(b)(5) (directing the Commission to provide a reasonable time and conditions for compliance). Otherwise, this language would have been superfluous. *See Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979) ("In construing a statute we are obliged to give effect, if possible, to every word Congress used"). Congress included Section 107(b)(5) in CALEA because it recognized that the Commission's evaluation of deficiency petitions challenging CALEA standards would differ based on the facts and circumstances involved. Because the carriers that will be affected by the Commission's decision in the instant deficiency petition proceeding are already covered by CALEA and have been aware of CALEA's packet data compliance obligations for quite some time, a shorter compliance period that takes these facts into account is reasonable and appropriate.

[136] *Order on Remand* at 6941-42 ¶ 127.

J-STD-025 within just two months.[137] The Commission's decision to adopt a relatively short compliance deadline was based on a number of factors, including (1) carriers' ability to typically put into effect any required changes to their network within six months of a Commission decision; (2) that much of the software required to implement the punch list items has already been developed, thereby significantly speeding implementation; and (3) carriers' significantly greater experience in meeting CALEA's capabilities than in the earlier stages of CALEA's implementation.[138] The Commission concluded that these factors – when taken together – made a shorter implementation timetable reasonable.[139]

The Commission's approach in the *Order on Remand* clearly recognized that the compliance period for deploying capabilities resulting from a deficiency proceeding can and should differ, based on the facts, circumstances, and record in a particular deficiency proceeding. There appears to be no reason to depart from that approach here. The majority of the additional and modified capabilities will not require a significant amount of effort to implement. The timing information (time stamping) capability is already included in J-STD-025-A and provided by carriers. Therefore, incorporating this capability into J-STD-025-B with respect to packet data services will require only minimal effort. Implementing the more precise location information

---

137 *Id.*

138 *Id.*

capability into J-STD-025-B should also not require a significant amount of effort, because the information already exists in wireless carriers' networks as a result of the Commission's E-911 Phase II requirement and because the proposed capability already takes account that such information be "reasonably available" to the carrier. In addition, although developing more robust capabilities to address security, performance, and reliability in the context of packet data services will require a certain amount of effort, that effort should be minimal. A twelve-month compliance period is warranted based on the facts and circumstances concerning J-STD-025-B and, therefore, the Commission should require telecommunications carriers to begin providing the additional and modified capabilities to law enforcement within twelve months after the effective date of the Commission's decision in this proceeding.

VII. Conclusion

For all of the foregoing reasons, DOJ respectfully requests that the Commission find that J-STD-025-B is deficient with respect to meeting the assistance capability requirements of CALEA because it does not provide the following required capabilities: (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. DOJ further requests that the Commission establish rules requiring telecommunications carriers to provide the above-described additional and modified capabilities. Finally, DOJ requests that the Commission require telecommunications carriers to provide the

---

139 *Id.*

additional and modified capabilities within twelve months after the effective date of the Commission's decision in this proceeding.

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

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

Dated: May 15, 2007

I, John R. Delmore, hereby certify that on this 15th day of May, 2007, I caused a true and correct copy of the **"Petition for Expedited Rulemaking,"** pertaining to "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" to be served upon the following parties as indicated:

Marlene H. Dortch, Secretary **(via hand-delivery)**
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Derek Poarch, Chief **(via e-mail)**
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dana Shaffer, Deputy Bureau Chief **(via e-mail)**
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Tom Beers, Deputy Chief **(via e-mail)**
Policy Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

John Delmore
John R. Delmore