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

In the Matter of:	)	
Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act	)	Docket No. _____

JOINT PETITION FOR EXPEDITED RULEMAKING

Louis J. Freeh, Director
Federal Bureau of Investigation

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Honorable Janet Reno
Attorney General of the United States

Stephen W. Preston
Deputy Assistant Attorney General

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

TABLE OF CONTENTS

SUMMARY

The Communications Assistance for Law Enforcement Act (CALEA) was enacted in 1994 to ensure that ongoing technological changes in the telecommunications industry would not compromise the ability of federal, state, and local law enforcement agencies to engage in lawful surveillance activities. To that end, Section 103 of CALEA explicitly obligates telecommunications carriers to ensure that their equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement agencies all communications and call-identifying information that law enforcement is authorized to acquire.

CALEA contemplates that the communications industry, acting in consultation with law enforcement agencies, will develop technical requirements and standards that implement the assistance capability requirements of Section 103 and act as a "safe harbor" for industry. At the same time, Congress recognized that the standards developed by industry might be inadequate to carry out the statutory mandates. Section 107(b) of CALEA therefore authorizes the Commission to issue rules establishing additional technical requirements and standards if a government agency believes that an industry standard is deficient.

The Department of Justice and the Federal Bureau of Investigation (FBI) are filing this petition to initiate an expedited rulemaking proceeding under Section 107(b) of CALEA and related provisions. They are taking this step because, after careful consideration and consultation, they have determined that the interim technical standard adopted by industry is seriously deficient. In the view

of the Department of Justice, the FBI, and other federal, state and local law enforcement agencies, the industry's interim standard is not adequate to ensure that law enforcement will receive all of the communications content and call-identifying information that carriers are obligated to deliver under Section 103 and the applicable electronic surveillance statutes. The interim standard also fails to ensure that information will be delivered in a timely manner. Unless the deficiencies in the interim standard are corrected by the Commission, information that is critical to public safety and law enforcement will be lost, and Congress' goal of preserving the surveillance capabilities of law enforcement agencies in the face of technological changes will be seriously compromised.

This petition explains why the industry's interim standard is deficient and what services and features should be added to correct its deficiencies and carry out the mandates of CALEA. The petition is accompanied by a proposed rule that sets forth, in specific terms, the changes that the petitioners believe should be adopted by the Commission. The petitioners request that the Commission initiate an expedited rulemaking proceeding leading to the adoption of the proposed rule and any other requirements and standards that the Commission determines to be appropriate under Section 107(b).

I. INTRODUCTION

1. The Department of Justice and the FBI, on behalf of themselves and other federal, state, and local law enforcement agencies,[1] respectfully request the Commission to initiate an expedited rulemaking to establish technical requirements or standards for electronic surveillance assistance by telecommunications carriers under the Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. and 47 U.S.C.). This petition is filed pursuant to Sections 103 and 107(b) of CALEA (47 U.S.C. §§ 1002 and 1006(b)), Sections 4(i) and 229(a) of the Communications Act of 1934 (47 U.S.C. §§ 154(i) and 229(a)), and Section 1.401(a) of the Commission's rules (47 C.F.R. §1.401(a)).

2. Section 103 of CALEA (47 U.S.C. § 1002) imposes affirmative obligations on telecommunications carriers to ensure that their equipment, facilities, and services are capable of providing specified assistance to law enforcement in the conduct of authorized electronic surveillance. Under Section 107(a) of CALEA (47 U.S.C. § 1006(a)), a carrier is deemed to be in compliance with Section 103 if it is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization to meet the requirements of Section 103. However, compliance with the industry standard is merely one way

---

[1] Following passage of CALEA, the FBI assembled the Law Enforcement Technical Forum ("LETF"), consisting of 21 representatives from federal agencies and 30 from state and local law enforcement agencies, as well as the Royal Canadian Mounted Police. LETF members participated in the development of this petition. In turn, the FBI and the LETF have coordinated CALEA implementation issues, and developed consensus positions, with several hundred of the major law enforcement agencies and prosecutors' offices across the United States.

of assuring compliance with Section 103; a carrier can satisfy its obligations by any means that meet Section 103's underlying assistance capability requirements. Moreover, if a government agency believes that technical requirements or standards adopted by an industry association or standard-setting organization are deficient, it may petition the Commission under Section 107(b) (47 U.S.C. § 1006(b)) to establish, by rule, technical requirements or standards that meet the requirements of Section 103.

3. On December 8, 1997, the Telecommunications Industry Association (hereafter referred to as "TIA") published an interim technical standard ("interim standard") concerning electronic surveillance assistance requirements for telecommunication carriers providing wireline, cellular, and personal communications services. This petition is being filed because the interim standard lacks specified electronic surveillance assistance capabilities and related provisions that are required by CALEA. The Department of Justice and the FBI ask the Commission, by rule, to supplement the interim standard by incorporating additional capabilities and provisions that will satisfy the requirements of Sections 103 and 107(b) of CALEA. A proposed rule that sets forth requested technical requirements and standards is contained in Appendix 1 of this petition.

4. The technical requirements and standards sought in this petition are intended to operate in addition to, not in lieu of, the interim standard. Thus, the interim standard should not be stayed pending a determination of this rulemaking.

5. The Department of Justice and the FBI urge the Commission to consider this matter on an expedited basis so that the deficiencies of the interim standard can be corrected as soon as possible. Expedited consideration will further the strong public safety interest in preserving law enforcement's ability to conduct effective, lawfully authorized electronic surveillance in its continuing efforts to combat criminal activity. Expedited consideration also will help to avoid delay in the development, manufacture, and deployment of CALEA-compliant solutions for existing and future equipment so that law enforcement agencies can effectively fulfill their public functions.

II. BACKGROUND

6. This petition concerns statutory obligations placed on telecommunication carriers by CALEA. To understand fully the nature and scope of those obligations, it is essential to understand the background of this legislation. As described below, CALEA was passed primarily at the behest of the FBI and other law enforcement agencies, despite opposition from the telecommunications industry, in order to ensure that lawful electronic surveillance as an invaluable crime-fighting tool is not thwarted by technological and structural changes in the telecommunications industry. CALEA is designed to preserve the ability of federal, state, and local law enforcement agencies to carry out lawful surveillance in the face of these changes.

A. Pre-CALEA Electronic Surveillance

7. For many decades, law enforcement agencies have been able to employ court-ordered electronic surveillance successfully in collecting evidence in criminal investigations. The principal statutory authority allowing these agencies to conduct electronic surveillance is contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter "Title III"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA") (codified at 18 U.S.C. §§ 2510 et seq.). In 1986, Congress modified Title III in order to update its provisions and clarify federal privacy protections and electronic surveillance standards in light of changes in computer and telecommunications technologies. In addition, Congress added a court order requirement for "pen registers" and "trap and trace" devices. (18 U.S.C. §§ 3121 et seq.).[1] ("Pen registers" do not intercept the contents of calls, but instead record outgoing dialed digits, tones, and any other signals from a subscriber's telecommunications equipment or facilities; "trap and trace" devices provide information concerning the origination of incoming calls.)

8. Title III imposes significant responsibilities on law enforcement officers in order to protect privacy to the maximum extent possible while allowing evidence gathering through electronic surveillance. For example, a law enforcement agency is obligated to demonstrate that other practical investigative techniques are unavailing before seeking electronic surveillance authorization (18

[1] The history of federal wiretap legislation is described in the Commission's Notice of Proposed Rulemaking in In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 97-356 (released Oct. 10, 1997), at 4-8 (cited hereafter as "FCC Notice").

U.S.C. § 2518(3)(c)), and it must minimize interception of non-criminal conversations (18 U.S.C. § 2518 (5)). In addition, tapes of intercepted communications must be sealed at the end of the interception period (18 U.S.C. § 2518(8)), and only authorized disclosures of such material are permitted (18 U.S.C. §§ 2511(1)(c) and 2517).

9. Law enforcement agencies have often conducted electronic surveillance with the assistance of the telecommunications industry, but sometimes have been forced to proceed without the industry's cooperation. In some instances, certain service providers have refused to render needed assistance to law enforcement officers even when surveillance was judicially authorized. See, e.g., Application of United States, 427 F.2d 639 (9th Cir. 1970). In light of this problem, in 1970, Congress amended Title III to make clear the responsibility of telephone service providers to provide assistance to law enforcement personnel. Specifically, Congress amended Title III to provide that interception orders shall "direct that a provider of wire or electronic communication service * * * shall furnish the applicant [for the order] forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider * * * is according the person whose communications are to be intercepted." 18 U.S.C. § 2518(4).

10. Despite the 1970 amendments to Title III, telephone service providers have continued in certain instances to refuse full cooperation for criminal investigations, forcing law enforcement officials to seek compulsion from the courts. See, e.g., United States v. New York Telephone Co., 434 U.S. 159 (1977) (compelling telephone company to provide assistance to the FBI in installing

pen registers); United States v. Mountain States Telephone and Telegraph Co., 616 F.2d 1122 (9th Cir. 1980) (compelling telephone company to program computerized electronic switching equipment so that the IRS could determine numbers from which incoming calls to target were being made); Michigan Bell Telephone Co. v. United States, 565 F.2d 385 (6th Cir. 1977) (compelling telephone company to employ both manual and electronic tracing devices on specified telephones).

11. Prior to 1984, the great majority of local and long distance telecommunications were carried by AT&T, which held a virtual monopoly on these services. This dominance resulted in a largely homogeneous telephone network in which the technology of the equipment used to conduct business was generally uniform throughout the network. The telephone system was largely based on "analog" technology, which converted voices into electronic patterns that mimic natural sound waves. The electronic impulses would then travel over copper wires, and were directed to the receiver by electronic contact switches. Law enforcement agents were consistently able to conduct electronic surveillance by gaining access to telephone lines between the service provider's central office and a telephone subscriber's home or office (the "local wire loop"). These interceptions were highly effective for the existing technologies, and law enforcement agents were able to intercept the content of all communications supported by a subscriber's service or carried over the subscriber's facilities, as well as information concerning the nature of any calls (such as from which numbers they came and to which numbers they went). In addition, these agents could verify the accuracy, integrity, and operability of the surveillance throughout the interception period.

12. Thus, until fairly recently, law enforcement officers could obtain all information available to the telephone service provider concerning use of the services that it rendered to a particular subscriber, including when and to which numbers calls were made, when and from which numbers calls were received, and the complete contents of those calls. In other words, everything then technologically possible to know about the telephone service being provided was available to authorized law enforcement officers. Further, there were no technological limitations on the number of interceptions that could be conducted.

13. This situation changed considerably and rapidly in the past 20 years, particularly following the breakup of AT&T in 1984. The number of long distance and local service providers has increased dramatically, and this number has expanded even further with the advent of wireless technologies. Law enforcement agencies must now deal with well over one thousand different telecommunications service providers who are employing a host of new technological developments. These developments are possible in part because analog technology is being replaced by digital technology, under which a communication is converted by computer into streams of binary data representing the digits “0” and “1”. Rather than being routed by an electrical contact switch, a call is typically routed by a computer at the carrier’s switching facility.

14. As this petition indicates, the development of new telecommunications technologies has provided subscribers with a range of new services that enable them to accomplish tasks with their telephone systems that could not be done before. For example, in the past decade or so, the following services became widely available to subscribers: call forwarding; call transferring; direct

implementation by a subscriber of new services; voice-activated dialing and speed dialing from the service provider's centralized facility; the ability to have voice "mail box" message systems accessed by a subscriber; and the ability to initiate a multi-party call and then depart, leaving the other parties still connected.

15. These new telecommunications technologies allow for the efficient transmission of multiple, simultaneous communications of various subscribers over fiber optic lines and wire facilities. Features such as call forwarding permit customers to redirect calls, thereby no longer requiring that communications be transmitted to the same specific location or through the same wire line loop. Likewise, "follow me" features expand the nature of call forwarding to national dimensions. And personal communications services enable users to define their own set of subscribed services, use any fixed or mobile terminal or telephone instrument, and make and receive calls across multiple networks without regard to their location. All of these services have removed a telephone subscriber from a fixed local wire loop that could be tapped by law enforcement agents, and thereby have greatly hampered the ability to conduct court approved electronic surveillance. See also FCC Notice at 10 ("In addition to the proliferation of services currently offered, the increase in the sheer number of service providers further complicates efforts to conduct the authorized implementation of electronic surveillance").

16. Moreover, as new technology is deployed, the principal technique used for electronic surveillance of telecommunications will also change. In the past, law enforcement officers typically utilized their own equipment physically to tap into an existing wire leading to a subscriber's house

or business. However, with the advent of digital transmissions and the use of a telecommunications carrier's computer to provide services at a centralized point, electronic surveillance will often be accomplished through the use of software employed by the carrier to route authorized information to law enforcement officers.

B. The Enactment of CALEA

17. In March 1994, FBI Director Freeh informed Congress that the telecommunications technological revolution was having a devastating impact on the ability of law enforcement officers to carry out their essential electronic surveillance duties. See Joint Hearings on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House of Representatives Comm. on the Judiciary, 103d Cong., 2d Sess. 5-6, 14 (March 18, 1994) (statement of Louis J. Freeh). Director Freeh explained to Congress that "[i]ndustry representatives have bluntly told law enforcement that the existing telecommunications systems and networks will thwart court authorized intercepts" (id. at 24). The developments in telecommunications technology "often prevent, and will continue to prevent common carriers from providing law enforcement with access to all of the communications and dialing information that are the subject of electronic surveillance and pen register court orders" (id. at 24). The telecommunications industry had been telling the FBI that "there is a serious problem, and they have been forecasting that within a very short period of time they will not be able to service

our court orders" (id. at 9); "they will not have in the switches the software necessary to make the connections to give us the access" (id. at 10).

18. In addition, based on a survey, Director Freeh pointed out that it was estimated that in the prior decade several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated or were not sought, in whole or in part, because of various technological impediments (id. at 24, 37).

19. Director Freeh noted that this problem was becoming quite serious for the public safety because "the nation's telecommunications networks are routinely used in the commission of serious criminal activities, including terrorism and espionage. Organized crime groups and drug trafficking organizations, which are often highly structured, rely heavily upon telecommunications to plan and execute their criminal activities and hide their illegal proceeds" (id. at 16). Accord id. at 6, 7-8.

20. The changes in the telecommunications industry have had such a great impact on law enforcement because, as Director Freeh explained, court-authorized electronic surveillance is "one of its most important investigative techniques — if not the most important. Use of the technique has been critical in fighting organized crime, drug trafficking, public corruption, fraud, terrorism, and violent crime, and in saving numerous innocent lives. In many of these cases, the criminal activity under investigation could never have been fully detected, prevented, adequately investigated, or successfully prosecuted without the use of evidence derived from court-ordered electronic surveillance" (id. at 17). Accord id. at 6, 8.

21. For example, Director Freeh described how electronic surveillance had allowed the FBI to intercept conversations in which Mafia members planned three murders, two of which the Bureau was able to prevent. And, court-ordered electronic surveillance allowed FBI agents and police officers in 1990, to learn about and stop a planned "shoot out" between rival Asian gangs in New York. Further, in 1990, relying heavily upon electronic surveillance, the FBI thwarted two individuals conspiring to abduct, torture, and kill a teenage boy for a "snuff murder" film. Id. at 20-21. Director Freeh also noted instances in which electronic surveillance helped solve outstanding criminal investigations, including one in 1991 of the murder of a United States court of appeals judge. Id. at 20-21.

22. Director Freeh pointed out to Congress how the Federal Government had been attempting since 1992 to work with telecommunications industry personnel at all levels to resolve the problems being caused for law enforcement agencies by the changes in the industry. The Government learned through these discussions that the needs of law enforcement were not being incorporated into carriers' system requirements, and several industry executives made clear that these needs would be met only if there were legislation so requiring. Id. at 25. The Government therefore began a legislative initiative in 1992, but met with industry resistance. Discussions between law enforcement agencies and industry officials continued, and industry representatives "recognize[d] the problems and impediments that [new] telecommunications technologies are creating for law enforcement" (id. at 26). Eventually, the Federal Government determined that comprehensive legislation was needed, and the Clinton Administration therefore proposed a bill in 1994.

23. Director Freeh explained that the purpose of the Administration's legislative initiative was "to maintain technological capabilities commensurate with existing statutory authority — that is, to prevent advanced telecommunications technology from repealing *de facto* the statutory authority already conferred by the Congress" (id. at 27) to carry out electronic surveillance. "With court approval, law enforcement is now technically able to wiretap on the old technology. We simply seek to ensure a failsafe way for law enforcement to conduct court-authorized wiretapping on the recently deployed and emerging technology" (id. at 6).

24. When legislation was initially proposed, there was concern that the Administration had not sufficiently demonstrated the existence of a problem. Therefore, the FBI conducted a new survey of federal, state, and local law enforcement officials, and presented further evidence to committees from both Houses of Congress in April 1994. See H.R. Rep. No. 103-827, 103d Cong., 2d Sess. 14-15 (1994), reprinted at 1994 U.S. Code Cong. & Admin. News (USCCAN) 3489 (cited hereafter as "House Report"). Following receipt of these data, "representatives of the telecommunications industry * * * acknowledge[d] that there will be increasingly serious problems for law enforcement interception posed by new technologies and the new competitive telecommunications market." Id. at 15; accord, 140 Cong. Rec. H10782 (Oct. 4, 1994) (Rep. Edwards) (the FBI "did their homework, and they proved there is a problem"); FCC Notice at 9-10 ("Call forwarding, three-way conferencing, voice recognition calling, digital features, and cellular services were specifically identified as making electronic surveillance difficult or impossible to conduct").

25. Following further hearings in August and September 1994, a bill "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes" (House Report at 1) was favorably reported in both Houses of Congress.[1] The bill was passed by Congress and signed into law by the President as the Communications Assistance for Law Enforcement Act (CALEA) on October 25, 1994. Pub. L. No. 103-414, 108 Stat. 4279 (1994).

26. The Judiciary Committees in the House of Representatives and the Senate explained that the purpose of CALEA "is to preserve the government's ability pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services." House Report at 9. Congress made clear that it intended to pay carriers for their reasonable costs incurred in modifying existing equipment to comply with new capability requirements, and for expansions in capacity to accommodate law enforcement needs. Id. at 10.

27. The Congressional reports on CALEA recognize the problems described by Director Freeh and others and the need for federal legislation to impose a requirement of cooperation on the telecommunications industry. House Report at 10-16; see also 140 Cong. Rec. H10782 (Oct. 4,

[1] Because joint Senate and House hearings on this proposed legislation were held, the Senate report on the legislation (S. Rep. No. 103-402, 103d Cong., 2d Sess. (1994)) is very similar to the House report. For simplicity, in this petition we cite only to the House report.

1994) (Rep. Oxley) ("Currently, the telecommunications industry is undertaking revolutionary changes in its technology, changes that could make it impossible for police agencies to execute lawful court orders. In some instances, cellular technology and new digital features have already frustrated court ordered wiretaps").

28. To meet this need, Congress designed CALEA to "require[] telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance. The bill will preserve the government's ability, pursuant to court order, to intercept communications that utilize advanced technologies such as digital or wireless transmission." House Report at 16. Congress made clear that its intent in imposing assistance requirements on telecommunications common carriers was "to preserve the status quo." House Report at 22.[1] CALEA was intended to "allow the FBI and Federal law enforcement to follow the exact same laws we have today and the same rules we have today, to be able to conduct wiretaps in kidnaping cases, national security cases and others." 140 Cong. Rec. S13999 (Oct. 4, 1994) (Sen. Leahy); accord FCC Notice at 9 ("Congress passed CALEA to preserve the ability of law enforcement officials to conduct

[1] The House report stated that in preserving the ability of law enforcement agencies to continue to conduct effective electronic surveillance, "[t]he Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling" and that it "expects industry, law enforcement and the FCC to narrowly interpret the requirements" (id at 22-23). Thus, Congress did not want the Commission to expand the requirements legislatively imposed through CALEA. As we describe in the discussion section of this petition, the capabilities being sought by law enforcement are those required by CALEA's language, and thus fit within a "narrow" interpretation of the statute's requirements.

authorized electronic surveillance in the face of the recent, rapid, technological changes in telecommunications that threaten their ability to intercept communications").

29. At the same time that Congress was compelling telecommunications carriers to assist law enforcement in carrying out electronic surveillance successfully, it intended CALEA to provide further privacy protections for specified types of communications,[1] and to ensure that compliance with the requirements of law enforcement would not impede the development and deployment of new technologies and customer services. House Report at 17-19. In addition, "[t]he legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements." House Report at 22-23.

30. For purposes of this petition, the central part of CALEA is Section 103(a) (47 U.S.C. § 1002(a)), which mandates that telecommunications carriers "shall ensure" that their equipment, facilities, or services are capable of expeditiously isolating and delivering intercepted communications and call-identifying information to law enforcement agencies. See FCC Notice at 10-11 ("While carriers have been required since 1970 to cooperate with law enforcement officials' efforts to conduct court-authorized electronic surveillance (see 18 U.S.C. § 2518(4)), the question

---

[1] Among other matters, Congress added privacy protections by limiting the nature of the data that can be obtained through pen registers and certain other types of surveillance, changing the nature of the order needed to obtain electronic mail addresses and communications, extending privacy protections to cordless telephones and certain data communications transmitted by radio, and stating explicitly that the statute does not limit the rights of subscribers to use encryption. See House Report at 17-18.

of whether carriers have an affirmative obligation to design or modify their systems to accommodate such surveillance has never been adjudicated. CALEA for the first time imposes such an affirmative obligation upon telecommunications carriers" (footnote omitted)).

31. Under Section 103(a) (47 U.S.C. § 1002(a)), each telecommunications carrier "shall ensure" that its "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications" are "capable of":

> (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier—
>
> > (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
> >
> > (B) in a manner that allows it to be associated with the communication to which it pertains,
>
> except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices, * * * 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.

32. CALEA thus does not expand law enforcement agencies' power or authority to conduct electronic surveillance; that authority continues to be defined principally by Title III. CALEA was instead designed to enable law enforcement agencies to keep pace with rapidly changing telecommunications technologies by preserving law enforcement officers' access to all communications authorized to be intercepted and by making available the same kinds of information about a subscriber's services and their use that has always been available to law enforcement officers. At the same time, CALEA protects important privacy interests of legitimate telephone users.

C. Post-Enactment Developments

33. Congress recognized that implementation of the assistance capability requirements in Section 103 would require a cooperative effort between law enforcement and industry. Therefore, Section 107(a)(1) of CALEA (47 U.S.C. § 1006(a)(1)) provided for the Attorney General to "consult" with appropriate standard-setting organizations of the telecommunications industry and other interested groups "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements."

34. Immediately after CALEA was enacted, the FBI engaged in extensive discussions with telecommunications industry representatives. In May 1995, a subcommittee of the industry TIA Standards Committee (Subcommittee TR45.2) began discussing the development of a standard electronic surveillance scheme to meet the CALEA requirements. Based on these discussions, and in response to industry requests for detailed technical specifications of its requirements, the FBI in 1996 published its Electronic Surveillance Interface Document, setting forth recommended technical specifications to meet the assistance capability requirements it believed to be required by Section 103 of CALEA.[1]

35. The FBI maintained that any CALEA-based standard should require telecommunications carriers to provide, in addition to other basic functions, a number of specific assistance capabilities. Among other things, the FBI sought provisions that would provide:

> — Access to the communications of all parties in a conference call supported by the subscriber's service or facilities;
>
> — Access to all subject-initiated dialing and signaling activity;
>
> — Information indicating whether a party is connected to a multi-party call at any given time ("party hold," "party join," and "party drop" messages);
>
> — Notification messages for in-band and out-of-band signaling;
>
> — Timely delivery of call-identifying information;
>
> — Automated reporting of surveillance status;
>
> — Delivery of all call-identifying information over call data channels; and

---

[1] See Electronic Surveillance Interface Document, Issue 1.0, Federal Bureau of Investigation (June 24, 1996), attached hereto as Appendix 2.

— A limited number of standardized delivery interfaces.

These provisions are discussed below and described more fully in Law Enforcement Ballot Comments to SP-3580 A (October 28, 1997), attached hereto as Appendix 3. The FBI sought these provisions in order to provide law enforcement agencies with essentially the same type of information they have historically been able to acquire so that they can continue to conduct electronic surveillance effectively in a carrier-controlled, switch-based or network-based surveillance environment.

36. In February 1997, TIA Subcommittee TR45.2 released its Lawfully Authorized Electronic Surveillance (LAES) standards document ("SP-3580") and put it to ballot. The SP-3580 proposed standard did not address any of the capabilities and provisions listed above. A number of law enforcement agencies, believing that SP-3580 was inadequate because it did not address these essential electronic surveillance capabilities, voted against adoption of the document. In addition, the law enforcement community submitted extensive ballot comments identifying the deficiencies of SP-3580. TIA then submitted a revised standard, called SP-3580A, which law enforcement representatives again opposed because it did not include the referenced capabilities. In July 1997, over the objection of law enforcement representatives, TIA established a parallel track in which an identical standards document, still without the referenced capabilities, was renamed as document PN4116 and sent to ballot as proposed interim standard TIA/EIA/IS-J-STD-025 ("J-STD-025"). Only industry votes were counted, even though all submissions, including 184 opposing submissions from the law enforcement community, ostensibly were "considered" by TIA Subcommittee TR45.2.

37. On December 8, 1997, TIA adopted J-STD-025 as an interim standard.[1] The interim standard fails to include any of the electronic surveillance capability requirements described above. After careful review, the Department of Justice has determined that the failure of the interim standard to include these provisions renders it deficient as a means of carrying out Section 103 of CALEA and the Congressional purposes underlying CALEA.[2]

38. Congress anticipated that standards adopted by industry might prove inadequate to carry out Section 103. Section 107(b) of CALEA therefore provides for any government agency (or other person) that believes an industry standard to be deficient to petition the Commission to establish, by rule, technical requirements and standards. Section 107(b) authorizes the Commission to establish technical requirements and 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 * * * ." 47 U.S.C. § 1006(b)(1).

---

[1] The title page and table of contents of J-STD-025 are attached hereto as Appendix 4 with permission from TIA. TIA has forwarded a document identical in substance to J-STD-025, denominated TIA SP3580A, to the American National Standards Institute for adoption as a national standard.

[2] See Letter of February 3, 1998 from Stephen R. Colgate, Assistant Attorney General, to Mr. Tom Barba, Steptoe & Johnson, attached hereto as Appendix 5.

39. The Attorney General and other Department of Justice officials have continued meeting with telecommunications industry representatives over the past few months in an effort to persuade industry that the interim standard fails to meet the requirements of CALEA and to arrive at standards that satisfy those requirements. However, these discussions have proven unsuccessful. Consequently, the Department of Justice and the FBI are filing this petition to invoke the authority and assistance of the Commission in an expedited rulemaking proceeding.

III. DISCUSSION

A. THE COMMISSION SHOULD ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS THAT MEET THE REQUIREMENTS OF CALEA

1. The Commission Has the Authority To Entertain This Petition and Grant the Relief Requested

40. As noted above, Section 107(b) of CALEA (47 U.S.C. § 1006(b)) vests the Commission with the authority to issue a rule establishing technical requirements or standards that meet the assistance capability requirements of Section 103 of CALEA. A government agency may petition for such a rule if it believes that a "publicly available technical requirement or standard adopted by an industry association or standard-setting organization" under Section 107(a)(2) of CALEA is deficient. In this case, the TIA interim standard is a "publicly available technical requirement or standard adopted by an industry association or standard-setting organization * * * to meet the requirements of section 103," and the Department of Justice and the FBI have concluded, for reasons discussed below, that the interim standard is deficient in significant respects. The Commission therefore has the authority under Section 107(b) to entertain this petition and establish appropriate technical requirements or

standards by rule. See FCC Notice at 65 ("The Commission may * * * establish technical standards or requirements * * * if a government agency or any other person believes that any standards issued [by industry] are deficient.").

41. The Commission is also authorized to issue a rule in this proceeding by Sections 4(i) and 229(a) of the Communications Act of 1934 (47 U.S.C. §§ 154(i) and 229(a)). Section 4(i) gives the Commission the general authority to "make such rules and regulations, and issue such orders, not inconsistent with [the Act], as may be necessary in the execution of its functions." 47 U.S.C. § 154(i). Section 229(a), which was added to the Communications Act by Section 301 of CALEA (108 Stat. 4292-93), specifically provides that "[t]he Commission shall prescribe such rules as are necessary to implement the requirements of" CALEA. Id. § 229(a). The authority conferred on the Commission by Section 4(i) and Section 229(a) of the Communications Act complements the authority conferred by Section 107(b) of CALEA.[1]

2. Action by the Commission Is Needed To Correct the Deficiencies of the TIA Interim Standard and Meet the Requirements of CALEA

42. Congress enacted CALEA "to preserve the ability of law enforcement officials to conduct authorized electronic surveillance in the face of the recent, rapid technological changes in

---

[1] Section 1.401(a) of the Commission's rules (47 C.F.R. § 1.401(a)) provides that "[a]ny interested person may petition for the issuance, amendment or repeal of a rule or regulation." The Department of Justice, the FBI, and other members of law enforcement are "interested persons" within the meaning of Section 1.401(a).

telecommunications that threaten their ability to intercept communications." FCC Notice at 9. For reasons set forth below and in the attachments to this petition, the TIA interim standard is not adequate to meet this statutory mandate. If the deficiencies in the interim standard are not cured, the ability of federal, state, and local law enforcement agencies to carry out lawfully authorized electronic surveillance will be seriously impaired, with potentially significant harm to public safety and law enforcement. The Commission therefore should supplement the interim standard with additional technical requirements and standards that satisfy the requirements of CALEA.

43. This petition identifies a number of provisions that have been omitted from the interim standard and that should be included in technical requirements and standards established by the Commission. Each of these provisions is set forth in the proposed rule that accompanies this petition (see Appendix 1). Adoption of the provisions of the proposed rule will cure the deficiencies in the interim standard, "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)), and satisfy the other criteria of Section 107(b) (47 U.S.C. § 1006(b)(2)-(5)).

44. In the discussion that follows, we address the deficiencies in the interim standard and explain the corresponding provisions of the proposed rule. Each provision of the proposed rule relates to one or more capabilities that are missing from the interim standard and that must be met under Section 103. In some instances, the capabilities missing from the interim standard can be implemented only in one way, and the provisions of the proposed rule represent the only means of satisfying the capability in question. In other instances, which we note below, the capabilities

missing from the interim standard could be implemented in more than one way. In those instances, the provisions of the proposed rule are intended to represent the most effective means (although not necessarily the only means) by which the capability can be carried out.

45. In many respects, the provisions of the proposed rule concern communications and call-identifying information that law enforcement historically has received. In other respects, which are noted specifically below, the provisions of the proposed rule will result in the delivery of call content and call-identifying information that law enforcement has not previously received, either because law enforcement was technically impeded from accessing the services or because the services were not available to the subscribers in the past. By its terms, Section 103 of CALEA obligates carriers to provide law enforcement with "all wire and electronic communications * * * to or from equipment, facilities, or services of a subscriber" and "call-identifying information that is reasonably available to the carrier"; Section 103 does not restrict this obligation to those communications and call-identifying information that were accessible to law enforcement in the pre-digital era. More generally, the language and legislative history of CALEA make clear that Congress intended for the electronic surveillance capabilities of law enforcement to keep pace with technological developments in the telecommunications industry. As technological changes have made possible new communications services, new information is generated regarding the use of such services by subscribers. Law enforcement cannot preserve the status quo in a meaningful sense unless it is able to obtain such information and thereby keep pace with the evolution of services and technologies. Moreover, all of the call content and call-identifying information at issue in this petition can lawfully be acquired by law enforcement pursuant to Title III surveillance orders and pen register orders, and

the failure to adopt the proposed requirements and standards will thus result in the inability of law enforcement to obtain information that it is legally entitled to acquire.

46. **(a)** Ability to intercept the communications of all parties in a conference call supported by the subscriber's service or facilities. Under Section 103(a)(1) of CALEA, telecommunications carriers are obligated to ensure that their equipment, facilities, and services are capable of " expeditiously isolating and enabling the government * * * to intercept * * * 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 * * * ." 47 U.S.C. § 1002(a)(1) (emphasis added). The TIA interim standard does not satisfy this requirement because it does not ensure the ability of law enforcement to intercept all of the communications of all parties in a conference call supported by the subscriber's service or facilities.

47. At the outset, we wish to be clear about the meaning of several terms used in our discussion of this issue and related issues in this petition. When we refer to "subscriber," we are referring to the person or entity whose "equipment, facilities, or services" (47 U.S.C. § 1002(a)) are the subject of an authorized law enforcement surveillance activity. The subscriber often will be a person or entity suspected of criminal activity, but in some instances, the subscriber will simply be someone whose relationship to a suspected criminal (e.g., spouse or employer) makes it likely that criminal activity will be transacted or discussed over the subscriber's facilities. When we refer to "intercept subject" or "subject," we are referring to any person who is using the subscriber's equipment, facilities, or services, and whose conversations (or dialing activity) therefore would be capable of

being acquired during an interception. In a particular investigation, the "intercept subjects" could include the subscriber, who may or may not be involved in criminal activity; a non-subscriber who is not involved in criminal activity; or a non-subscriber who is involved in criminal activity. As explained below, to the extent that innocent persons are intercept subjects, their interests are protected by Title III's minimization requirements.

48. Title III does not require the subscriber to be "on the line" in order for law enforcement lawfully to intercept communications taking place over the subscriber's facilities or supported by the subscriber's service. With the exception of "roving wiretaps" (see 18 U.S.C. § 2518(11)), interception orders under Title III are directed at particular telecommunications facilities, not at the subscriber, who may not even be a target of the investigation. An interception order must specify "the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted." 18 U.S.C. § 2518(4)(b); see also id. § 2518(1)(B)(ii).[1] But the government is not required to show that the subscriber whose facilities are to be monitored is involved in any way with the criminal activity at issue. Instead, the government need only show probable cause to believe that the facilities "are being used, or are about to be used, in connection with the commission

---

[1] Although Congress did not define "facility," it is used throughout Title III to describe the thing to be searched, or the communications pathway where the communications are to be intercepted. In practice, the facility is described by the subscriber's telephone number, which would entail network facilities that support and are identifiable with the service associated with that telephone number. It is commonly accepted within the telecommunications industry that "facility" includes numerous components within the entire transmission path over which a communication travels from one conversing party to another. For example, "Facility" is defined as the "[t]ransmission path between two or more points provided by a common carrier." North American Telecommunications Association, INDUSTRY BASICS (4th ed.).

of [the specified] offense, or are leased to, listed in the name of, or commonly used by" the intercept target(s). Id. § 2518(3)(d) (emphasis added). With some frequency, Title III orders are issued for facilities of a subscriber who has some connection with a person suspected of criminal activity but who has no involvement in the criminality himself (e.g., an employer, neighbor, or relative).

49. Neither does Title III confine the government to communications in which the individual under investigation is taking part. When the government executes an interception order, it may intercept any communications carried over the facilities covered by the order that relate to the criminal activity under investigation and are otherwise within the scope of the order, even if the individual under investigation does not participate in such communications. See United States v. Kahn, 415 U.S. 143 (1974); see also 18 U.S.C. § 2518(4)(a) (interception order need not specify the identities of the persons whose communications are to be intercepted if the identities are not known). The government is, of course, obligated to "minimize the interception of communications not otherwise subject to interception" under Title III. 18 U.S.C. § 2518(5).[1] But this minimization obligation means only that the government must minimize the interception of communications that are unrelated to criminal activity; it does not mean that the government is foreclosed from intercepting communications that do involve criminal activity merely because they do not involve a particular investigatory target.

---

[1] Minimization is ordinarily effected by manually discontinuing the interception and recording of conversations when criminal conduct is not being discussed.

50. In the context of traditional two-party "plain old telephone service" (POTS), telecommunications historically have been accessible at any place within the local loop associated with a call. Thus, any communication that could be "tagged" or identified as connected to a particular subscriber's telephone service would be technically subject to interception, regardless of who is being intercepted over that service.

51. POTS is being replaced by telephone services with greater functionality, including conference calling capabilities, which allow a subscriber (or other person using the subscriber's services) to join several different parties, each on a separate "leg" of the call, in one call. Title III interception orders authorize law enforcement to acquire all criminal communications of all parties conversing over the subscriber's facilities or services, including communications on any "leg" of a conference call at all times. Under the TIA interim standard, however, law enforcement would be able to intercept only those communications occurring over the leg of the call to which the subscriber's terminal equipment is actually connected to each leg of the call at any point in time. As long as the subscriber's terminal equipment is connected, law enforcement could monitor all legs of the call. But law enforcement would have no access to certain communications supported by the subscriber's service or carried over the subscriber's facilities in the event that the person using the subscriber's services placed some of the conferenced parties on hold or dropped off the call. This does not amount to a reduction in the information that has been available to law enforcement under POTS, but as we show below, it nevertheless falls short of carrying out the legal obligations imposed by Section 103 of CALEA.

52. Under the interim standard, an intercept subject might initiate a conference call with two associates, A and B, then place A and B on hold while answering an incoming call. A and B could continue talking while the subject speaks to the incoming caller on another line. Law enforcement would not receive the content of the conversation between A and B, even though that conversation is being supported by the subscriber's service or carried by the subscriber's facilities, may legally be intercepted under the Title III order, and is pertinent to the criminal activity under investigation.

53. The failure to provide law enforcement with the communications of all parties in a conference call when some call participants are temporarily placed on hold or the subscriber drops off the call could deprive investigators and prosecutors of important evidence, particularly in conspiracy cases. Participants in a conspiracy may continue to discuss criminal activities among themselves when an intercept subject puts them on hold. Similarly, criminal conversations supported by the subscriber's service or carried over the subscriber's facilities may continue even after the intercept subject hangs up. Without the capability to intercept these conversations, vital evidence that law enforcement is authorized to intercept may be lost.

54. For example, a prisoner who wishes to speak to criminal associates about an ongoing criminal enterprise, such as drug smuggling, can call his girlfriend, the subscriber whose facilities and services are being monitored by law enforcement, and have her bring his associates into a conference call supported by the girlfriend's facilities and services. The girlfriend can then drop off the call while the prisoner and his associates discuss their plans. This particular scenario is one that law enforcement has encountered on multiple occasions and continues to encounter. Under the

interim standard, law enforcement loses its ability to monitor the conversation between the prisoner and his associates as soon as his girlfriend hangs up, even though the conference call is being supported by the girlfriend's service and facilities and the conversation provides direct and otherwise unavailable evidence of continuing criminal activity.

55. The failure of the interim standard to provide law enforcement with access to all communications supported by a subscriber's service or carried over the subscriber's facilities, without regard to the intercept subject's presence on the line, renders the interim standard plainly deficient. As noted above, Section 103(a)(1) of CALEA expressly requires carriers to provide law enforcement with "all wire and electronic communications carried by the carrier * * * to or from equipment, facilities, or services of a subscriber * * * ." 47 U.S.C. § 1002(a)(1) (emphasis added). The communications of all parties, including other criminal associates that are connected (or placed on hold) in a conference call supported by a subscriber's telecommunications service, are therefore squarely within the language of Section 103(a)(1), for the conference call continues to be carried by the subscriber's facilities and supported by the subscriber's service even when the subscriber is not on the line. The House Report specifically states that CALEA was intended "to preserve the government's ability * * * to intercept communications involving * * * services and features such as * * * conference calling." House Report at 9 (emphasis added). Nothing in CALEA requires the subscriber or intercept subject to be "on the line" in order for law enforcement lawfully to intercept communications occurring over the subscriber's facilities or supported by the subscriber's service. And as noted above, Title III similarly focuses on the subscriber's facilities and services rather than

on the participants of the call. Thus, to the extent that industry may believe that Title III does not authorize law enforcement to intercept the communications of parties other than the subscriber or intercept subject in a conference call supported by the subscriber's service or carried over the subscriber's facilities, that belief is mistaken.

56. The proposed rule requires telecommunications carriers to "ensure that their equipment, facilities, or services are capable of providing to law enforcement all content of conferenced calls over a subscriber's equipment, facility, or services * * * ." Appendix 1, § 64.1708(a). The rule defines this capability as "the ability to monitor a multiparty or conference call established by the subscriber's equipment, features, or services where two or more parties are allowed to converse after the subject leaves the conversation, temporarily or permanently." Ibid. This capability is a necessary component of the general assistance capability mandated by Section 103(a)(1) of CALEA and must be included in any technical requirements and standards established by the Commission.

57. **(b)** Access to call-identifying information. The interim standard is also deficient in its provisions regarding access to "call-identifying information." CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunication carrier." 47 U.S.C. § 1001(2). Section 103(a)(2) of CALEA obligates telecommunications carriers to "expeditiously isolat[e] and enabl[e] the government * * * to access call-identifying information that is reasonably available to the carrier

* * * ." 47 U.S.C. § 1002(a)(2). As we now show, the interim standard is deficient because it fails to include assistance capabilities required to satisfy this statutory obligation.

58. Acting pursuant to pen register orders,[1] law enforcement traditionally has acquired all dialing input by the intercept subject and other signaling information relevant to determining the status of a call. This information included certain tones (e.g., call waiting) and signaling information (e.g., the subject's pressing of the flash hook) indicating (1) call waiting, (2) the placing of a party on hold, (3) a conference call, or (4) transfer of a call. By acquiring such dialing and signaling information, law enforcement could identify the final destination of a call, and in many instances who was a party to a call at any given time.

59. Modern telecommunication technology no longer relies on dialed digits as the exclusive means of processing, establishing, controlling, and maintaining calls. Other signaling is switch-based or network-based and occurs at the carrier's central office or elsewhere in the network.[2] The broad definition of "call-identifying information" in CALEA (47 U.S.C. § 1001(2)) is designed to

---

[1] When attached to a subscriber's telephone facilities or service, pen register devices draw in all of the dialing and signaling information that traverses the facilities or service to complete the establishment of a call. Also, these devices print out whether the ringing indicates a busy signal, show the beginning time of call placement ("off hook"), the duration of a call, and the concluding time of a call ("hook"), and also indicates when a called party answers. By definition, a pen register device "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line." 18 U.S.C. § 3121.

[2] In intelligent networks (IN), the routing of calls may be controlled by network elements other than the switch.

ensure, inter alia, that law enforcement has access to the same kind of call processing signaling information to which it always had access through the use of pen registers.[1] By defining "call-identifying information" as "information that identifies the origin, direction, destination, or termination of each communication," Congress demonstrated an intent to provide law enforcement with meaningful information that would enable it to understand the status of the call and identify the parties connected to the call throughout the entire call, not just the fact that a call was initiated or completed.

60. The interim standard falls short of the statutory requirement. While the interim standard provides for the delivery of most call-identifying information associated with the initiation and completion of a call, it omits three vital capabilities relating to call-identifying information. Those capabilities are: (i) access to subject-initiated dialing and signaling activity; (ii) messages indicating whether a party is connected to a multiparty call at any given time ("party hold," "party join," and "party drop" messages); and (iii) notification messages for network-generated in-band and out-of-band signaling. These capabilities are necessary to provide accurate and complete call-identifying information, and they should be incorporated by the Commission in its technical requirements and standards. In addition, the Commission should require that all call-identifying information be delivered over a call data channel. As we explain below, delivery of call-identifying information over

---

[14] Prior to CALEA, law enforcement agencies obtained, pursuant to pen register orders, signaling information that indicated whether the subject had gone "off hook" to initiate a call and information indicating that the subject had gone "on hook" to terminate a call (party release). Hence, law enforcement agencies were able to make sense out of calling efforts through the acquisition of such call-identifying information.

a call data channel may not always be necessary in order for a carrier to perform its assistance capability obligations under Section 103, but doing so represents the most efficient and privacy-enhancing means of discharging those obligations.

61. **(i)** Subject-initiated dialing and signaling activity. When a subscriber receives services such as call forwarding or call transfer, the subscriber or another person using the subscriber's telephone may input dialing or signaling information within a call to control such services. This information may be generated when the subject presses a feature key, such as a hold or transfer key, or when the subject presses the flash hook. For example, a subject who is speaking to one associate (A) may press a transfer key (thereby placing A on hold), call another associate (B), speak to B, then press the transfer key again and drop off the call, leaving A and B to continue the call with each other. The call continues to be supported by the subscriber's service and facilities even after the subject has dropped from the call.

62. The interim standard does not require the delivery of a call data message when the intercept subject inputs dialing or signaling information within a call in this fashion. As a result, under the interim standard, law enforcement will not receive call-identifying information indicating that the intercept subject has, for example, pressed or dialed certain feature keys to manipulate the call. This is information that law enforcement traditionally has been capable of receiving and is legally authorized to receive.[1] Absent a requirement that carriers deliver this information, however, law

---

[1] In the past, law enforcement was able to detect flash hook signaling by detecting recorded changes to the electrical signaling on the analog local loop. In modern digital systems, the

enforcement will lose access to the information in a digital environment, because digital switching prevents law enforcement from having the same access to the intercept hardware or location that it has today.

63. Absent a message indicating that the subject has pressed one of the feature keys or the flash hook, law enforcement will be presented with potentially severe investigative, evidentiary, and prosecutorial problems. Law enforcement may be unable to determine what has happened to a call when the call dramatically changes for no apparent reason. For example, a subject who is engaged in criminal conspiracy with two associates may use his flash hook capability to move back and forth rapidly between the two associates in two concurrent call legs. Without the receipt of a message showing the "flash" event, law enforcement may be unable to follow the course of the conversation or determine to whom the subject is speaking at any point in the conversation.

64. In addition, law enforcement will be left with an incomplete and potentially inaccurate evidentiary picture of the subject's dialing and signaling activities incidental to his calls. The absence of messages indicating dialing or signaling that significantly changes the call would undermine the ability of law enforcement to present critical evidence and testify in court on such fundamental matters as whether the subject was still involved in the call at a particular time; if so, in what fashion; and if not, what happened to the call.

---

equivalent signaling is done via data messaging.

65. CALEA was enacted to prevent the loss of such critical information and evidence. Industry has suggested that dialing and signaling beyond the digit keys and feature codes initiating a call are not "call-identifying information." However, a subject's dialing and signaling inputs during a call that control services like call forwarding and call transfer come squarely within CALEA's definition of "call-identifying information," for they constitute "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2). As explained above, without this signaling information, law enforcement will be unable to identify the destination of each communication. Moreover, CALEA's legislative history makes clear that CALEA was intended "to preserve the government's ability * * * to intercept communications involving * * * features and services such as call forwarding, speed dialing, and conference calling * * * ." House Report at 9. The interim standard is fundamentally deficient in this regard.

66. The interim standard also excludes information about another important kind of subject-initiated dialing and signaling activity: "post-cut-through" dialing. In long distance calls, credit card calls, and (in some instances) local calls, the dialing and signaling information necessary to complete a call and reach the intended party frequently occurs after the "cut-through."[1] For example, when

---

[1] "Cut-through" means the completion of a connection in one direction (partial), or both directions (full), between two call appearances. See Appendix 1 (§ 64.1702). There are two communications paths that must be connected in order for one party to communicate with another party through a telephone switch: the forward talk path and the reverse listen path. Normally, when a call is set up, the caller's reverse listen path is connected to the called party's talk path first, because often the "called party" is an additional switch which may put a busy signal or some announcement on that path. That is referred to as "partial cut-through." When the second switch provides an answer signal to the first switch, because the called party answered or the second switch needs to

using a credit card, a subject may dial through one service (X) to the carrier's (Y's) 800-number service and will then be prompted to continue dialing the telephone number to reach the party being called (i.e., the destination of the call). The numbers dialed are then transmitted over X's equipment, facilities, and services to reach the called party. The numbers dialed after the connection is made to Y's service occur after the "cut-through." Thus, the destination of the call is revealed only by the numbers dialed after the cut-through.

67. The interim standard does not require carriers to provide law enforcement with access to post-cut-through dialing information. Under the interim standard, therefore, law enforcement will not have access to digits dialed after the call is connected. This is information which law enforcement traditionally received in the pre-CALEA POTS environment.[1] Without this information, law enforcement will be unable to determine the destination of some subscriber-initiated calls.

68. The inability to obtain post-cut-through dialing information creates obvious investigative and evidentiary problems. For example, law enforcement agents may find it substantially more difficult,

---

collect additional digits to route the call, the first switch will connect the caller's forward talk path to the called party's listen path. When both paths are connected it is called "full cut-through."

[1] In the analog era, law enforcement obtained information via pulses and tones, which were signaled across the analog local loop to which law enforcement was directly connected. Much of this information is now digitized and therefore not capable of being interpreted by law enforcement through use of a pen register. In addition, information regarding many relatively new features does not pass through to the local loop, but remains accessible only in the switch.

if not impossible, to establish the identity of the party to whom the intercept subject is speaking if they are unable to identify the phone number associated with that party. Thus, in an illegal drug case, law enforcement might be unable to link a drug distributor with the source of his drugs. Similarly, in a child pornography case or other case in which a subject uses the telephone to contact buyers, law enforcement might be limited to the arrest of a single subject rather than all participants, because law enforcement would only have information about which long distance company the subject was using — not the subsequent post-cut-through digits that would have identified the called parties.[1]

69. A carrier's failure to provide law enforcement with all of the subject's dialing, including post-cut-through dialing, amounts to a failure to provide law enforcement with the number of the party that the subject actually called. The failure to mandate access to all dialing and signaling information necessary to complete the call therefore renders the interim standard fundamentally and critically deficient under Section 103 of CALEA. Under CALEA's definition of call-identifying information, post-cut-through dialing and signaling information that completes a call is "signaling information" that identifies the "destination" of the call. 47 U.S.C. § 1001(2). Omission of this information conflicts with the carrier's basic obligation under Section 103(a)(2) to "isolat[e] and enabl[e] the government * * * to access call-identifying information that is reasonably available to

---

[1] Even if law enforcement could eventually obtain the post-cut-through dialing information from the long distance carrier, it would not be accessible in a timely fashion, so as to permit the dialing to be associated with the call content, as required by Section 103(a)(2)(B) of CALEA (47 U.S.C. § 1002(a)(2)(B)). Moreover, a subject could change to a new long distance carrier at the beginning of each call.

the carrier." Id. § 1002(a)(2). It also conflicts with the additional obligation to ensure that call-identifying information is provided "in a manner that allows it to be associated with the communication to which it pertains." Id. § 1002(a)(2)(B).

70. Industry has suggested that its obligation under Section 103 of CALEA ends once a call effort connects, for example, to an 800 calling card service. Law enforcement believes that the Commission has addressed this issue and concluded otherwise. The Commission has recognized that a call is not "completed" when it connects to an 800 calling card service, but rather when it connects to the called party.[1] Under CALEA, therefore, the "call-identifying information" that must be associated with a "communication" includes all dialing required to complete the call.

71. CALEA does not draw any distinction between pre-cut-through and post-cut-through dialing or signaling information used to process, direct, or complete a call. Nor is there any privacy-based constraint under CALEA, the pen register statutes, or the Constitution that prevents a carrier from providing all such dialing information, whether pre-cut-through or post-cut-through.[2] Congress was aware that federal officials have long obtained all dialing information of a criminal subject, including

---

[1] See FCC Report and Order, In re Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, Docket No. 96-388 (Sept. 20, 1996), at 33 ("a 'completed call' is a call that is answered by the called party").

[2] See United States v. New York Telephone Co., 434 U.S. 159 (1977) (dialing information obtained by a pen register device does not constitute the contents of a communication requiring a Title III court order); Smith v. Maryland, 422 U.S. 735 (1979) (no Fourth Amendment protection for dialing information).

post-cut-through dialed numbers, pursuant to pen registers executed in the "local loop," and Congress expressed no intention in CALEA to change this capability. Without such information, law enforcement will be unable to determine the destination of subject-initiated calls. Therefore, access to post-cut-through dialing information is required under CALEA and should be incorporated into technical requirements and standards established by the Commission.

72. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing law enforcement with access to all subject-initiated dialing and signaling, including the use by a subject of flash hooks, feature keys, and all other key usage." Appendix 1 (§ 64.1708(c)). The proposed rule further provides that carriers "shall ensure that their equipment, facilities, or services are capable of extracting the digits dialed by the subject following cut-through at the access point and delivering those digits to the law enforcement agency in a post-cut-through InBandsDigit message containing those digits." Id. (§ 64.1708(i)).

73. **(ii)** Information on participants in a multi-party call. A subscriber may subscribe to services or features that would support a multi-party call. If so, various associates can be added to, placed on hold during, or dropped from a call. The interim standard does not require carriers to provide any signaling information or message indicating that a party has joined a call, been placed on hold, or dropped from a call. The exclusion of this information from the interim standard will deprive law enforcement of important investigative and evidentiary information to which it is lawfully entitled.

74. Law enforcement seeks the delivery of three messages that would provide it with access to information about which parties are participating in a call. A "party hold" message would be generated when any party is placed on hold by the intercept subject. A "party join" message would be generated when (1) one or more parties previously placed on hold are added to the current call or (2) a party joins an existing call with an intercept subject. A "party drop" message would be generated when a party is released from a multi-party call and the call continues among two or more other parties.

75. Party hold, party join, and party drop messages enable law enforcement to identify who is connected in a subject's conference call at any point in the conference. Knowledge of when participants join or depart a call enables law enforcement to identify the source and recipient of each communication within a conferenced call. Without these messages, law enforcement would not know who joins or leaves a conference call, whether the subject alternated between calls, or which parties heard or said parts of a conversation. Such information can be critical for investigatory purposes, particularly in conspiracy cases. For example, if an organized crime leader issues instructions to carry out a murder in the course of a multi-party call, and law enforcement cannot tell which of a number of conferenced associates were participating in the conversation at the time, it may be substantially more difficult to prevent the murder from taking place.

76. In addition, incomplete call-identifying information prevents the collection of evidence that parties remained on a call after they first joined. Thus, if a party remains silent, a law enforcement agency executing a Title III interception order has no way of demonstrating that the party heard

significant portions of the communication. The lack of such evidence may allow doubt to be raised as to whether a party participated in all communications in a call and may jeopardize prosecutions based on that evidence.

77. In the analog environment, law enforcement obtained, pursuant to pen register orders, signaling information indicating that a subject joined other participants in a multi-party call. However, law enforcement was unable to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call, because such information resided within, and required access to, the switch. Law enforcement could therefore identify the range of participants who might be involved in a multi-party call, but would have to infer specifically which participants heard portions of the call. CALEA's definition of "call-identifying information" now obligates carriers to provide this information.

78. Industry has suggested that party join, party hold, and party drop messages do not constitute "call-identifying information" as that term is defined by CALEA. However, Congress chose to define "call-identifying information" as dialing or signaling information that is specific to "each communication" generated or received by a subscriber. 47 U.S.C. § 1001(2). When calls placed to or by a subject are affected by triggering the joining, holding, and releasing of parties, each function essentially has the same fundamental purpose and effect — it controls the "direction," "destination," or "termination" of the communication of each "leg" of the call. Information that enables law enforcement to identify the destination of a call or to understand its status thus falls squarely within CALEA's definition of call-identifying information. Ibid. The interim standard's failure to include

party join, party hold, and party drop messages therefore renders it deficient under Section 103 of CALEA.

79. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing messages to law enforcement that enable law enforcement to identify the parties to a conversation at all times." Appendix 1 (§ 64.1708(b)). The proposed rule defines specific requirements and parameters for "party join," "party hold," and "party drop" messages. Id. § 64.1708(b)(1)-(9).

80. **(iii)** Access to all network-generated in-band and out-of-band signaling. When a call attempt is sent to or from a subscriber's service, it produces network-generated signals such as ringing, busy signals, or a call waiting signal. These signals may be either "in-band" (transmitted over the same circuit as the communication) or "out-of-band" (transmitted over a separate circuit). For subject-originated call attempts, such signals indicate whether the subject ends a call because the associate's line is ringing, busy, or before the network could complete the call to the associate. For incoming call attempts to the subject, the signals indicate whether the subject's telephone was alerted by tones, a visual indicator, or by a text message. Signaling information generated by call attempts has both investigatory and evidentiary significance for law enforcement. For example, criminals may use ringing signals as a way of conveying pre-arranged messages to each other without having to engage in direct conversations over the phone system.

81. The interim standard does not require carriers to provide law enforcement with notification of network-generated call progress signals. This omission is inconsistent with the requirements of Section 103(a)(2) of CALEA, for despite industry's apparent contrary view, such signaling falls squarely within CALEA's definition of "call-identifying information." Call-identifying information includes "signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). A call attempt may "terminate" with ringing (without an answer), a busy tone, or a trunk busy signal; signaling such as this conveys information on call termination and therefore constitutes call-identifying information. Similarly, a network-generated call-waiting tone or a "stutter" dial tone (which indicates that a call was redirected to a voice mail system and a voice mail message was recorded) would identify the "direction" or "destination" of a call, and would therefore constitute call-identifying information. In short, CALEA requires carriers to provide law enforcement with any signaling information indicating how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended. This information historically has been available to law enforcement on call content channels; stutter dial tones and other tones are audible signals sent to the subscriber over the local loop, to which law enforcement has access. However, digital switching and new technology have given rise to network-generated call progress messages that are not available over call content channels.

82. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing notification messages to law enforcement over the CDC [call data

channel] of in-band and out-of-band signaling from the subscriber's service throughout each call." Appendix 1 (§ 64.1708(d)). The rule provides that notification messages "shall be triggered and delivered to the law enforcement agency to report out-of-band signaling delivered through a subscriber's service that can be sensed by the subject and to report in-band signaling applied by the equipment, facilities, or services supporting the subscriber's terminal." Ibid. The rule also defines specific requirements and parameters for notification messages. Id. § 64-1708(d)(1)-(3).

83. **(iv)** Delivery of call-identifying information on call data channel. In the interim standard, industry proposes to deliver certain call-identifying information over "call data" channels or circuits that would be separate from the "call content" channels or circuits that deliver intercepted communications. However, industry has suggested that other call-identifying information, such as the post-cut-through digits described above, need not be provided over the call data channel, but that law enforcement instead should extract that information from a separately leased call content channel.

84. Industry contends that Section 103 does not mandate delivery over a call data channel of call-identifying information that is capable of being extracted from the call content channel. We agree that a carrier could comply with its delivery obligations under Section 103 without delivering this information in this fashion.[1] However, CALEA contemplates that carriers will employ the most efficient and effective means of delivering authorized surveillance information to law enforcement.

---

[1] As industry appears to recognize, certain call-identifying information must be delivered over a call data channel because it is not available on a call content channel.

See, e.g., 47 U.S.C. §§ 107(a)(1) (requiring consultation between law enforcement and industry "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements of section 103") (emphasis added); id. § 109 (addressing recovery of costs incurred to establish the capabilities required by Section 103). Having two separate channels to access and process call-identifying information would result in a substantial and unnecessary duplication in equipment, facilities, and cost. Unless all call-identifying information is delivered over a call data channel, law enforcement would be required, for the execution of a pen register order alone, to procure both a call data channel and a call content channel to ensure delivery of all of the dialing activity used to complete or control a call, even though that information could easily be delivered over a single call data channel. This kind of duplication of effort and expense is inconsistent with the spirit and purposes of CALEA.

85. A more cost-effective solution is to specify that all call-identifying information, including all dialed digits, be delivered to law enforcement over the call data channel. Requiring that appropriate call-identifying information be delivered over a call data channel or circuit is consistent with the legislative purpose of providing law enforcement with the information in the most efficient and effective means reasonable. In addition, delivering call-identifying information over a call data channel minimizes the risk of inadvertent intrusions on call content when the government is seeking only call-identifying information. It thus furthers the carriers' responsibilities under Section 103(a)(4)(A) of CALEA (47 U.S.C. § 1002(a)(4)(A)) to provide access to call-identifying information "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted." For these reasons, the proposed rule

provides that carriers shall deliver post-cut-through dialed digits and notification messages for in-band and-out-band signaling over the call data channel. Appendix 1 (§ 64.1708(d), (i)(1)).

86. **(c)** Timely delivery of call-identifying information. Section 103(a)(2)(A) of CALEA (47 U.S.C. § 1002(a)(2)(A)) obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission" of the communication to which it pertains, or "at such later time as may be acceptable to the government." In addition, Section 103(a)(2)(B) requires that call identifying information be made available "in a manner that allows it to be associated with the communication to which it pertains." A carrier relies on dialing and signaling information associated with a particular call in order to process and control that call from origin to destination and termination, including any redirection signaled during the call.

87. Law enforcement currently acquires contemporaneous information regarding the processing and content of a call through its monitoring of the local loop. It is imperative for law enforcement to be able to associate the call-identifying information to the call to which it pertains in an expeditious manner so that law enforcement can promptly and accurately correlate relevant evidence, and respond in emergency and life-threatening cases. Assume, for example, that the subject places a call to a "contract killer," and that the call involves a murder that is to take place immediately. If, while intercepting the "contract murder" communication, law enforcement cannot immediately associate the call-identifying information with the communication, law enforcement officers may be unable to save a life because they are not able to identify promptly, through the acquisition of the

telephone dialing information, whom the subject had called and where that party's telephone was located.

88. The prompt receipt of call-identifying information is also critical, for example, in illegal gambling cases, where the subject typically uses a "flash hook" feature to continuously accept incoming calls being held on "call-waiting." Without expeditiously receiving the call-identifying information, law enforcement would be unable to identify the separate calls.

89. The prompt receipt of call-identifying information that is clearly associated with a particular communication is also critical for law enforcement to carry out its statutory obligation of "minimizing" the interception of non-criminal communications to promote privacy. See generally 18 U.S.C. § 2518(5). To carry out its minimization obligations, law enforcement must quickly identify all parties to a conversation, even in multi-party calls, to determine the criminal culpability of the parties to the call. If a subject makes a call to a known non-culpable person or entity, such as a relative or business that is known not to be involved in criminal activity, law enforcement should immediately minimize the interception. In a multi-party call, if a subject drops off the call or an additional subject joins the call, law enforcement must promptly recognize that these events have occurred, ascertain which subjects are party to the call, and determine what, if any, minimization procedures should be employed. Without the prompt receipt of call-identifying information these requirements cannot be met.

90. Despite the importance of prompt delivery of call-identifying information, the interim standard places no requirements on when call data is to be delivered to law enforcement. The interim standard therefore would permit carriers to deliver call-identifying information at a time other than "before, during, or immediately after" the communication — and consequently would threaten law enforcement's traditional ability to associate call-identifying information with the communication to which it pertains. The failure of the interim standard to impose a specific delivery time requirement renders it manifestly deficient under Section 103(a)(2) of CALEA.

91. CALEA does not specify a particular time frame that would satisfy the "association" requirement of Section 103(a)(2)(B). However, the establishment of a reasonably short and objective timing requirement is essential to effectively implement that requirement and to ensure that call-identifying information is, in fact, delivered "before, during, or immediately after" a communication.

92. The proposed rule provides that carriers shall access and deliver call-identifying information to law enforcement "contemporaneously with the communications to which it pertains, or in a manner comparable to the speed with which other signaling messages are sent in the public network so that call-identifying information may be associated with the related communications." Appendix 1 (§ 64.1708(e)). Consistent with carrier network processing of call-identifying information, the proposed rule specifies an accuracy rate of 100 milliseconds (ms) for time stamps (i.e., no more than 100 ms difference between the time of the event and the time recorded in the time stamp) and

delivery "in as near real time as possible, but no later than three seconds after the occurrence of the associated call event * * * ." Id. § 64.1708(e)(1)-(3).

93. The particular timing requirements in the proposed rule are not the only ones that would satisfy Section 103(a)(2). Nevertheless, either these requirements or other reasonable and comparably effective ones are necessary. Adoption of such requirements will enable call data to be associated with the correct call and will permit law enforcement to react quickly in situations where innocent lives are threatened. For example, when a ransom call or a bomb threat call is made, the calling number will be provided quickly and will give law enforcement an opportunity to prevent harm to potential victims that would not be available if the interim standard's lack of timing requirements were left unaltered.

94. **(d)** Automated delivery of surveillance status information. Action by the Commission is also warranted with respect to the delivery of surveillance status information. Section 103 of CALEA provides that a telecommunications carrier "shall ensure" that its equipment is capable of intercepting communications and isolating call-identifying information. Section 103 thereby places an affirmative obligation upon the carrier to verify that its equipment is operational and that law enforcement has access to all communications and information within the scope of the authorized surveillance.

95. Any other interpretation of Section 103's "ensure" requirement would be inconsistent with Congress' clear intent to preserve capabilities available to law enforcement prior to CALEA's

passage. Law enforcement traditionally has had the ability, when it conducts interceptions, promptly to discern, through the application of a tone to the circuit, if there is any mistake, interruption, or trouble affecting an interception delivery effort. In addition, law enforcement has had the ability to ensure that all of a subject's communications are intercepted, because it acquires sufficient signaling information to know that law enforcement is monitoring the correct subscriber.

96. The TIA interim standard does not recognize any affirmative obligation on the part of carriers to assure law enforcement that the carriers' equipment is operational. Yet absent mechanisms to ensure that a carrier's equipment is functioning, law enforcement will not be able to verify the efficacy, accuracy, and integrity of its surveillance. Without such mechanisms, all intercepted evidence will be subject to challenge as incomplete or inaccurate. Because the TIA interim standard imposes no obligation on carriers to "ensure" that their equipment is capable of isolating and delivering all relevant communications and call-identifying information within the scope of a surveillance order, the standard is deficient under CALEA.

97. In principle, carriers can provide law enforcement with necessary surveillance status information by a variety of means. In practice, the most efficient and reliable means is through the automated delivery of status reporting messages. The proposed rule therefore calls for the automated delivery of three kinds of surveillance status signals: (i) a continuity tone or signal, which would ensure that law enforcement is notified immediately if the delivery channels from the carrier have failed; (ii) a surveillance status message, which would verify that the surveillance is on the correct service and is operational; and (iii) a message reporting any changes in the service features of a

subscriber that might affect law enforcement's ability to obtain all of the communications it is entitled to acquire under a court order or other lawful authorization. The automated delivery of these signals is not the only means by which of the requirements of Section 103 could be satisfied, but it is the most practical and cost-effective means and therefore should be included in the technical requirements and standards established by the Commission. The provision of these signals will preserve law enforcement's ability, when a switch- or network-based interception is controlled by the carrier, to verify and document that all of a subject's calls and call-identifying information are being intercepted and "expeditiously" delivered.

98. **(i)** Continuity tone. Law enforcement can verify and document that all of a subject's calls were intercepted only if it has a means to discern promptly an interruption in an interception. The proposed rule provides for carriers to deliver "a continuity check in the form of an in-band signal * * * or tone * * * that will verify that CCCs [call content channels] between the carrier and a law enforcement agency are in working order." Appendix 1 (§ 64.1708(h)). As noted, law enforcement has the ability to deliver such a tone itself today when it conducts interceptions. If such a capability is not preserved, law enforcement will lose the ability automatically to verify the efficacy, accuracy, and integrity of an interception effort.

99. **(ii)** Surveillance status message. Today, law enforcement employs non-automated means to determine whether the interception device is accessing the correct equipment, service, or facility. However, digital switching will preclude law enforcement from performing this function because law enforcement will no longer have access to the intercept location. The proposed rule therefore

provides for the automated delivery of surveillance status messages. Appendix 1 (§ 64.1708(f)). The rule provides for surveillance messages to be triggered and delivered "whenever a surveillance is activated, updated, or deactivated," and "periodically from once every hour to once every 24 hours for the duration of a surveillance." Id. § 64.1708(f)(1)-(2). The receipt of surveillance status messages would indicate that the interception is working correctly and is accessing the correct subscriber's service. It would also confirm that the path over which the message was sent is still operational. Without this information, law enforcement would not know when the software is turned on or off, or if it has failed. Law enforcement could not verify that the subject is being monitored, leaving open the possibility that important evidence is being lost. Providing this message will enable law enforcement to quickly correct any faults in the implementation of an interception.

100. Absent an automated surveillance status message, an interception could be overridden inadvertently or removed by carrier personnel for hours or days without law enforcement's knowledge. This circumstance could occur even with a continuity check because the continuity tone applies to the status of a call content channel or circuit, while the surveillance status message applies to the operation of the surveillance software in the switch. Thus, without surveillance status messages, law enforcement could receive an active circuit without being able to confirm that the surveillance software itself was activated and functioning properly. Further, if the subjects of surveillance cease their service or change their telephone numbers, law enforcement would be unable to obtain continuous surveillance coverage or could be put in the position of monitoring the telecommunications of an uninvolved third party.

101. **(iii)** Feature status message. The proposed rule also provides for automated delivery of messages indicating changes in a subscriber's call features and services (e.g., conference calling and call forwarding). Appendix 1 (§ 64.1708(g)). The provision of an appropriate automated message would enable law enforcement to procure the number of delivery channels or circuits required to ensure that the interception is fully effected and delivered as authorized. Whenever a subscriber has call forwarding or other features permitting the subscriber or another person to make multi-party calls, law enforcement must have access to multiple call content channels to ensure that it will receive all communications and call-identifying information that are subject to a court order or other lawful authorization. Without knowing what features are activated on a subscriber's service, law enforcement cannot know how many interception delivery channels and circuits are necessary. And without adequate delivery circuits, call content and call-identifying information evidence will be lost.

102. A carrier that fails to provide information on changes in a subscriber's calling features or services, in a timely manner, fails to satisfy its obligation under Section 103 to "ensure" that its equipment is capable of delivering all communications and associated call-identifying information to law enforcement. Law enforcement historically has been able to obtain this kind of information, but it has had to do so through relatively slow manual means. Because there were relatively few services or features a subscriber could choose that would affect the number of delivery channels needed for an interception effort, the fact that law enforcement received information on service changes by manual means did not significantly impair law enforcement's surveillance capabilities. In today's digital environment, however, the need for prompt notification is acute, because digital

switching has enabled customers to make rapid and instantaneous changes in their services and features, and because so many services and features trigger the need for multiple delivery channels.

103. As a practical matter, the automated nature of the foregoing features is extremely important. It would be impractical both for law enforcement and for telecommunications carriers themselves if carriers were to attempt to meet their obligations under Section 103 through a system that relied upon extensive human intervention. Under such an approach, law enforcement officials would have to contact carrier employees on a daily or hourly basis to verify these aspects for every electronic surveillance effort underway. By contrast, automating these functions would provide the information promptly and without human intervention, thereby lessening the burden on law enforcement and carriers and reducing the likelihood that critical communications and call-identifying information will be lost. Therefore, while the automated delivery of surveillance status messages is not the only possible means by which carriers can meet their obligations under Section 103, the automated surveillance status message provisions of the proposed rule represent the most appropriate way to "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)).

104. **(e)** Standardization of delivery interface protocols. In order for call content and call-identifying information to be delivered from a carrier to law enforcement, the parties must use equipment with a common delivery interface protocol. Section 103 does not obligate carriers to use any particular interface protocol, and the Department of Justice and the FBI are not asking the Commission to impose such an obligation by rule. However, a limitation on the number of interface

protocols is necessary to "ensure" that, as a practical matter, all content and call-identifying information to which law enforcement is entitled can actually be delivered. Unless a relatively small number of standardized protocols are employed, each carrier will be free to employ a separate interface protocol, and law enforcement agencies could be faced with prohibitive practical and financial burdens in equipping themselves to deal with scores of different protocols. As a practical matter, law enforcement agencies thus would be denied access to information to which they are guaranteed access by CALEA.

105. Although the interim standard contains non-binding information regarding the delivery interface protocols preferred by law enforcement, it does not contain any limitation on the number of protocols that may be used by carriers to deliver call content and call-identifying information. The proposed rule limits the number of interface protocols to no more than five. Appendix 1 (§ 64.1708(j)). Within this limit, the proposed rule leaves industry free to determine for itself which interface protocols will be used. While we are proposing a limit of five protocols, we do not mean to suggest that five is the only reasonable limit. The adoption of some reasonable limit, however, is necessary to ensure that the capability assistance requirements of Section 103 are not rendered illusory in practice by a proliferation of protocols.

3. The Technical Requirements and Standards of the Proposed Rule Satisfy the Criteria of Section 107(b) of CALEA

106. As noted above, Section 107(b) of CALEA identifies a number of criteria to be considered by the Commission in establishing technical requirements and standards. The provisions of the proposed rule meet each of these statutory criteria.

107. **(a)** Section 107(b)(1). The first criterion of Section 107(b) is that the technical requirements and standards "meet the assistance capability requirements of section 103" and do so by "cost-effective methods." 47 U.S.C. § 1006(b)(1). The foregoing discussion demonstrates that the provisions of the proposed rule meet Section 103's assistance capability requirements. In some instances, the requirements of the proposed rule embody the only means by which Section 103's requirements can be fully met. In other instances, while more than one mechanism or requirement might suffice to discharge a carrier's assistance obligations, the interim standard fails to mandate any such mechanism or requirement at all, and the proposed rule identifies a reasonable means of ensuring that those capability requirements are met.

108. The Department of Justice and the FBI further believe that the provisions of the proposed rule represent cost-effective means of meeting the assistance capability requirements of Section 103. A precise assessment of the cost-effectiveness of the proposed rule depends in part on cost information that industry, rather than law enforcement, possesses. However, during the course of discussions between law enforcement and industry over the development of standards to implement of Section 103, industry has not identified less expensive means of obtaining the results that law

enforcement believes to be required by CALEA. If it emerges during the course of this rulemaking proceeding that there are less costly alternatives that are equally effective in terms of carrying out the assistance capability requirements of Section 103, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

109. In some respects, such as the selection of a limited number of standardized delivery interface protocols (part III.A.2.e supra), adoption of the proposed rule should affirmatively reduce the overall cost of implementing CALEA to industry as well as law enforcement. Moreover, many of the capabilities requested by law enforcement in this petition would merely build upon features commonly used by telecommunications carriers today in the provision of services to customers, and could therefore be implemented at incremental cost to the carriers. For example, a carrier that supports a conference calling capability uses software to keep track of who is part of a conference call and to maintain the call through conferencing bridging equipment. If a carrier already has the ability to monitor when parties are added to, placed on hold during, or dropped from the conference call, a requirement that the carrier deliver that information to law enforcement will not impose a significant cost burden. Similarly, to route calls and for billing purposes, carriers receive and interpret subject-initiated dialing activity that directs a call through the carrier's network or allows the subject to control call services. In this regard, law enforcement simply seeks access to information that the carrier necessarily processes and maintains. In addition, in seeking notification messages reflecting network-generated signaling information, law enforcement is simply asking

carriers to transmit to law enforcement information that carriers' software is already fully capable of delivering to the carriers themselves or transmitting to their subscribers.

110. **(b)** Section 107(b)(2). The second criterion in Section 107(b) is that the technical requirements and standards "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). The capabilities and features in the proposed rule in no way jeopardize these privacy and security interests. As explained above, Title III contains numerous provisions designed to ensure that lawful surveillance does not unnecessarily intrude on the privacy of communications that are outside the legitimate scope of the criminal investigation, and CALEA itself contains additional privacy safeguards. See, e.g., 18 U.S.C. § 3121(c) (as amended by Section 207(b) of CALEA); 47 U.S.C. § 1002(a)(4)(A). In important respects, the provisions of the proposed rule actually enhance these privacy protections. For example, information on participants in a multi-party call that is conveyed by party hold and party join messages enhances privacy because law enforcement can more readily avoid recording conversations that are not of a criminal nature. Similarly, receipt of surveillance status messages ensures that the interception software is working correctly and is not accessing the service of an innocent subscriber. And the delivery of all call-identifying information, including post-cut-through dialed digits, over a call data channel would obviate the need to access a call content channel when law enforcement agencies are seeking only call-identifying information.

111. **(c)** Section 107(b)(3). The third criterion in Section 107(b) is that the technical requirements and standards "minimize the cost of * * * compliance on residential ratepayers." 47 U.S.C.

§ 1006(b)(3). The Department of Justice and the FBI believe that the provisions of the proposed rule impose the least financial burden on residential ratepayers consistent with the underlying need to meet the assistance capability requirements of Section 103, and industry has not indicated otherwise in prior discussions regarding the implementation of Section 103. A precise assessment of the impact of the proposed rule on residential ratepayers depends in part on cost information that is in the possession of industry rather than law enforcement. If it is shown during this rulemaking proceeding that there are alternatives to the provisions of the proposed rule that are equally effective in terms of carrying out Section 103 but would result in a smaller burden on residential ratepayers, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

112. It should be noted that Section 229(e)(3) of the Communications Act of 1934 (47 U.S.C. § 229(e)(3)), as amended by CALEA, requires the Commission to convene a Federal-State Joint Board to recommend the appropriate changes to Part 36 of the Commission's rules regarding the recovery of CALEA-related costs. The Commission has initiated a rulemaking in this matter,[1] and in the course of the rulemaking, the Commission has addressed cost recovery issues for non-reimbursable CALEA expenditures and whether changes are required to Part 36 of the Commission's rules in this regard. The Commission has not yet ruled on this issue. Once the Federal-State Joint Board issues its recommendation and the Commission issues a decision in this matter, industry and

[1] In the Matter of Jurisdictional Separations Reform and Referral to the Federal-State Joint Board, CC Docket No. 80-286 (released October 7, 1997).

law enforcement will know more about how non-reimbursed CALEA costs are to be recovered from residential ratepayers.

113. **(d)** Section 107(b)(4). The fourth criterion in Section 107(b) is that the technical requirements and standards "serve the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C. § 1006(b)(4). The provisions of the proposed rule are fully consistent with this criterion. The proposed rule does not impose any material restrictions on the adoption and provision of new technologies and services to the public by the telecommunications industry. It simply ensures that industry will take the steps necessary to carry out its statutory assistance obligations in conjunction with such technological advances.

114. **(e)** Section 107(b)(5). Finally, Section 107(b)(5) provides for the Commission to "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." The Department of Justice and the FBI suggest that the Commission provide a reasonable time for compliance with the technical standards adopted in this rulemaking proceeding by making the standards effective 18 months after the date of the Commission's decision and order in this proceeding. The Commission should further direct that industry will designate standardized delivery interface protocols within 90 days after the date of the Commission's decision and order.

B. THE COMMISSION SHOULD CONSIDER THIS MATTER ON AN EXPEDITED BASIS

115. The Commission has the authority to act on this petition on an expedited basis. Expedited consideration of a petition is warranted when a petitioning party makes a showing that it is necessary to serve the public interest. Omnipoint Corporation v. PECO Energy Company, PA 97-002, 1997 FCC LEXIS 2056, at *2 and cases cited at n.14 (Released April 18, 1997). In this case, important considerations of public safety and effective law enforcement call for expedition.

116. Expedition is warranted because effective electronic surveillance in a carrier-controlled, switch-based or network-based environment cannot be conducted without the electronic surveillance requirements set forth in this petition. This is because electronic surveillance in switch- and network-based environments depends, in great measure, upon carriers providing law enforcement the functions and capabilities that, in the past, law enforcement officers themselves could obtain. If telecommunications carriers follow only the TIA interim standard, not only will electronic surveillance information critical to criminal investigations and prosecutions be lost, but the safety of undercover officers, intercept subjects, and the public may be endangered. Thus, the deficiencies in the TIA interim standard must be remedied as soon as possible.

117. In addition, the product manufacturing and deployment schedules to produce the software and hardware necessary to comply with CALEA must be set in motion well in advance of the date that the technology actually becomes publicly available for use. If the deficiencies in the TIA interim standard are not addressed immediately, law enforcement, telecommunications carriers, and

equipment manufacturers will be uncertain as to how to proceed. Moreover, a delay in a standard that fully meets CALEA's requirements may also result in an increase in costs both to the government and to industry.

118. The CALEA-related deadlines that could be threatened by the failure to resolve the standards issue in a timely manner are set forth in the FBI's CALEA Implementation Report of January 26, 1998, which was submitted to the Chairman of the Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, House Appropriations Committee. Appendix B to that report sets forth platform roll-out dates for five switch manufacturers, all of which include software solution availability dates in the 1998-2000 time frame.[1]

---

[1] See CALEA Implementation Report, "Solution Availability Timeline," attached hereto as Appendix 6.

IV. CONCLUSION AND RELIEF REQUESTED

119. As the foregoing discussion demonstrates, the TIA interim standard omits electronic surveillance capabilities that are contemplated by the provisions and policies of CALEA, and the electronic surveillance information obtained through each capability is authorized under the applicable surveillance laws. Further, these capabilities are necessary for law enforcement properly and effectively to conduct electronic surveillance. In enacting CALEA, Congress intended to ensure that new technologies and services will not hinder law enforcement access to the communications content and call-identifying information that is the subject of an authorized electronic surveillance request. Absent the capabilities identified in this petition, the interim standard fails to carry out that intent and does not meet the requirements of Section 103 of CALEA.

120. For the foregoing reasons, the Department of Justice and the FBI, on behalf of themselves and other federal, state, and local law enforcement agencies, respectfully request that the Commission issue an order initiating an expedited rulemaking proceeding for the establishment of technical requirements and standards under Section 107(b) of CALEA. The Department of Justice and the FBI request that this petition be placed on public notice no later than Friday, April 27, 1998. Following the receipt of public comment on the petition, the Commission should issue a Notice of Proposed Rulemaking that proposes adoption of the provisions contained in this petition and proposed rule and/or any other requirements and standards that the Commission determines to be appropriate under Section 107(b) and the other statutory provisions applicable to this matter.

Because of the important public safety and law enforcement interests at stake, we request that the final decision and order in this matter be issued no later than September 28, 1998.

121. The Department of Justice and the FBI further respectfully request that the Commission not stay the interim standard during the consideration of the issues raised in this petition, but rather leave the interim standard in effect pending the issuance of a final decision in the rulemaking proceeding.

DATE: March 27, 1998

Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

_____

_____

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Stephen W. Preston
Deputy Assistant Attorney General
Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

Before the
Federal Communications Commission
Washington, D.C. 20554

Certificate of Service

In the Matter of:	)	
Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act	)	Docket No. _____

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), 14800 Conference Center Drive, Suite 300, Chantilly, Virginia 20151, hereby certify that, on March 27, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Joint Petition For Expedited Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Chantilly, Virginia this 27th day of March, 1998.

_____
David Yarbrough

In the Matter of
Establishment of Technical Requirements and Standards
for Telecommunications Carrier Assistance Capabilities Under the
Communications Assistance for Law Enforcement Act

Service List

*The Honorable William E. Kennard, Chairman
Federal Communications Commission
1919 M Street, N.W.-Room 814
Washington, D.C. 20554

*The Honorable Harold Furchtgott-Roth, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 802
Washington, D.C. 20554

*The Honorable Susan Ness, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 832
Washington, D.C. 20554

*The Honorable Michael Powell, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 844
Washington, D.C. 20554

*The Honorable Gloria Tristani, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 826
Washington, D.C. 20554

*Christopher J. Wright
General Counsel
Federal Communications Commission
1919 M Street, N.W.-Room 614
Washington, D.C. 20554

*Daniel Phythyon, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*David Wye
Technical Advisor
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W.-Room 500B
Washington, D.C. 20554

*Geraldine Matise
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*Kent Nilsson
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*David Ward
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 210N
Washington, D.C. 20554

*Marty Schwimmer
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 290B
Washington, D.C. 20554

*Lawrence Petak
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

*Charles Iseman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554 Policy Division

*Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Tom Barba
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Jay Kitchen
President
Personal Communications Industry Association
500 Montgomery Street
Suite 700
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
1401 H Street, N.W.
Suite 600
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry Solutions
1200 G Street, N.W.
Suite 500
Washington, D.C. 20005

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

***HAND DELIVERED**