

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

FILED/ACCEPTED

MAY 15 2007

Federal Communications Commission  
Office of the Secretary

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

TABLE OF CONTENTS .....	i
SUMMARY .....	iii
I. Introduction .....	1
II. History of the Development of J-STD-025-B .....	6
III. Overview of the Capabilities Not Provided for in J-STD-025-B.....	8
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.....	10
A. Packet Activity Reporting.....	12
1. Packet Activity Reporting Is a Required CII Capability .....	12
2. The Commission Should Require Carriers to Provide a Packet Activity Reporting Capability .....	16
B. Timing Information (Time Stamping).....	19
1. Timing Information Is a Required CII Capability .....	19
2. The Commission Should Reaffirm That Timing Information (Time Stamping) Is a Required Capability .....	21
C. Capability to Provide All Reasonably Available Location Information for a Mobile Handset at the Beginning and the End of a Communication .....	26
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 .....	26
2. All Reasonably Available Signaling Information That Reveals the Location of a Mobile Handset Should Be Provided to Law Enforcement Pursuant to Lawful Authorization .....	28
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 ..	30
V. The Security, Performance, and Reliability Capabilities Missing from J-STD-025-B Are Required by CALEA and Critical to Complying with Its Mandate.....	40
A. Security, Performance, and Reliability Capabilities Are Required by CALEA Section 103.....	41
1. Security .....	41
2. Performance and Reliability .....	42
B. The Commission Should Make Clear That Carriers Are Required to Provide Capabilities That Adequately Address Security, Performance, and Reliability.....	44

1. Security .....	46
2. Performance and Reliability .....	47
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.....	51
A. Adopting the Capabilities Identified in this Petition Will Meet the Assistance Capability Requirements of CALEA Section 103 by Cost- Effective Methods .....	52
B. The Capabilities Identified in This Petition Will Help Protect the Privacy and Security of Communications .....	54
1. Packet Activity Reporting.....	54
2. Timing Information (Time Stamping).....	55
3. Location Information.....	55
4. Security, Performance and Reliability Capabilities.....	58
C. The Additional and Modified Capabilities Minimize the Cost of Compliance on Residential Ratepayers .....	58
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 .....	61
E. Twelve Months Is a Reasonable Transition Period Within Which to Incorporate the Capabilities Described in this Petition.....	62
VII. Conclusion .....	65

## 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”),<sup>1</sup> hereby petitions the Federal Communications Commission (“Commission”) to initiate an expedited rulemaking proceeding regarding American National Standard Institute (“ANSI”)<sup>2</sup>

---

<sup>1</sup> 47 U.S.C. § 1006(b).

<sup>2</sup> 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](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<sup>3</sup> packet data wireless services (“J-STD-025-B”).<sup>4</sup>

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.<sup>5</sup> Specifically, Section 103 requires a telecommunications carrier to ensure that its equipment, facilities, or services are

---

<sup>3</sup> “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.*

<sup>4</sup> 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.

<sup>5</sup> 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.<sup>6</sup>

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<sup>7</sup> 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

---

<sup>6</sup> 47 U.S.C. § 1002(a).

<sup>7</sup> 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<sup>8</sup> 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).<sup>9</sup> 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;<sup>10</sup>

---

<sup>8</sup> 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.

<sup>9</sup> 47 U.S.C. § 1006(b).

<sup>10</sup> 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 . . . ." <sup>11</sup> 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. <sup>12</sup>

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-

---

<sup>11</sup> *Id.* § 1006(a)(2).

<sup>12</sup> 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,<sup>13</sup> which contains CALEA capabilities for circuit-switched voice wireline and wireless communications services.<sup>14</sup> 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)<sup>15</sup> were eliminated from J-STD-025-B.

In accordance with its consultative role,<sup>16</sup> 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

---

<sup>13</sup> 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.

<sup>14</sup> 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.

<sup>15</sup> *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).

<sup>16</sup> *See* 47 U.S.C. § 1006(a)(1).

by Section 103 but were missing from the standard.<sup>17</sup> 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.<sup>18</sup>

### 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);

---

<sup>17</sup> 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).

<sup>18</sup> 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.<sup>19</sup> 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

---

<sup>19</sup> 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.<sup>20</sup> 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

---

<sup>20</sup> 47 U.S.C. §§ 1002(a)(2)-(4), 1004.

the carrier.”<sup>21</sup> 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.”<sup>22</sup> 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.<sup>23</sup> 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).<sup>24</sup>

---

<sup>21</sup> See *id.* § 1002(a)(1)-(2).

<sup>22</sup> *Id.* § 1001(2).

<sup>23</sup> *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).

<sup>24</sup> *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.”<sup>25</sup> 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

---

<sup>25</sup> *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.<sup>26</sup> 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.<sup>27</sup>

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

---

<sup>26</sup> 47 U.S.C. § 1001(2).

<sup>27</sup> 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.<sup>28</sup> 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.<sup>29</sup> 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.<sup>30</sup> 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

---

<sup>28</sup> 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.

<sup>29</sup> *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.

<sup>30</sup> 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,<sup>31</sup> and often identifies the application type understood to be using that port.<sup>32</sup> A contact or “well-known” port can also be used to provide services to unknown callers.<sup>33</sup> 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.<sup>34</sup> 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.<sup>35</sup> Port numbers also help refine and narrow endpoints of particular types of communications, assisting law enforcement in focusing on specific

---

<sup>31</sup> See *Definition of Port Number*, available at [http://compnetworking.about.com/od/basicnetworkingconcepts/1/bldef\\_port.htm](http://compnetworking.about.com/od/basicnetworkingconcepts/1/bldef_port.htm) (last viewed May 14, 2007).

<sup>32</sup> 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.

<sup>33</sup> See IETF RFC 1700, Reynolds and Postel, at 15 (Oct. 1994).

<sup>34</sup> 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).

<sup>35</sup> 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.”<sup>36</sup>

Third, transport layer protocol ensures reliable data delivery and end-to-end data integrity by providing connection-oriented services between two end systems.<sup>37</sup> 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.<sup>38</sup>

## **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.<sup>39</sup> 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

---

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

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> 47 U.S.C. § 1002(a)(2)-(3).

(3).<sup>40</sup>

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.<sup>41</sup> 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.<sup>42</sup> This would be akin to having a pen register/trap and trace (“PR/TT”) in place that is unable either to

---

<sup>40</sup> *Id.* § 1002(a)(1)-(3).

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

<sup>42</sup> 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.<sup>43</sup> 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.

<sup>43</sup> 47 U.S.C. § 1002(a)(1)-(2).

privacy and security of communications not authorized to be intercepted<sup>44</sup> with the government's authority to collect CII.<sup>45</sup>

## **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).<sup>46</sup> Specifically, the Commission stated:

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

---

<sup>44</sup> See *id.* §§ 1002(a)(4)(A), 1006(b)(2).

<sup>45</sup> 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.

<sup>46</sup> *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.”<sup>47</sup>

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.<sup>48</sup> The timing information requirement – including the specific parameters for delivery of the required timing information – was codified in the Commission’s rules<sup>49</sup> 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

---

<sup>47</sup> *Id.*

<sup>48</sup> *Id.* at 16835 ¶ 96.

<sup>49</sup> 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.<sup>50</sup> 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*."<sup>51</sup> Notwithstanding that the Commission's *Third R&O* clearly addressed both circuit-mode and packet-mode communications,<sup>52</sup> 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-

---

<sup>50</sup> See ANSI/J-STD-025-A-2003, § 4.7.

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

<sup>52</sup> *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.<sup>53</sup> 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,<sup>54</sup> the Commission set a September 2001 deadline for packet-mode compliance,<sup>55</sup> 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*

---

<sup>53</sup> *Id.*

<sup>54</sup> *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.

<sup>55</sup> *Id.* at 16819 ¶ 55.

*particular amendments to J-STD-025.*"<sup>56</sup> 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.<sup>57</sup>

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]."<sup>58</sup>

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.<sup>59</sup> The less accurate the time stamp, the greater the possibility that multiple events occurring in the

---

<sup>56</sup> *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*.

<sup>57</sup> *Third R&O* at 16795 ¶ 1, 16819-20 ¶¶ 55-56.

<sup>58</sup> 47 C.F.R. § 1.20007(b)(5).

<sup>59</sup> *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,<sup>60</sup> and in light of the Commission's conclusion in the *Third R&O* that timing information is CII under Section 102(2),<sup>61</sup> 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

---

<sup>60</sup> *Id.* at 16795 ¶ 1.

<sup>61</sup> *Id.* at 16835 ¶ 95.

parameters for delivery of the required timing information.<sup>62, 63</sup>

**C. Capability to Provide All Reasonably Available Location Information for a Mobile Handset at the Beginning and the End of a Communication<sup>64</sup>**

**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

---

<sup>62</sup> 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).

<sup>63</sup> 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.

<sup>64</sup> 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.<sup>65</sup> 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.<sup>66</sup> As both the Commission and

---

<sup>65</sup> See 47 U.S.C. §§ 1002(a)(1) and (2).

<sup>66</sup> 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.<sup>67</sup> 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.<sup>68</sup>

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).

<sup>67</sup> *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”).

<sup>68</sup> *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,<sup>69</sup> 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.<sup>70</sup> 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.”<sup>71</sup> 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.”<sup>72</sup> In upholding the Commission’s conclusions concerning location information,<sup>73</sup> 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

---

<sup>69</sup> See 47 U.S.C. § 1002(a)(2).

<sup>70</sup> See *id.* § 1002(a)(2)(B).

<sup>71</sup> *Third R&O* at 16815 ¶ 44.

<sup>72</sup> *Third R&O* at 16815 n.95.

<sup>73</sup> See *United States Telecom. Ass’n*, 227 F.3d at 463.

statute to be given effect.”<sup>74</sup> 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

---

<sup>74</sup> *Id.*

legally authorized to receive.<sup>75</sup> 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.<sup>76</sup> At that time, the Commission declined to require carriers to

---

<sup>75</sup> 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.

<sup>76</sup> 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.”<sup>77</sup> 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.”<sup>78</sup>

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).

<sup>77</sup> See *Third R&O* at 16816 ¶ 46. As discussed below, this has not generally been the case.

<sup>78</sup> *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.<sup>79</sup> 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.<sup>80</sup> Carriers also have introduced new and improved wireless location service offerings to their subscribers.<sup>81</sup> 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.<sup>82</sup> Thus, as a result of the

---

<sup>79</sup> 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).

<sup>80</sup> 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.

<sup>81</sup> See, e.g., [http://www.nextel.com/en/services/gps/mobile\\_locator.shtml](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.

<sup>82</sup> 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.<sup>83</sup>

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"<sup>84</sup> has not been borne out by subsequent experience. In

---

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

<sup>83</sup> 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.

<sup>84</sup> 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.<sup>85</sup> Even worse, in some cases, the cell site location information that carriers provide to law enforcement is

---

<sup>85</sup> 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.<sup>86</sup> 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.

---

<sup>86</sup> 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.<sup>87</sup>

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.<sup>88</sup> 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.<sup>89</sup> 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.

<sup>87</sup> 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).

<sup>88</sup> *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.*

<sup>89</sup> *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.<sup>90</sup> 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

---

<sup>90</sup> 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.<sup>91, 92</sup> In order to avoid any confusion, DOJ recommends that the toggle

---

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

<sup>91</sup> 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.

<sup>92</sup> 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.<sup>93</sup>

---

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).

<sup>93</sup> 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.<sup>94</sup>

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.<sup>95</sup>

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

---

<sup>94</sup> See *id.* § 1002(a)(4).

<sup>95</sup> 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.<sup>96</sup> 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.<sup>97</sup>

## 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

---

<sup>96</sup> 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).

<sup>97</sup> 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. . . .<sup>98</sup> 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. . . .<sup>99</sup>

CALEA obligates carriers to address quality of service concerns specifically for both the interception and the delivery of CII and communications content packets.<sup>100</sup> 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.<sup>101</sup>

---

<sup>98</sup> 47 U.S.C. § 1002(a)(2).

<sup>99</sup> *Id.* § 1002(a)(3).

<sup>100</sup> *Id.* § 1002(a)(2)-(3).

<sup>101</sup> 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.<sup>102</sup> 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.<sup>103</sup> 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

---

<sup>102</sup> 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,

---

<sup>103</sup> *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.<sup>104</sup>

---

<sup>104</sup> 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.<sup>105</sup> Complete, accurate, and reliable collection and delivery of the intercepted information

---

§ 1002(a)(4) (emphasis added).

<sup>105</sup> 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”<sup>106</sup> and deliver such intercepted communications to the government.<sup>107</sup> 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.<sup>108</sup>

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

---

<sup>106</sup> 47 U.S.C. § 1002(a)(1) (emphasis added).

<sup>107</sup> *Id.* § 1002(a)(3).

<sup>108</sup> 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.<sup>109</sup> 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.<sup>110</sup>

---

<sup>109</sup> 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.

<sup>110</sup> 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.<sup>111</sup> 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).

---

<sup>111</sup> 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.<sup>112</sup>

The requested capabilities are necessary to meet CALEA's assistance requirements, which are in turn vital to protecting public safety and national security.<sup>113</sup> 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,"<sup>114</sup> 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.<sup>115</sup>

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

---

<sup>112</sup> 47 U.S.C. § 1006(b).

<sup>113</sup> *Id.* § 1002.

<sup>114</sup> *Order on Remand* at 6914 ¶ 57.

<sup>115</sup> *Id.* at 6914-16 ¶¶ 57-58.

made such a calculation when it determined the assistance capability requirements of CALEA.”<sup>116</sup>

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.

---

<sup>116</sup> *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.<sup>117</sup> 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,<sup>118</sup> 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.<sup>119</sup>

---

<sup>117</sup> 47 U.S.C. § 1002(a)(1)-(2).

<sup>118</sup> *See supra* Section IV.A.

<sup>119</sup> *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.<sup>120</sup> 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 . . .*”<sup>121</sup> 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

---

<sup>120</sup> See *Third R&O* at 16835-36 ¶¶ 95-96.

<sup>121</sup> 47 U.S.C. § 1006(b)(2) (emphasis added).

capability requested in this Petition,<sup>122</sup> 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.<sup>123</sup> 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.<sup>124</sup>

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

---

<sup>122</sup> 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.

<sup>123</sup> 47 U.S.C. § 1002(a)(2)(B).

<sup>124</sup> *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.”<sup>125</sup> 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.<sup>126</sup> 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

---

<sup>125</sup> 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.

<sup>126</sup> 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.<sup>127</sup> 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

---

<sup>127</sup> 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.<sup>128</sup>

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

---

<sup>128</sup> 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.<sup>129</sup>

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."<sup>130</sup> 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

---

<sup>129</sup> *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*,<sup>131</sup> DOJ believes that twelve months after the effective date of the Commission's decision in this proceeding is an appropriate compliance period.<sup>132,133</sup> 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.<sup>134</sup> Moreover, TIA and industry have been aware of the additional and

---

<sup>130</sup> 47 U.S.C. § 1006(b)(4).

<sup>131</sup> *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*").

<sup>132</sup> 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).

<sup>133</sup> 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.

<sup>134</sup> *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.<sup>135</sup> 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.<sup>136</sup> There, the Commission required – based on the particular facts, circumstances, and record in that proceeding – that carriers deploy the additional punch list capabilities for

---

<sup>135</sup> 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.

<sup>136</sup> *Order on Remand* at 6941-42 ¶ 127.

J-STD-025 within just two months.<sup>137</sup> 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.<sup>138</sup> The Commission concluded that these factors – when taken together – made a shorter implementation timetable reasonable.<sup>139</sup>

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

---

<sup>137</sup> *Id.*

<sup>138</sup> *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

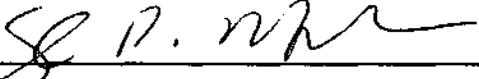
---

<sup>139</sup> *Id.*

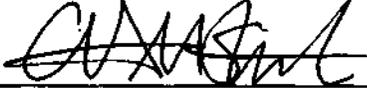
additional and modified capabilities within twelve months after the effective date of the Commission's decision in this proceeding.

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

## **APPENDIX A**

1 TIA TR-45 Mobile and Personal Communications Systems Standards  
 2 TR-45 Lawfully Authorized Electronic Surveillance Ad Hoc Group

3  
 4 **TITLE:** Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities  
 5 for packet-based communications pursuant to the Communications Assistance for Law Enforcement  
 6 Act (CALEA).

7  
 8 **DATE:** January 21, 2002

9  
 10 **SOURCES:**



**CALEA Implementation Section**

Lou Degni  
 14800 Conference Center Drive, Suite 300  
 Chantilly, VA 20151-3810  
 Tel: (703) 814-4729  
 Fax: (703) 814-4720  
 e-mail: ldegni1@askcalea.net

11  
 12 **DISTRIBUTION:** TR45 LAES Ad Hoc Group

13  
 14 **ABSTRACT:** This contribution proposes content for a Stage 1 description of capabilities needed  
 15 by Law Enforcement Agencies for the surveillance of packet-based communications, pursuant to the  
 16 Communications Assistance for Law Enforcement Act (CALEA). This material should provide a  
 17 framework for refining the packet-based communications requirements published in J-STD-025,  
 18 Lawfully Authorized Electronic Surveillance.

19  
 20  
 21 The contributor grants a free, irrevocable license to the Telecommunications Industry Association (TIA) to incorporate text or other  
 22 copyrightable material contained in this contribution and any modifications thereof in the creation of a TIA Publication; to copyright and  
 23 sell in TIA's name any TIA Publication even though it may include all or portions of this contribution; and at TIA's sole discretion to permit  
 24 others to reproduce in whole or in part such contribution or the resulting TIA Publication. This contributor will also be willing to grant  
 25 licenses under such copyrights to third parties on reasonable, non-discriminatory terms and conditions for purpose of practicing a TIA  
 26 Publication which incorporates this contribution.

27  
 28 This document has been prepared by the contributors to assist the TIA Engineering Committee. It is proposed to the Committee as a basis  
 29 for discussion and is not to be construed as a binding proposal on the contributors. The contributor specifically reserves the right to amend  
 30 or modify the material contained herein and nothing herein shall be construed as conferring or offering licenses or rights with respect to any  
 31 intellectual property of the contributors other than provided in the copyright statement above.

32  
 33 The company represented by this individual may have patents or published pending patent applications, the use of which may be essential  
 34 to the practice of all or part of this contribution incorporated in a TIA Publication and the company represented by this individual is willing  
 35 to grant a license to applicants for such intellectual property contained in this contribution in a manner consistent with 2a) or 2b) of Annex  
 36 H of the TIA Engineering Manual.

## Table of Contents

1		
2		
3	<b>1. Introduction.....</b>	<b>4</b>
4	1.1. Background and Context .....	4
5	1.2. Purpose and Scope of Contribution .....	5
6	1.3. Organization .....	5
7	1.4. Notation .....	5
8	<b>2. Definitions.....</b>	<b>5</b>
9	<b>3. User Perspective of Law Enforcement Agency Needs (Stage 1).....</b>	<b>8</b>
10	3.1. Communications Access.....	8
11	3.1.1. Separate Access to Communication-Identifying Information and Communication	
12	Content .....	8
13	3.1.2. Access to Communication-Identifying Information .....	9
14	3.1.2.1. Subscriber Information .....	10
15	3.1.2.2. Network Protocol Identifiers and Service Access Ports .....	10
16	3.1.2.3. Signaling and Control Information .....	10
17	3.1.2.4. Communication Attempt Alerts.....	11
18	3.1.3. Access to Communication Content .....	12
19	3.1.4. Access Requirements for Specialized Service Capabilities .....	12
20	3.1.4.1. Forwarding, Redirected Communications, and Mobility .....	13
21	3.1.4.2. Multiple Recipients.....	13
22	3.1.5. Separation of Subscriber Physical Interface from the TC .....	13
23	3.1.6. Real-Time, Full-Time Access to Communications .....	14
24	3.1.7. Subject Verification and Subscriber Information.....	15
25	3.1.7.1. Association of Communications With Intercept Subject .....	15
26	3.1.7.2. Service Profile Information .....	16
27	3.2. Delivery of Intercepted Communications.....	16
28	3.2.1. Transmission.....	16
29	3.2.2. Correlation of Communication Content with Communication-Identifying Information	
30	.....	17
31	3.2.3. Non-Alteration of Transmitted Content .....	17
32	3.2.4. Content Decoding, Decompression, and Decryption .....	17
33	3.2.5. Use of Standard, Generally Available Delivery Interface .....	18
34	3.2.6. Congruence With Existing Delivery Interfaces.....	18
35	3.2.7. Consolidated Delivery Interface and Transmission Facilities.....	19
36	3.3. Performance and Quality .....	19
37	3.3.1. Reliability .....	19
38	3.3.1.1. Availability .....	19
39	3.3.1.2. Fault Management .....	19
40	3.3.2. Quality of Service .....	20
41	3.3.3. Timing Requirements .....	20
42	3.3.3.1. Time Stamp Accuracy .....	20
43	3.3.3.2. Event Timing .....	20
44	3.4. Security and Integrity .....	21
45	3.4.1. Transparency of Interceptions .....	21
46	3.4.2. Security of Delivered Surveillance.....	21
47	3.4.2.1. Separation of Surveillance Interfaces from Subscriber Traffic.....	21
48	3.4.2.2. Encryption of Delivered Communication-Identifying Information and	
49	Communication Content .....	21
50	3.4.3. Procedural Safeguards .....	22

1     3.5. Capacity and Transmission Bandwidth ..... 22  
2       3.5.1. Simultaneous Interceptions..... 22  
3       3.5.2. Transmission Bandwidth ..... 23  
4     **4. Recommendation ..... 23**  
5  
6

# 1. Introduction

## 1.1. Background and Context

Lawfully Authorized Electronic Surveillance (LAES) is a critically important investigative tool whereby law enforcement agencies are permitted to intercept communications and/or acquire “communication-identifying information<sup>1</sup>” of monitored subjects. Many serious criminal investigations would be thwarted without the availability of LAES as an investigative technique.

The legal authority for LAES is found in various federal statutes, including but not limited to the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3121 et seq., which governs the collection of called and calling party information through pen registers and trap and trace devices, and the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510, et seq., which governs interceptions of communications content and is commonly referred to as either “Title III” or the “Wiretap Act.” The assistance of Telecommunications Carriers (TCs)<sup>2</sup> in supporting LAES has long been authorized and required pursuant to these federal statutes. In addition, TCs are required to design their systems so as to ensure that they are capable of enabling the government to conduct LAES, pursuant to the 1994 Communications Assistance for Law Enforcement Act (CALEA).<sup>3</sup> CALEA clarifies the extent to which a TC must provide capabilities to assist law enforcement in conducting LAES.

The current industry standard for the support of LAES is specified in TIA/EIA J-STD-025, *Lawfully Authorized Electronic Surveillance*. Although the focus of the J-STD-025 specification is the surveillance of predominantly circuit-mode communications (i.e., voice and data calls using circuit-switched transmission paths dedicated to each call), the specification includes requirements for the interception of packet-based communications. The Federal Communications Commission (FCC) issued a Third Report and Order upholding the packet-based portions of the J-STD-025 specification and requested further study of packet-based communications by the telecommunications industry.

The FCC held in the order released on September 21, 2001 that wireline, cellular, and broadband PCS carriers must implement a packet-based communications surveillance capability by November 19, 2001.

The advent and advances in the use of packet-based switching and transport technologies for the conveyance of communications has challenged the ability of service providers to support LAES functionality. Increasingly, many new packet-based communications services and architectures have been developed which impede or even preclude the use of LAES. Such packet-based communications services may include, but are not necessarily limited to Public IP Network Access and Transport services, Carrier-Grade Voice-Over-Packet (CGVoP) services, Voice over Packet

---

<sup>1</sup> The term “communication-identifying information” is defined in this document as dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by the subscriber by means of any equipment, facility, or service of a TC. The term is intended to be understood as covering the same information described in the Communications Assistance for Law Enforcement Act, 47 U.S.C. 1001(2) as “call identifying information.”

<sup>2</sup> The terms Telecommunications Carriers (TCs) and carriers are used synonymously and interchangeably in this contribution.

<sup>3</sup> See generally 47 U.S.C. §1001 to §1010; CALEA applies to telecommunications carriers but not to information services. See 47 U.S.C. §§1002(b)(2)(A), 1001(6).

1 Internet Gateway (VPIGW) services, and Wireless IP services. These packet-based communications  
2 services can be provided via either landline (e.g., dial-up analog, Digital Subscriber Line (xDSL), or  
3 cable modem) or wireless access technologies.

4  
5 The J-STD-025 specification addresses LAES for packet-based communications only at a high-level  
6 and does so primarily by providing for the delivery of the entire packet stream associated with an  
7 intercept subject. In particular, the packet-based communications surveillance capabilities in the J-  
8 STD-025 specification do not explicitly identify the communication-identifying information-aspects  
9 of the packet-mode surveillance solution, nor does it address aspects of packet-based  
10 communications content delivery, which differ from the current circuit-mode content delivery  
11 capabilities. In order to guide TCs in further revising LAES solutions for the surveillance of packet-  
12 based communications, extensions to the J-STD-025 specification are needed. The first stage in  
13 defining such extensions is the definition of end-user (i.e., law enforcement) needs for LAES  
14 capabilities in the TC networks that support packet-based communications services.

## 16 **1.2. Purpose and Scope of Contribution**

17  
18 The purpose of this contribution is to define the capabilities needed, from a Law Enforcement  
19 Agency (LEA) perspective, to support LAES of packet-based communications and the interface  
20 between TCs and the surveillance collection systems of LEAs. Specifically, it provides a “Stage 1”  
21 user-view description of the general capabilities, features, and information needed by law  
22 enforcement for LAES of packet-based communications.

## 24 **1.3. Organization**

25  
26 The remainder of this contribution is organized as follows:

- 28 • Section 2 summarizes key terms and acronyms used in this contribution, and where necessary,  
29 expands the definitions contained in J-STD-025 for the circuit-mode environment to  
30 accommodate the packet-mode environment as well.
- 32 • Section 3 describes the approach law enforcement has taken towards LAES of packet-based  
33 communications.
- 35 • Section 4 defines the fundamental needs of law enforcement for LAES in a packet-mode  
36 environment.
- 38 • Section 5 proposes how this Stage 1 description would be incorporated into J-STD-025.

## 40 **1.4. Notation**

41  
42 In this document, Law Enforcement needs are identified in terms of essential capabilities, tagged  
43 with the notation (EC), and sequentially numbered.

## 45 **2. Definitions**

1 **Associate (expanded J-STD-025 definition<sup>4</sup>)**

2  
3 A telecommunication user whose equipment, facilities, or services are used to communicate or  
4 attempt to communicate with a subject.

5  
6 **Intercept Subject or Subject (expanded J-STD-025 definition<sup>5</sup>)**

7  
8 A telecommunication service subscriber whose incoming, outgoing, and redirected communications,  
9 call- or communication-identifying information, or both, have been authorized by a court to be  
10 intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to  
11 access the particular equipment, facility, or communication service (e.g., network address, terminal  
12 identity, subscription identity).

13  
14 **Communication (same as J-STD-025 definition)**

15  
16 Communications encompasses the term “electronic communications,” as defined in 18, U.S.C.  
17 2510(12), any transfer of messages, signals, writing, images, sounds, data, or intelligence of any  
18 nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-  
19 optical system, etc. As used herein, the term also includes the term “wire communications” as  
20 defined in 18, U.S.C. 2510(1).

21  
22 **Communication-Identifying Information (same as J-STD-025 definition as Call-Identifying**  
23 **Information)**

24  
25 Communication-identifying information, as used in this document, is synonymous with call-  
26 identifying information. As defined in CALEA, the “dialing or signaling information that identifies  
27 the origin, direction, destination, or termination of each communication generated or received by a  
28 subscriber by means of any equipment, facility, or service of a TC. (47 U.S.C. Section 1001(2).)”<sup>6</sup>

29  
30 **Communications Content (correction of J-STD-025 definition for Content)**

31  
32 Defined in 18 U.S.C. 2510 (8) to be “when used with respect to any wire, oral or electronic  
33 communications, includes any information concerning the substance, purport, or meaning of that  
34 communication.”

35  
36 **Communications Session (or Session) (new definition)**

37  
38 The duration between establishment and release of the capability for the transmission of  
39 communication between an intercept subject and the service provider's network, during which  
40 communication may occur between the subject and one or more associates.

41  
42 **Communication attempt (new definition)**

---

<sup>4</sup> The J-STD-025 definition for Associate is “a telecommunication user whose equipment, facilities, or services are communicating with a subject.”

<sup>5</sup> The J-STD-025 definition for Intercept subject is “a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).”

<sup>6</sup> See also Section 3.1.2 for examples of communication-identifying information for packet-based services as addressed in this document.

1

2 The initiation (successful or unsuccessful) of communication between the intercept subject and an  
3 associate by either party.

4

5 **Session Identifier (new definition)**

6

7 Unique identifier for the intercept subject's network access session in a service provider's network. If  
8 content surveillance is authorized, this parameter uniquely identifies the network access session for  
9 which the subject's incoming, outgoing, and redirected packet activity is to be delivered to a LEA,  
10 and is used to correlate communication-identifying information with the communication content.

11

12 **Minimization (new definition)**

13

14 A procedure that law enforcement officers are required to apply when conducting LAES so as to  
15 minimize the interception of communications not otherwise subject to interception. See 18 U.S.C. §  
16 2518(5).

17

18

### 3. User Perspective of Law Enforcement Agency Needs (Stage 1)

The essential capabilities provided in this contribution are based on law enforcement needs regarding surveillance of packet-based communications. Many of these capabilities are similar to existing capabilities for circuit-mode communications, but are generalized to include packet-based communications. Others prescribe additional functionality specific to the surveillance of packet-based communications services.

The capabilities are grouped into the following functional categories as addressed in the corresponding sections of this contribution:

- Communications Access (3.1)
- Delivery of Intercepted Communications (3.2)
- Performance and Quality (3.3)
- Security and Integrity (3.4)
- Capacity (3.5).

#### 3.1. Communications Access

##### 3.1.1. Separate Access to Communication-Identifying Information and Communication Content

**(EC) 1.** Law enforcement agencies need separate access to an intercept subject's communication-identifying information and communication content (when access to communication content is authorized), consistent with the scope of lawful authorization.

The terms communication-identifying information and communication content are used to describe specific aspects of packet-based communications surveillance and are described below in more detail in an effort to clarify their use in the packet-mode context. The use of the communication-identifying information and communication content terms is intended to be understood as covering the same information described in the Communications Assistance for Law Enforcement Act, 47 U.S.C. 1001(2) as "call identifying information" and "content".

- Communication-identifying information for packet-based communications refers to the information necessary to identify the intercept subject's communications traffic, to determine the parties to a packet-based communication, and to describe, qualify, or otherwise determine, the origin, direction, destination, or termination of the intercept subject's communications.
- Communication content for packet-based communications refers to information concerning the substance, purport or meaning of the communications contained within the intercept subject's incoming, outgoing, or redirected packet data.

In the packet environment, communications content may include both voice and data communications of the intercept subject as transported by the packet-based equipment for the purpose of providing a service.

The specific nature of the communication-identifying information in the packet environment may vary according to the nature of the communications service provided and the mechanisms and

1 protocols used to carry the communications to and from the intercept subject and the associates.  
 2 Associates may include other end-users, equipment, facilities, services, or entities that communicate  
 3 with or attempt to communicate with the intercept subject via the subject's service. Examples may  
 4 include other subscribers to the service, subscribers of other, interconnected TCs, or entities  
 5 otherwise accessible to the intercept subject via the service.

6  
 7 More specific capabilities for law enforcement access to communication-identifying information and  
 8 communications content in the packet environment are discussed in Sections 3.1.2 and 3.1.3,  
 9 respectively.  
 10

### 11 3.1.2. Access to Communication-Identifying Information

12  
 13 **(EC) 2.** Law enforcement agencies need access to available communication-identifying  
 14 information to determine the parties to a communication (originating and terminating), or  
 15 otherwise determine the origin, direction, destination, or termination of the intercept subject's  
 16 communications, regardless of whether or not interception of communication content is  
 17 authorized.  
 18

19 **(EC) 3.** Law enforcement agencies need access to communication-identifying information for  
 20 all completed and attempted communications. An attempted communication is one that was  
 21 initiated, but fails to complete between the originating (source) and terminating (destination)  
 22 parties (e.g., a failed voice call due to unavailable terminating party equipment, or data packets  
 23 originated by the subject that could not be delivered to an associate).  
 24

25 **(EC) 4.** Law enforcement agencies need any success or failure information available to the  
 26 carrier regarding each communication.  
 27

28 Law enforcement recognizes that there may be instances where certain information for attempted  
 29 communications may not be available.  
 30

31 Communication-identifying information for packet-based communications may include, but is not  
 32 necessarily limited to, information in the following categories:  
 33

- 34 • **Subscriber Information** - Information regarding the intercept subject's and associates'  
 35 subscriber identification and service. This may include network addresses (e.g., Directory  
 36 Numbers (DNs), Internet Protocol (IP) addresses), service account identifiers, and subscriber  
 37 service information.
- 38 • **Network Protocol Identifiers and Service Access Ports of Subject Traffic** - The network  
 39 protocol identifiers, and transport-layer service access port numbers of packets generated by  
 40 or destined to the intercept subject, regardless of whether the communications is successfully  
 41 delivered to the intended destination.
- 42 • **Signaling and Control Information** - Information used in communication establishment,  
 43 maintenance and termination, as relevant to the service. This should include redirection or  
 44 re-routing indications, when available.
- 45 • **Communication Attempt Alerts** - Notification that a communication attempt concerning  
 46 the intercept subject has occurred.  
 47

### 1 **3.1.2.1. Subscriber Information**

2  
3 (EC) 5. Law enforcement agencies need access to available Subscriber Information associated  
4 with each communication generated by or destined to the intercept subject. Subscriber  
5 Information<sup>7</sup> includes, but is not necessarily limited to, the following information about the  
6 intercept subject and the associates with whom the subject communicates:  
7

- 8 1. Network Addresses – Information used by the network for sending and receiving  
9 communications to and from the intercept subject. This may include addresses provided to  
10 and by network address translation mechanisms. The intercept subject’s and associates’  
11 network addresses may include, but are not necessarily limited to, Directory Numbers  
12 (DNs), mobile station identifiers, Internet Protocol (IP) addresses (dynamically assigned or  
13 static), and domain names.  
14
- 15 2. Service Account Identifiers<sup>8</sup> – Information provided by a subscriber to the TC for access to  
16 network resources and identification of the allowed services. A subscriber’s service account  
17 identifiers may include, but are not necessarily limited to, login identifiers (IDs), account  
18 numbers, and subaccount numbers. Because subscribers’ network address information may  
19 be associated with a subscriber for only a limited period of time, such as the duration of a  
20 network access communications session, in many cases, a Service Account Identifier is the  
21 only information that is permanent and available to the carrier (and law enforcement) for  
22 identification of the subscriber and his/her traffic.  
23
- 24 3. Subscriber Service Information – Additional characteristics about the nature of the  
25 communication that identify the capabilities of the service as used by the intercept subject  
26 (e.g., authorized bandwidth for the subscriber’s communications session or call, encoding  
27 format of communications). Access to this information for the intercept’s associates may be  
28 limited to what is received by the TC during the communication establishment stage.  
29

### 30 **3.1.2.2. Network Protocol Identifiers and Service Access Ports**

31  
32 (EC) 6. Law enforcement agencies need access to the network protocol identifiers (i.e., the IP  
33 header field that identifies the Transport Layer protocol) and transport-layer service access ports  
34 used in a communication in order to identify the network-relevant services that the subject is  
35 using and/or providing.  
36

37 Such information may be provided, for example, in the transport-layer protocol (e.g., TCP or UDP)  
38 headers of data packets associated with the intercept subject.  
39

### 40 **3.1.2.3. Signaling and Control Information**

41  

---

<sup>7</sup> Information regarding the intercept subject’s subscriber identification. In packet networks it is often the case that the facilities used to identify the intercept subject’s communications are logical rather than physical and fixed. Subscriber Identification Information is the term used in this document for the identification of the intercept subject’s “logical facilities” associated with the service offered by the carrier.

<sup>8</sup> Service account identifier information can be provided to the carrier by passive means (e.g., intercept subject equipment provides this information to the network) or actively input by the intercept subject (e.g., submission of a login ID to the TC).

1 (EC) 7. Law enforcement agencies need access to reasonably available signaling and control  
 2 information for all communications originated by, terminated to, or redirected by the intercept  
 3 subject for the service under LAES. This information is needed regardless of whether it is carried  
 4 in-band with content or on out-of-band signaling channels (either physically or logically  
 5 separated). Signaling and control information includes, but is not necessarily limited to, the  
 6 following:

- 7
- 8 1. Account login events that indicate when an intercept subject has initiated a communications  
 9 service or network access communications session with the service provider's network (e.g.,  
 10 access to the resources associated with the VPIGW service).
- 11 2. All communication-identifying digits dialed by the subject, or otherwise input (e.g., E.164  
 12 addresses and abbreviated dialing sequences) and any signaling information used to  
 13 establish or direct call flow or activate service features (e.g., such as three-way calling for a  
 14 CGVoP service).
- 15 3. Routing information derived by the originating TC based on its interpretation of the  
 16 subject's user input or other call direction commands.
- 17 4. Redirecting routing information, when communications are forwarded or transferred using  
 18 service capabilities. Law enforcement needs access to the redirected-to routing information  
 19 when the intercept subject transfers or forwards communications to another address. For a  
 20 communication terminating to the intercept subject, law enforcement agencies need access  
 21 to any available redirection address information when multiple forwards or transfers are  
 22 involved in the communication attempt<sup>9</sup>.
- 23 5. Location of mobile subscribers. Law enforcement agencies need information on the most  
 24 accurate geographical information known to the network about the location of a mobile  
 25 subscriber at the establishment and termination of each intercepted packet-based call or  
 26 communications session, where such location information is relevant to the control of the  
 27 call or communication session within and between carrier networks.
- 28 6. Changes initiated by the intercept subject (sent to the TC's network) to the encoding  
 29 characteristics of the content stream (e.g., dynamic CODEC changes to a VoP  
 30 communications stream).

#### 31 **3.1.2.4. Communication Attempt Alerts**

32 (EC) 8. Law enforcement agencies need notification of all communication attempts generated by  
 33 or destined to the intercept subject, when known by the TC for that service, regardless of whether  
 34 or not those communications attempts are successful.

35 Such communications attempts include, but are not necessarily limited to:

- 36
- 37
- 38
- 39
- 40 1. Attempts to establish a network access communications session (e.g., successful or failed  
 41 logins or mobile binding establishment attempts).
- 42
- 43 2. Successful and unsuccessful communications attempts generated by or destined to the  
 44 intercept subject.
- 45

---

<sup>9</sup> Redirected-to routing information is required for multiple forwards or transfers as long as the subject's equipment, facility, or service continues to be involved in the communication.

- 1           3. Data packet activity between an intercept subject and an associate, including successfully  
2           transferred packets and denied, blocked or rejected packets.

### 3    3.1.3. Access to Communication Content

4  
5    LEA access to communication content for packet-based communications services is needed  
6    regardless of the service architecture used in the communication, including cases when the  
7    communications between the intercept subject and associates are sent and received over separate  
8    channels, or may be accessed at different IAPs at different geographical locations in the carrier's  
9    network.

10  
11       **(EC) 9.** Law enforcement agencies need access to the communications transmitted, or caused to  
12       be transmitted, to and from the network address, terminal equipment, or other identifier  
13       associated with the intercept subject throughout the service areas operated by the TC served  
14       with the lawful authorization.

15  
16    The communications between the intercept subject and other parties (associates) may take place  
17    using a variety of access and packet transport technologies, including cable, digital subscriber line  
18    (xDSL), IP, frame relay, and asynchronous transfer mode. In many cases these technologies may be  
19    combined in a carrier's network with numerous potential intercept access points for the intercept  
20    subject's communications content.

21  
22    There are several ways to establish and maintain subscriber connections in a packet environment.  
23    Connection arrangements may be categorized is as follows:

- 24  
25       • Carriers may offer their services using connection-oriented technology and protocols where a  
26       dedicated path or virtual path is established through the network prior to a communication  
27       exchange.  
28       • Carriers may offer their service utilizing connectionless technology and protocols where each  
29       packet in a communication is routed individually.

30  
31  
32    The specific nature of the accessed communications content may vary according to the service and  
33    the technology employed. Communication content includes any type of information carried by the  
34    carrier to or from the intercept subject (that is, any transfer of signs, signals, writing, images, sounds,  
35    data, or intelligence of any nature). For voice services, such as CGVoP or VPIGW, accessed content  
36    shall consist of the transported packets containing the encoded voice communications along with  
37    sufficient protocol information to decode and decrypt the voice-band contents. For non-voice  
38    services, content refers to the transported application data payloads comprising the intercept  
39    subject's communications.

### 41   3.1.4. Access Requirements for Specialized Service Capabilities

42    Access to an intercept subject's packet-based communications shall include communications that  
43    involve the use of specialized service capabilities such as packet forwarding, mobility information,  
44    network-based encryption, and multi-way communications.

1 **3.1.4.1. Forwarding, Redirected Communications, and Mobility**

2  
3 (EC) 10. Law enforcement agencies need access to communication content for communications  
4 generated by and destined to the intercept subject, including communications that have been  
5 redirected or have multiple communication recipients.

6  
7 (EC) 11. For redirected (forwarded or transferred) communications, law enforcement agencies  
8 need access to the intercept subject's communications until the carrier's network no longer has  
9 access to the communication.

10  
11 (EC) 12. If access to an intercept subject's communications cannot be maintained, law  
12 enforcement agencies need carriers to provide, as part of communication-identifying  
13 information, the identity of the new carrier and/or service area to law enforcement. The identity  
14 of the new TC and/or service area should be provided to law enforcement as soon as it is  
15 available.

16  
17 (EC) 13. If the new TC's<sup>10</sup> or service area's identity is unavailable, law enforcement agencies  
18 need to be provided with any information that will permit the LEA to determine or infer this  
19 information.

20  
21 **3.1.4.2. Multiple Recipients**

22  
23 (EC) 14. Law enforcement agencies need continuous access to communication content for  
24 services involving multiple communication recipients (for example, voice communications  
25 involving conference calls to multiple associates).

26  
27 (EC) 15. Law enforcement agencies need access to communication content when the intercept  
28 subject's communication stream is placed on hold during a multi-way communication, but the  
29 remaining parties' communications continue to be supported by the intercept subject's  
30 equipment, facilities, or service. Law enforcement needs continued access to the remaining  
31 parties' communications as long as the carrier maintains access to the communication.

32  
33 Law enforcement must be able to determine when to continue monitoring a communication and when  
34 to minimize the monitoring activity based on the circumstances of the investigation. (See the  
35 definition for minimization in Section 2.) In this case, law enforcement will arrange for any  
36 additional bandwidth necessary for the delivery of intercepted information.

37  
38 **3.1.5. Separation of Subscriber Physical Interface from the TC**

39 Packet technologies allow for the separation of a subscriber's physical interface to the packet  
40 network from the carrier that provides the communications service to the subscriber. In these cases,  
41 different carrier(s) may provide the connectivity between the intercept subject and the carrier  
42 network that is offering a packet-based service and must facilitate LAES for the service. This case is  
43 similar to a scenario in the circuit-switched wireline environment where an Incumbent Local  
44 Exchange Carrier (ILEC) provides the distribution facilities to the intercept subject, but a

---

<sup>10</sup> Note that the new TC may not be geographically located in the same area as the TC serving the intercept subject.

1 Competitive Local Exchange Carrier provides the voice service (via its PSTN switch). In this  
 2 scenario, the CLEC is the service provider that may provide the LAES assistance capabilities<sup>11</sup>.

3  
 4 **(EC) 17.** In cases where an intercept subject's physical interface to the packet network is  
 5 separated from the carrier that provides the packet-based communications service for which the  
 6 intercept subject is under LAES, the ability to facilitate lawful access to communication content  
 7 and communication-identifying information is with the TC that offers the packet-based  
 8 communications service to the intercept subject, and has access to communication-identifying  
 9 information and communications content for the subject. This applies even if that TC does not  
 10 necessarily offer direct physical connectivity (via their own facilities) to the intercept subject.

11  
 12 Law enforcement recognizes a carrier's access to the LAES information may be constrained.  
 13 Specifically, the carrier may have access to only the communication-identifying information and  
 14 partial access or even no access to the communication content, as it may bypass the carrier providing  
 15 the service and assistance to law enforcement. While the content for the communications may  
 16 bypass the carrier providing the service, the carrier providing the service is the only carrier that may  
 17 have knowledge of the establishment of the call or communications session and the identities of the  
 18 communication endpoints for that call or communications session (via the service account identifiers  
 19 and routing information for the two end points).

20  
 21 **(EC) 18.** In the case where the TC's access to the intercept subject's communications are  
 22 constrained, law enforcement agencies need access to all communications content and  
 23 communication-identifying information of the intercept subject available to the carrier, and any  
 24 additional information that would assist law enforcement in determining the service area or  
 25 other carrier(s) that have access to any additional information or communications of the subject  
 26 that are authorized to be intercepted.

27  
 28 This handoff information will enable law enforcement agencies to determine other service area(s)  
 29 and/or carrier(s) from which surveillance is needed.

### 30 31 **3.1.6. Real-Time, Full-Time Access to Communications**

32  
 33 **(EC) 19.** Law enforcement agencies need a real-time monitoring capability for interceptions of  
 34 packet-based communications. The term "real-time" refers to the ability to access and monitor  
 35 communications that occurs concurrently with the transmission to or from the intercept subject's  
 36 equipment, facility, or service.

37  
 38 In actuality, there is a small transmission or propagation delay from the moment the intercept  
 39 subject's communications are intercepted until the moment the signals reach the LEA monitoring  
 40 equipment. The immediacy with which the carrier must provide access to the intercept subject's  
 41 communications will vary according to aspects of the communications being accessed:

- 42  
 43 • For **communication-identifying information**, this will depend upon the nature of the  
 44 communication-identifying information:  
 45

---

<sup>11</sup> In this scenario, the LAES assistance responsibilities are performed by the competitive local exchange carrier who provides the switch-based voice service to the intercept subject.

- 1           – For **communication-management-related communication-identifying**  
 2 **information** (i.e., the information used to identify, direct and control the intercept  
 3 subject’s traffic), real-time refers to access that occurs concurrently with the  
 4 establishment and control of a call or communications session. Access to  
 5 communication-identifying information generated during call or communications  
 6 session establishment shall be provided before, during or immediately after the  
 7 transmission to or from the intercept subject.  
 8
- 9           – For **non-connection-management associated events** (for example, service profile  
 10 changes, or changes to the intercept subject’s subscriber account information), real-  
 11 time refers to access that occurs as soon as the information is available to the carrier  
 12 and can reasonably be made available to law enforcement. (See also Section 3.1.7.2  
 13 regarding the reporting of service profile changes.)  
 14
- 15 • For **communications content**, real-time refers to intercept and delivery that occurs  
 16 concurrently with the transmission of communications to or from the intercept subject (in  
 17 other words, as the communications takes place).  
 18

19 Additional needs related to the immediacy of delivery of communication-identifying information and  
 20 communications content to law enforcement on the delivery interface are addressed in Section 3.1.7.  
 21

22 **(EC) 20.** Law enforcement agencies require a full-time monitoring capability for interceptions  
 23 of packet-based communications. The term “full-time” refers to the ability to access and monitor  
 24 all service activity associated with the intercept subject on a 24 hour-per-day basis.  
 25

### 26 3.1.7. Subject Verification and Subscriber Information

27 Law enforcement agencies need administrative information from the TC for non-connection  
 28 management associated events to verify the association of the intercepted packet-based  
 29 communications with the intercept subject, and to identify the services and features subscribed to by  
 30 the intercept subject, both prior to intercept implementation and during the interception.  
 31

#### 32 3.1.7.1. Association of Communications With Intercept Subject

33 **(EC) 21.** Law enforcement agencies need, both prior to intercept implementation and during the  
 34 interception, information necessary to verify the association of the intercepted communications  
 35 with the network identifier (e.g., DN, login ID, IP address), terminal equipment identifier (e.g.,  
 36 MAC Address), and/or personal number of the intercept subject designated in the lawful  
 37 authorization. Specifically, law enforcement agencies must be able to verify that the  
 38 communications facility or service being intercepted corresponds to the subject or subjects  
 39 identified in the lawful authorization.  
 40  
 41

42  
 43 TCs are not expected to verify the type of communications (i.e., the application of the content  
 44 channel) used by the intercept subject beyond the service offered by the carrier.  
 45

##### 46 3.1.7.1.1. Association of Dynamic Addresses and Service Account Identifiers

47

1 In many packet-based communications services, the addressing used to route the intercept subject's  
 2 communications (e.g., an IP address) is dynamically assigned upon the establishment of a  
 3 communications session and is released upon termination of the communications session, such that it  
 4 must be correlated with a permanent subscriber identifier for the service (e.g., a directory number,  
 5 login ID, or account number of the intercept subject).

6  
 7 **(EC) 22.** During interception of packet-based communications services where the address used to  
 8 identify and route an intercept subject's communications is dynamically assigned, law  
 9 enforcement agencies need the TC to provide the following information as part of  
 10 communication-identifying information for the intercepted communications:

- 11
- 12 1. the temporary address dynamically assigned to the intercept subject and used for the
- 13 communications session;
- 14
- 15 2. the key identifier(s) used by the carrier to associate the intercept subject's identity with the
- 16 dynamically assigned address;
- 17
- 18 3. a unique identifier for the communication session; and
- 19
- 20 4. a time-stamp, which is necessary to correlate the dynamic address with the intercept
- 21 subject's identity for the duration of the communications session.
- 22

### 23 **3.1.7.2. Service Profile Information**

24  
 25 Law enforcement agencies need the intercept subject's service profile information (subscription  
 26 information) in response to a lawful inquiry. Service profile information may be required before and  
 27 during interception.

28  
 29 **(EC) 23.** Law enforcement agencies need notification from carriers of changes made to the  
 30 intercept subject's service profile during an ongoing interception when changes are directly  
 31 initiated by the intercept subject.

32  
 33 Service profile information is needed to determine service features and capabilities the intercept  
 34 subject might use and, correspondingly, how much capacity should be allocated to perform the  
 35 LAES. For example, the subject of an ongoing interception may add additional bandwidth to their  
 36 service. In this case, law enforcement may use the service profile change information to determine  
 37 whether to update the intercept authorization and/or arrange for additional bandwidth to support the  
 38 delivery of intercepted communications.

## 39 40 **3.2. Delivery of Intercepted Communications**

### 41 **3.2.1. Transmission**

42  
 43 **(EC) 24.** Law enforcement agencies need TCs to transmit intercepted communications to an  
 44 LEA monitoring facility designated by the law enforcement agency.

45  
 46 Law enforcement agencies will work with TCs in advance to arrange for delivery of intercepted  
 47 communications to the LEA's monitoring location. Guidelines for the transmission of intercepted  
 48 communications are included in Sections 3.2.2 through 3.2.7.

### 1 3.2.2. Correlation of Communication Content with Communication-Identifying 2 Information

3  
4 (EC) 25. If communication-identifying information and communication content are separated,  
5 law enforcement agencies need TCs to provide identifiers on the delivery interface that will  
6 ensure accurate association of the communication-identifying information with communication  
7 content.  
8

9 For certain packet-based communications where communication content surveillance is authorized, it  
10 should include appropriate encapsulation of the subject's sent and received packets within delivery  
11 messages appropriate for the delivery interface. Those delivery interface messages must contain  
12 added correlation descriptors that can be used to associate each packet with the intercept subject's  
13 service, and a specific packet-based communications session or call reported via communication-  
14 identifying information.

### 15 3.2.3. Non-Alteration of Transmitted Content

16  
17 (EC) 26. Law enforcement agencies need TCs to be able to transmit the intercepted  
18 communications to an LEA monitoring location without altering the communication content or  
19 meaning (exclusive of any processing [e.g., protocol/encoding format changes, encryption]  
20 required for delivery to law enforcement).  
21

22 (EC) 27. Law enforcement agencies need TCs to protect intercept controls, intercepted call  
23 content, and communication-identifying information consistent with the carrier's security  
24 policies and procedures in order to prevent unauthorized access, alteration, mutilation or  
25 manipulation, and disclosure of the transported data.  
26

27 Any minimization of the intercept subject's communication content (see definition in Section 2) in  
28 order to comply with the lawful intercept authorization is the sole responsibility of the law  
29 enforcement agency.

### 30 3.2.4. Content Decoding, Decompression, and Decryption

31 Law enforcement agencies' collection systems must be able to properly process communication  
32 content delivered by the TC. Intercept subject communications are encoded, and could also be  
33 compressed and encrypted.  
34

35 If the TC provides or controls the encoding, compression and/or encryption for the intercept subject's  
36 communications or at least is knowledgeable of this processing, the TC must either transmit the  
37 communication content in a decoded, decompressed and decrypted form, or provide the information  
38 (e.g., encoding method, compression method, encryption keys) needed by the law enforcement  
39 agency's collection system to perform this processing.  
40

41 (EC) 28. When the TC provides or controls the encoding, compression and/or encryption for the  
42 intercept subject's communications or at least is knowledgeable of this processing, law  
43 enforcement needs the TC to either transmit the communication content, when authorized,  
44 toward the law enforcement agency's collection system in a decoded, decompressed and  
45 decrypted form, or provide to the law enforcement agency's collection system the information  
46 necessary to decode, decompress and/or decrypt the communication content.

1  
2 Law enforcement prefers that the TC perform any decoding, decompression and/or decryption prior  
3 to the delivery of communication content. Since some of the communication content may be sent  
4 using proprietary protocols or special encoding formats that may make it difficult for law  
5 enforcement to convert back to the original end user communication, this preference is greater if  
6 proprietary or specialized encoding, compression and/or encryption had been used.

7  
8 For cases where carriers provide network-based encryption, protocol conversion, or special encoding  
9 for intercept subject traffic, it is desirable for the carrier to provide access to communication content  
10 prior to encryption, conversion and/or encoding for traffic that is ingress to the network and after  
11 encryption, conversion and/or encoding for egress traffic.

12  
13 When pre- or- post-encryption/conversion/encoding access is not provided for such specially  
14 modified traffic, carriers should provide all information available to the network that would facilitate  
15 law enforcement's ability to analyze, decode, decrypt, and/or convert the content stream, understand  
16 the involved protocols or encoding formats, or otherwise discern the content.

17  
18 For example, if an intercept subject uses a voice service over a packet network where the subject's  
19 equipment encodes the communications stream based on a command from the carrier, when  
20 delivering this communication content to law enforcement, the carrier should provide information on  
21 the encoding scheme used for the communication in addition to delivering the content itself.  
22 Similarly, if the carrier's network provides secure virtual private networking services for the subject  
23 or associates, including network tunneling with encryption, the carrier is expected to provide either  
24 the decrypted content stream or information on the protocols and encryption keys used to encrypt the  
25 content.

### 27 **3.2.5. Use of Standard, Generally Available Delivery Interface**

28  
29 It is highly desirable to law enforcement agencies that the facilities, data communications protocols,  
30 and data format used for the transmission of the intercepted communications to the LEA monitoring  
31 location be standard, cost effective, and generally available.

32  
33 Examples of such common, generally available, delivery interface technologies include Digital  
34 Signal/Level 0 (DS0) facilities, ATM Permanent Virtual Circuits (PVCs), IP Version 4 (IPv4)  
35 packets at the network layer, and the Transmission Control Protocol (TCP) at the transport layer.  
36 Additional protocols and formats can be jointly agreed upon by law enforcement and TCs.

### 37 **3.2.6. Congruence With Existing Delivery Interfaces**

38 Law enforcement recognizes that the CALEA law does not limit the number or types of interfaces  
39 used for the transmission of the intercepted communications to an LEA monitoring location.  
40 However, it is highly desirable to law enforcement that TCs reuse or apply formatting from existing  
41 specifications for surveillance delivery interfaces for their service. The intention is to consolidate the  
42 number of interfaces law enforcement will need to comply with. For example, when developing a  
43 surveillance delivery interface for voice services over a packet network, an implementation's  
44 adoption of traditional J-STD-025 messages and parameters (where applicable) would be highly  
45 desirable for law enforcement.

1 It is highly desirable to law enforcement that TCs reuse or re-apply message formatting and encoding  
 2 definitions from existing specifications, including the J-STD-025 specification, for the surveillance  
 3 delivery interfaces for comparable packet-based communication services.

#### 4 **3.2.7. Consolidated Delivery Interface and Transmission Facilities**

5 It is highly desirable to law enforcement that TCs minimize the number of physical transmission  
 6 facilities used to deliver the intercepted communications to each LEA monitoring facility.

7  
 8 For example, in many Voice over Packet solutions several network elements may be involved in the  
 9 interception of communication content and communication-identifying information. In these cases,  
 10 law enforcement would prefer a connection from a single centralized delivery function or system to  
 11 the monitoring facility, rather than several connections from each network element involved in the  
 12 surveillance access.

### 13 **3.3. Performance and Quality**

#### 14 **3.3.1. Reliability**

15 Reliability refers to the probability that a system or product will perform in a satisfactory manner for  
 16 a given period of time when used under specified operating conditions.

##### 17 **3.3.1.1. Availability**

18 Some packet-based communications services may be offered with specific levels of reliability to  
 19 subscribers as part its service-level agreements. Other packet-based communications services are  
 20 offered with grades of reliability, such that there are no assurances provided for establishing a  
 21 transport-layer connection to the destination point or the successful delivery of subscriber messages  
 22 to their intended destinations. In these cases, the network does not make any assurances on the  
 23 quality or reliability of the communication service offered to the subscriber.

24  
 25 **(EC) 29.** During the interception period, law enforcement agencies need the reliability of the  
 26 service supporting the interception be at least equal to the reliability of the subject's service,  
 27 when the network assures the reliability of the communication service offered to the subscriber.

28  
 29 **(EC) 30.** During the interception period, law enforcement agencies need the reliability of the  
 30 service supporting the interception be higher than the reliability of the intercept subject's  
 31 service, when the network does not make any assurances on the reliability of the communication  
 32 service offered to the subscriber.

33  
 34 **(EC) 31.** Law enforcement agencies require reliable delivery to the LEA collection system  
 35 regardless of whether reliable delivery methods are employed by the network in offering service  
 36 to the intercept subject.

37  
 38 **(EC) 32.** Law enforcement needs TCs to establish plans for ensuring that system upgrades,  
 39 software upgrades, and other network management procedures do not disrupt or terminate  
 40 ongoing interceptions.

##### 41 **3.3.1.2. Fault Management**

1 (EC) 33. Law enforcement agencies need carriers to support capabilities to detect and resolve  
2 problems with:

- 3 1. the interception of communication-identifying information and communication content; and
- 4 2. the transmission of the intercepted communications to the designated LEA monitoring  
5 facility.

### 8 3.3.2. Quality of Service

9 Quality of service in regard to the interception refers to the quality specification of the  
10 communications channel or system used to transmit the intercepted communications to the LEA  
11 monitoring facility. For example, quality of service may be measured based on quantitative factors,  
12 such as packet loss, bit error rate, or any other parameter used to measure transmission quality.

13  
14 (EC) 34. Law enforcement agencies need for the quality of service of the intercepted  
15 transmissions delivered to the LEA monitoring facility to comply with performance standards of  
16 TCs for the monitored packet-based communications service.

### 17 3.3.3. Timing Requirements

18 Accurate time-stamps and prompt delivery of intercepted packet-based communications to the  
19 monitoring facility are critical to the conduct of law enforcement investigations. The following  
20 capabilities address these aspects of LAES.

#### 21 22 3.3.3.1. Time Stamp Accuracy

23 Law enforcement agencies need time stamp information to correlate the communication-identifying  
24 information with delivered communications content.

25  
26 Communication-identifying message must be time stamped within a specific amount of time from  
27 when the event triggering the message occurred. This time stamp would allow the LEA to associate  
28 the message with the communication content.

29  
30  
31 (EC) 35. Law enforcement agencies need communication-identifying information to be time-  
32 stamped within a specific amount of time from when an event triggering the generation of the  
33 communication-identifying information occurs. Time stamping shall be provided for  
34 encapsulated intercept subject packets delivered to the LEA.

#### 35 36 3.3.3.2. Event Timing

37  
38 Communication-identifying information must be transmitted over the delivery interface to the LEA  
39 collection system within a defined amount of time after the event occurs, in order for the LEA to  
40 correctly associate the communication-identifying information with communication content.

41  
42 (EC) 36. Law enforcement agencies need communication-identifying information within a  
43 defined amount of time after the occurrence of the corresponding event in the network.  
44

## 1 **3.4. Security and Integrity**

### 2 **3.4.1. Transparency of Interceptions**

3  
4 **(EC) 37.** Law enforcement agencies need each interception to be transparent to the subject, the  
5 subject's associates, and to all parties except the investigative agency or agencies requesting the  
6 interception, and specific individuals involved in implementing the intercept capability. At a  
7 minimum, the transparency of an interception must satisfy the following criteria:

- 8
- 9 1. Indications that an interception is underway should not be discernible to anyone using the
- 10 subject facilities or other any other parties.
- 11 2. If the implementation of an interception occurs during an ongoing communication, the
- 12 interception should not disrupt or interrupt the ongoing communication (that is, no
- 13 interruption or alteration of communications shall occur on active channels).
- 14 3. If the implementation of an interception causes changes in the operation of services and
- 15 features, such changes should not be perceptible to the subject or other parties.
- 16 4. If any noise/packet loss/increased latency/error rate increase is introduced by the
- 17 implementation of an interception, such noise/packet loss/increased latency/error rate
- 18 increase should not be perceptible to the subject or other parties.
- 19

20 Law enforcement agencies need TCs to notify the appropriate law enforcement agency upon learning  
21 that intercept transparency was or may have been compromised. In such a situation, TCs should  
22 recognize that time is of the essence because the safety of the public and other law enforcement  
23 officers may be at risk.

24  
25 To meet law enforcement needs for transparency, the services and transmission characteristics  
26 provided to the intercept subject or any other subscriber should continue to comply with industry  
27 standards.

### 28 **3.4.2. Security of Delivered Surveillance**

#### 29 30 **3.4.2.1. Separation of Surveillance Interfaces from Subscriber Traffic**

31  
32 **(EC) 38.** If any part of a surveillance solution employed by a carrier uses shared network  
33 resources with its subscribers' traffic, law enforcement agencies need the surveillance  
34 information to be logically, physically, or otherwise separated and protected from access by the  
35 carrier's subscribers.

36  
37 TCs are not expected to ensure a level of security for intercept access and transparency beyond the  
38 capabilities of their own equipment.

#### 39 40 **3.4.2.2. Encryption of Delivered Communication-Identifying Information and** 41 **Communication Content**

42  
43 The confidentiality and transparency of surveillance data must be protected as it transits between the  
44 TC delivery function and the LEA monitoring facility.

1 (EC) 39. If shared network resources are to be used for the delivery of communication-  
 2 identifying information and communication content to an LEA, law enforcement needs the  
 3 communication-identifying information and communication content to be encrypted on the  
 4 delivery interface.  
 5

### 6 3.4.3. Procedural Safeguards

7  
 8 TCs are expected to institute prudent procedures and apply technical solutions, where necessary, to  
 9 maintain the confidentiality and transparency of intercepted communications. Such measures should  
 10 be consistent with the risk of compromising the information pertaining to intercept activities.  
 11

12 (EC) 40. Law enforcement agencies need TCs to establish operating practices and procedures  
 13 containing safeguards that preclude unauthorized or improper access to or use of interception  
 14 capabilities and to prevent any compromises of transparency.  
 15

16 Examples of such procedural safeguards include:  
 17

- 18 a. Restrictions on access to information about interception capabilities;
- 19 b. Physical security to limit access to systems controlling or supporting interceptions;
- 20 c. Security mechanisms for activating and deactivating interceptions or accessing captured  
 21 communication-identifying information or communications content (e.g., via access  
 22 passwords and possibly case-level security);
- 23 d. Procedures to prevent subjects from being notified of service changes caused by the  
 24 implementation of interceptions;
- 25 e. Restriction of knowledge of interceptions to authorized telecommunications carrier personnel  
 26 (i.e., personnel with a “need-to-know”).  
 27

## 28 3.5. Capacity and Transmission Bandwidth

### 29 3.5.1. Simultaneous Interceptions

30  
 31 (EC) 41. Law enforcement agencies must be able to perform multiple, simultaneous  
 32 interceptions within a carrier’s network and at each of its relevant network elements (Intercept  
 33 Access Points) located throughout the carrier’s service area. The capability for multiple,  
 34 simultaneous interceptions shall include the following:  
 35

- 36 1. Ability to access and monitor all simultaneous communications originated, received, or  
 37 redirected by the intercept subject.  
 38
- 39 2. Ability for multiple law enforcement agencies to monitor, simultaneously, the same  
 40 intercept subject while maintaining transparency, including between agencies. Up to five  
 41 LEAs must be able to simultaneously monitor the same intercept subject.  
 42
- 43 3. Ability of the TCs to simultaneously support a number of separate (i.e., multiple subjects)  
 44 legally authorized interceptions within its service area, including different levels of  
 45 authorization for each interception (i.e., communication-identifying information only, or  
 46 communication-identifying information and communication content).

1

**2 3.5.2. Transmission Bandwidth**

3

4 Individual law enforcement agencies are responsible, with the assistance of carriers, for ordering and  
5 acquiring sufficient transmission bandwidth from each TC in a timely manner for the lawful  
6 interception capability to be performed and for communication-identifying information and  
7 communication content to be delivered from the TC to the LEA's collection system(s) such that the  
8 required number of intercept subjects and their packet-based service characteristics can be  
9 appropriately handled.

10

**11 4. Recommendation**

12

13 It is proposed that this Stage 1 description be incorporated into Section 4 (Stage 1 Description: User  
14 Perspective) of J-STD-025, Revision B. The J-STD-025 specification's Stage 1 description only  
15 minimally addresses surveillance capabilities for packet-based communications (i.e., Section 4.6.3,  
16 Packet Data IAP), where full content is being provided for selected packet streams. It is proposed that  
17 the Stage 1 material from this contribution be incorporated within Section 4. The detailed  
18 organization of the section structure and any needed revisions to existing text for circuit-mode  
19 surveillance are for further study.

20

## **APPENDIX B**

# T1BALLOT

---

**From:** Les Szwajkowski [lmski.calea@fbi.gov]  
**Sent:** Wednesday, September 17, 2003 2:38 PM  
**To:** T1BALLOT  
**Cc:** pdhollar@lafayettegroup.com  
**Subject:** T1 Letter Ballot LB 1174

ACCREDITED STANDARDS COMMITTEE  
T1-TELECOMMUNICATIONS  
LETTER BALLOT

\*\*-- ACTION REQUESTED --\*\*

REPLY TO: ATIS                      Letter Ballot Number: LB 1174  
T1 Secretariat                      Document Number: J-STD-025B  
1200 G St., NW, Suite 500      Date: 08/19/03  
Washington, DC 20005          Ballot Period: 4 Weeks  
FAX: 202.347.7125              Ballot Closes: 09/17/03  
EM: [t1ballot@atis.org](mailto:t1ballot@atis.org)

Authorized By: T1P1/T1S1  
Distributed By: T1 Secretariat

Subject: Draft Proposed Trial-Use/Interim Standard - Lawfully  
Authorized Electronic Surveillance (Joint TIA/T1  
draft proposal)

Statement: The T1P1 and T1S1 members at their August 2003  
plenary approved this draft proposed  
Trial-Use/Interim Standard for letter ballot. This  
dpANS for Trial-Use is under the Joint T1/TIA  
Standards Document (JSD) Process where TIA is the  
lead organization and sole submitter to ANSI.  
Please note: Due to an interest category imbalance  
at the time of this letter ballot, weighted voting  
of a .87 value applies to the manufacturing interest  
group.

Question: Do you approve this draft proposed standard for  
Trial-Use per ANSI procedures for future submittal  
to ANSI for approval as an American National  
Standard?

Ballot: YES \_\_\_\_\_ NO X (Comments Required)

Ballot: YES \_\_\_\_\_ (w/ comments) ABSTAIN \_\_\_\_\_ (w/ reasons)

ABSTAIN \_\_\_\_\_

(IF VOTING "NO, WILL VOTE CHANGE TO "YES" IF THE ATTACHED  
CHANGES ARE MADE?)

YES X NO \_\_\_\_\_

Signature \_Leslie M. Szwajkowski\_\_\_\_\_ Principal\_X\_ Alternate\_\_\_\_

Organization \_FBI-CIU (formally the ESTS)\_\_\_\_\_ DATE\_9/17/03

Telephone #: \_703-814-4808\_\_\_\_\_

ESTS's comments are attached.

# LB 1174

## Vote:

The CALEA Implementation Unit (CIU) (formerly the Electronic Surveillance Technology Section) of the Federal Bureau of Investigation has reviewed Letter Ballot 1174 (LB 1174) (PN-4465-RV1) and has concluded that the document does not supply Law Enforcement (LE) with the capabilities it needs to perform surveillance activities for packet-mode communications. CIU has also concluded that LB 1174 does not provide the level of detail necessary for a document of this importance and is likely to create confusion for Telecommunication Service Providers (TSPs), equipment manufacturers, and LE in their efforts to implement packet-mode surveillance. As a result of both the deficiencies and the insufficient level of detail in the proposed J-STD-025-B (as discussed below) CIU votes **No** on LB 1174 and maintains that J-STD-025-B should not be adopted as the standard for packet-mode communications.

## General Comments:

The stated intent of J-STD-025-B is to define "...the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance." CIU's position is that the revised document J-STD-025-B is significantly deficient in addressing packet-mode communications. Therefore, CIU cannot support adoption of a deficient standard that will have the effect of affording TSPs or equipment manufacturers "safe harbor" with respect to packet-mode communications.

LE is the sole user of the surveillance capabilities described in the document. Notwithstanding this, CIU believes that the expressed needs of LE with regard to packet-mode communications were given only cursory consideration during the development of J-STD-025-B. LE, through CIU, expended considerable effort throughout the course of the J-STD-025-B developmental timeline to (1) propose an approach to packet-mode surveillance that would best meet the needs of LE while minimizing the cost of development and implementation and (2) develop the Stage 1 language and requirements for packet-mode surveillance in a technology-neutral manner. The following list of CIU's contributions clearly demonstrates the extent of LE's efforts to convey its needs to TR45 LAES Ad Hoc Group:

- TR45.LAES/2001.08.29: Proposal for work product of TR 45 LAES Ad Hoc Group work on Packet-Mode Data Surveillance Capabilities to be contained in a new document.
- TR45.LAES/2001.11.07.06: Overview of Packet Surveillance Fundamental Needs for Law Enforcement.
- TR45.LAES/2001.12.18.02: Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.01.21.06: Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.01.21.03: Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities for packet-based communications pursuant to the Communications Assistance for Law Enforcement Act (CALEA).
- TR45.LAES/2002.02.12.05 (plus Revision 1): Framework for Development of LAES of Packet-based Communications.

- TR45.LAES/2002.02.12.09: Comments on Motorola Contribution (TR LAES/2002.02.12.03) on CALEA Requirements and Quotations.
- TR45.LAES/2002.04.22.03 (plus Revision 1): Stage 1 material for PN-4465-RV1.
- TR45.LAES/2002.05.21.03: Stage 1 material for PN-4465-RV1.

In particular, contribution TR45.LAES/2002.01.21.06 provided a comprehensive Stage 1 description of LE's needs including 41 essential capabilities specifically worded to cover the differences in terminology and technology between packet-mode and circuit-mode communications. This contribution and others made by CIU were repeatedly rejected based on the argument that the definitions or requirements were "already in the document." CIU made these contributions principally because, in its view, the existing standard (J-STD-025A) makes explicit reference to circuit-mode technology but not packet-mode technology and, therefore, the new language was critical to the stated goal of creating the expanded standard.

The net effect of the TR45 LAES Ad Hoc Group's consistent rejection of the contributions submitted by CIU relevant to LE's needs as sole user of the capability is to render the J-STD-025-B document essentially equivalent to the existing J-STD-025-A document. For example, J-STD-025-B contains no detailed requirements for services such as voice over packet communications. The J-STD-025-B document, in its present form, is, therefore, superfluous and of no value to either the industry or LE.

More specifically, CIU finds that J-STD-025-B, as circulated for balloting, is deficient in the following areas which are of major concern to LE:

1. Terminology does not include the concept of a 'session' as distinct from a 'call.'
2. Subject and associate's media information (e.g., network address, media format) would not be reported.
3. Bandwidth and bearer control events associated with the call would not be reported
4. Intercept subject and associate's contact address information would not be reported (if these become available during, for example, SIP-based call setup).
5. Definitions for party identities have not been extended to support identifiers used by common packet protocols (e.g., URI for SIP).
6. Concept of reporting location (of a mobile subscriber) would not include personal mobility (e.g., common for SIP phones).
7. Address registration and de-registration would not be reported.
8. Reporting of post-cut-through addresses would not be extended to addresses other than E.164 numbers (e.g., a SIP URI).
9. Intercept subject's request for permission to originate or terminate a call to/from an associate would not be reported (needed for cases where the call control signaling would not be reported because call control is end-to-end and therefore not performed by the carrier's call management nodes).
10. Address resolutions would not be reported.
11. Certain call redirections would not be reported, even when the subject's service is aware of them (e.g., associate redirections occurring subsequent to the subject becoming involved in a call).
12. Call release information (e.g., cause) known/used by the subject's service would not be reported.
13. Regarding cdma2000 intercept solution, the rejection of TR45.LAES/2002.01.21.06 containing the Stage 1 language and requirements by TR45 LAES Ad Hoc Group for

the “common” requirements sections of the standard render the technology-specific cdma2000 interception solution deficient. Critical topics such as performance, reliability, security, and capacity, specific to packet-mode communications, are missing.

14. Packet Activity Reporting (i.e., reporting of IP address and transport layer port number information for the source and destination of an IP packet) is vital to any packet data surveillance solution and is missing from the cdma2000 interception solution.
15. For cdma2000, the location information that can be provided at the beginning and end of a session is limited to cell site identification. Technology has already been developed that can provide more accurate location information such as longitude and latitude, and this should be reported to LE when available in the network.

While some might argue that the detailed requirements for packet-mode communications are found in normative references listed within J-STD-025B, CIU and LE are being asked to approve a standard that would be afforded “safe harbor” status for packet-mode surveillance that:

1. does not reflect LE’s stated User requirements
2. does not contain the text of specific requirements for enabling surveillance of packet-mode communications and
3. cites, as a normative reference for packet-mode surveillance capabilities, a document that is incomplete and furthermore does not have “safe harbor” status itself.

In light of the above, CIU’s position is that J-STD-025B, in and of itself, lacks specific requirements for packet-mode communications and, therefore, cannot be claimed to have “safe harbor” status for packet-mode communications.

For these reasons, CIU believes J-STD-025B should not be adopted, and that TSPs and equipment manufacturers should not be afforded “safe-harbor” with respect to packet-mode communications by virtue of their compliance with a deficient standard (J-STD-025-B).

## **APPENDIX C**



## U.S. Department of Justice

Federal Bureau of Investigation

---

*Electronic Surveillance Technology Section  
14800 Conference Center Drive, Suite 300  
Chantilly, VA 20151*

April 16, 2004

Re: Reply to "Call for Comments" on J-STD-025-B as a Trial Use Standard

Ms. Susan Carioti  
ATIS  
1200 G St, NW, Suite 500  
Washington, DC 20005

Dear Ms. Carioti:

This letter provides a reply to the call for comments on the use of J-STD-025-B as a Trial Use Standard announced in the March 19, 2004 issue of *ANSI Standards Action* as well as an explanation of the perceived futility of further interactions in the balloting process for this document, as T1 has yielded all comment resolution procedures to TIA, where LE is not being treated fairly.

The fact that the CALEA Implementation Unit (CIU) of the FBI is dissatisfied with the content of proposed J-STD-025-B and the procedures followed to create it has not been a secret for some time. To wit, the following is a quote from a letter dated February 28, 2003, that was sent from the Electronic Surveillance Technology Section (ESTS), of which CIU is a part, to the Chairperson of the TIA TR 45 LAES AHG.

Attached to this letter is the set of comments that indicates the numerous technical issues

**The undefined scope and approach adopted by the group has fostered the development of a work product that is ill defined and unusable. ESTS submitted several contributions proposing a general approach, and capabilities required by law enforcement for interception of packet-based communications, and none of these contributions were accepted. Further, the group has broadened its scope to include legal and regulatory issues well beyond the purview of any industry standards-setting organization. This has shifted the focus away from the development of technical interception capabilities.**

Law Enforcement has with this proposed trial use standard and which was provided in this organization's response to the ballot of J-STD-025-B. As indicated in the official response to ESTS from TIA, which acted as the lead SDO in this joint activity with ATIS, no action was taken on these comments. "Due to the lack of a contribution or representation for CIU at the October meeting, discussion resulted in no further action being taken on the CIU ballot comments. No changes were made to PN-4465-RV1 as a result of your ballot comments. The overall status of your ballot comments is 'No Action'." While we have difficulty understanding how such an approach to comments on a proposed standard is consistent with that of an ANSI-accredited standards development organization, it is characteristic of the lack of serious consideration of the input by this organization. One may see extensive evidence of this by referencing the meeting reports of the TIA

Ms. Susan Carioti  
April 16, 2004

TR 45 LAES AHG - where this document was developed - for the record of how the contributions from Law Enforcement were treated.

It is important to observe that 47 USC § 1006 (a) (1) specifically directs the Attorney General, in coordination with federal, state, and local Law Enforcement agencies to consult with appropriate associations and standards-setting organizations. The Attorney General has delegated its consultative authority under 47 USC § 1006 (a) (1) to the Director of the Federal Bureau of Investigation, see 28 C.F.R. 0.85(o), which in turn tasked CIU with performing this required consultation. Therefore, CIU is representative of not just the FBI but of all Law Enforcement relative to consultation with industry in the matter of lawfully authorized electronic surveillance capability development. This clearly identifies this organization as an affected party and the sole voice for this constituency in the preparation of this proposed trial use (or "interim" in the parlance of TIA) standard. We note that the synopsis of the document in the *ANSI Standards Action* indicates that "this document defines the interfaces between a telecommunications service provider (TSP) and a law enforcement agency (LEA) to assist the LEA ... ." Since ESTS is the official representative of one side of this interface standard and this organization believes that its input to the specification of this interface has been systematically and inappropriately discounted and ignored, it is hard to imagine a reasonable individual supporting that J-STD-025-B should be recognized as a trial use standard.

Furthermore, the lead SDO for this document continues to confuse the application of this document. In the same issue of *ANSI Standards Action* that J-STD-025-B is proposed as a trial use standard through January 1, 2007, TIA has announced a PINS to issue the document as an American National Standard. The project form approved by TIA TR 45 indicates a proposed completion date of June, 2004. As if this didn't cause enough confusion for the industry, the March 26 issue of *ANSI Standards Action* announced a PINS for J-STD-025-C - an extension of version B. The project form, approved by TIA TR 45, indicates a proposed completion date of November, 2004 for that document. Other correspondence will respond directly to the confusion introduced by these other documents.

Sincerely,



Greg Milonovich,

Supervisory Special Agent, FBI  
CALEA Implementation Unit  
(703) 814-4713

Copy to:  
Ms. Aivelis Colon, ATIS  
Ms. Susan Hoyler, TIA  
ANSI Board of Standards Review

## Annex 1 - LB 1174 Vote by CIU

The CALEA Implementation Unit (CIU) of the Electronic Surveillance Technology Section of the Federal Bureau of Investigation has reviewed Letter Ballot 1174 (LB 1174) (PN-4465-RV1) and has concluded that the document does not supply Law Enforcement (LE) with the capabilities it needs to perform surveillance activities for packet-mode communications. CIU has also concluded that LB 1174 does not provide the level of detail necessary for a document of this importance and is likely to create confusion for Telecommunication Service Providers (TSPs), equipment manufacturers, and LE in their efforts to implement packet-mode surveillance. As a result of both the deficiencies and the insufficient level of detail in the proposed J-STD-025-B (as discussed below) CIU votes **No** on LB 1174 and maintains that J-STD-025-B should not be adopted as the standard for packet-mode communications.

### General Comments:

The stated intent of J-STD-025-B is to define "...the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance." CIU's position is that the revised document J-STD-025-B is significantly deficient in addressing packet-mode communications. Therefore, CIU cannot support adoption of a deficient standard that will have the effect of affording TSPs or equipment manufacturers "safe harbor" with respect to packet-mode communications.

LE is the sole user of the surveillance capabilities described in the document.

Notwithstanding this, CIU believes that the expressed needs of LE with regard to packet-mode communications were given only cursory consideration during the development of J-STD-025-B. LE, through CIU, expended considerable effort throughout the course of the J-STD-025-B developmental timeline to (1) propose an approach to packet-mode surveillance that would best meet the needs of LE while minimizing the cost of development and implementation and (2) develop the Stage 1 language and requirements for packet-mode surveillance in a technology-neutral manner. The following list of CIU's contributions clearly demonstrates the extent of LE's efforts to convey its needs to TR45 LAES Ad Hoc Group:

- TR45.LAES/2001.08.29: Proposal for work product of TR 45 LAES Ad Hoc Group work on Packet-Mode Data Surveillance Capabilities to be contained in a new document.
- TR45.LAES/2001.11.07.06: Overview of Packet Surveillance Fundamental Needs for Law Enforcement.
- TR45.LAES/2001.12.18.02: Framework for Development of LAES of Packetbased Communications.
- TR45.LAES/2002.01.21.06: Framework for Development of LAES of Packetbased Communications.
- TR45.LAES/2002.01.21.03: Stage 1 Description of Lawfully Authorized Electronic Surveillance (LAES) capabilities for packet-based communications pursuant to the Communications Assistance for Law Enforcement Act (CALEA).
- TR45.LAES/2002.02.12.05 (plus Revision 1): Framework for Development of LAES of Packet-based Communications.
- TR45.LAES/2002.02.12.09: Comments on Motorola Contribution (TR LAES/2002.02.12.03) on CALEA Requirements and Quotations.
- TR45.LAES/2002.04.22.03 (plus Revision 1): Stage 1 material for PN-4465-RV1.
- R45.LAES/2002.05.21.03: Stage 1 material for PN-4465-RV1.

In particular, contribution TR45.LAES/2002.01.21.06 provided a comprehensive Stage 1 description of LE's needs including 41 essential capabilities specifically worded to cover the differences in terminology and technology between packet-mode and circuit-mode communications.

This contribution and others made by CIU were repeatedly rejected based on the argument that the definitions or requirements were "already in the document." CIU made these contributions principally because, in its view, the existing standard (J-STD-025A) makes explicit reference to circuit-mode technology but not packet-mode technology and, therefore, the new language was critical to the stated goal of creating the expanded standard.

The net effect of the TR45 LAES Ad Hoc Group's consistent rejection of the contributions submitted by CIU relevant to LE's needs as sole user of the capability is to render the J-STD-025-B document essentially equivalent to the existing J-STD-025-A document. For example, J-STD-025-B contains no detailed requirements for services such as voice over packet communications.

The J-STD-025-B document, in its present form, is, therefore, superfluous and of no value to either the industry or LE.

More specifically, CIU finds that J-STD-025-B, as circulated for balloting, is deficient in the following areas which are of major concern to LE:

1. Terminology does not include the concept of a 'session' as distinct from a 'call.'
2. Subject and associate's media information (e.g., network address, media format) would not be reported.
3. Bandwidth and bearer control events associated with the call would not be reported
4. Intercept subject and associate's contact address information would not be reported (if these become available during, for example, SIP-based call setup).
5. Definitions for party identities have not been extended to support identifiers used by common packet protocols (e.g., URI for SIP).
6. Concept of reporting location (of a mobile subscriber) would not include personal mobility (e.g., common for SIP phones).
7. Address registration and de-registration would not be reported.
8. Reporting of post-cut-through addresses would not be extended to addresses other than E.164 numbers (e.g., a SIP URI).
9. Intercept subject's request for permission to originate or terminate a call to/from an associate would not be reported (needed for cases where the call control signaling would not be reported because call control is end-to-end and therefore not performed by the carrier's call management nodes).
10. Address resolutions would not be reported.
11. Certain call redirections would not be reported, even when the subject's service is aware of them (e.g., associate redirections occurring subsequent to the subject becoming involved in a call).
12. Call release information (e.g., cause) known/used by the subject's service would not be reported.
13. Regarding cdma2000 intercept solution, the rejection of TR45.LAES/2002.01.21.06 containing the Stage 1 language and requirements by TR45 LAES Ad Hoc Group for the "common" requirements sections of the standard render the technology-specific cdma2000 interception solution deficient. Critical topics such as performance, reliability, security, and capacity, specific to packet-mode communications, are missing.
14. Packet Activity Reporting (i.e., reporting of IP address and transport layer port number information for the source and destination of an IP packet) is vital to any packet data surveillance solution and is missing from the cdma2000 interception solution.
15. For cmda2000, the location information that can be provided at the beginning and end of a session is limited to cell site identification. Technology has already been developed that can provide more accurate location information such as longitude and latitude, and this should

be reported to LE when available in the network.

While some might argue that the detailed requirements for packet-mode communications are found in normative references listed within J-STD-025B, CIU and LE are being asked to approve a standard that would be afforded "safe harbor" status for packet-mode surveillance that:

1. does not reflect LE's stated User requirements
2. does not contain the text of specific requirements for enabling surveillance of packet-mode communications and
3. cites, as a normative reference for packet-mode surveillance capabilities, a document that is incomplete and furthermore does not have "safe harbor" status itself.

In light of the above, CIU's position is that J-STD-025B, in and of itself, lacks specific requirements for packet-mode communications and, therefore, cannot be claimed to have "safe harbor" status for packet-mode communications.

For these reasons, CIU believes J-STD-025B should not be adopted, and that TSPs and equipment manufacturers should not be afforded "safe-harbor" with respect to packet-mode communications by virtue of their compliance with a deficient standard (J-STD-025B).