Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of:	**)**	
	)	
Communications Assistance for Law Enforcement Act	**)**	**CC Docket No. 97-213**
	)	

To: The Commission

COMMENTS OF
THE FEDERAL BUREAU OF INVESTIGATION
REGARDING IMPLEMENTATION OF THE
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

Dated: December 12, 1997

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of:	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	
	)	

Comments of the Federal Bureau of Investigation
Regarding Implementation of the Communications
Assistance for Law Enforcement Act (CALEA)

I. INTRODUCTION

1. The Federal Bureau of Investigation (FBI), by its attorneys, respectfully submits its comments in the above-referenced proceeding on its own behalf and on behalf of other Federal, state, and local law enforcement agencies (hereinafter referred to collectively as "Law Enforcement").[1] The Communications Assistance for Law Enforcement Act (CALEA)[2]

[1] Following the enactment of CALEA, the FBI assembled the Law Enforcement Technical Forum ("LETF"), which consists of representatives from 21 Federal and 30 state and local law enforcement agencies, as well as the Royal Canadian Mounted Police. LETF members have participated in the development of the positions submitted with these comments. 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.

[2] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.). The purpose of CALEA is to preserve electronic surveillance capabilities authorized by Federal and state law. The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801-*et seq*., authorizes the government to conduct electronic surveillance for intelligence purposes. However, because of the classified and sensitive nature of electronic surveillance conducted under FISA, the FBI will, hereinafter, focus its comments upon criminal law-based electronic surveillance authority and activity. These comments are not intended to apply to those additional classified issues raised under FISA.

The Commission and telecommunications carriers should recognize, however, that nothing in CALEA, or the regulations to be promulgated in this proceeding, relieves carriers of their obligations to provide all necessary assistance to law enforcement under FISA, as set forth at 50 U.S.C. § 1805(b)(2)(B). While the techniques used for electronic surveillance collection under FISA are essentially the same as under criminal law-based Federal electronic surveillance authority and activity, there are legally specified administrative procedures regarding the handling of classified electronic surveillance orders and materials. These administrative procedures are most appropriately addressed directly by the FBI with

assigns a set of roles and responsibilities to the telecommunications industry, law enforcement, the Federal Communications Commission (FCC), and other governmental agencies in the implementation of the various regulatory requirements and other mandates under the statute. This proceeding was implemented to deal specifically with those roles assigned by Congress to the Commission. Law Enforcement welcomes and is pleased to participate in the Commission's effort.

II. BACKGROUND

2. Historically, law enforcement officers, after securing a lawful electronic surveillance order[3] would serve a secondary "assistance order" on the affected carrier to obtain relevant line and appearance information and leased line delivery circuits.[4] Moreover, in most cases, after serving the assistance order on the carrier, law enforcement technical agents were able to effect the authorized intercept themselves at locations in the "local loop," removed from the carrier's central office or switch. Such local loop-based interceptions, which historically dealt with ordinary, two-party, plain old telephone service (POTS) communications, were highly effective and successful. Thus, in the past, law enforcement was able to intercept *all* of the communications content and call identifying information supported by a subject-subscriber's POTS telephone service.

3. In addition, in the past, there were fewer carriers within a region, and those carriers' security personnel, as a general rule, were easy to ascertain and contact. As a result, in most cases, law enforcement was readily able to determine the identity of the relevant carrier and generally able to obtain the necessary assistance without unreasonable delays.

---

telecommunications carriers on an as needed basis pursuant to Executive Order 12958. Moreover, the FBI believes that the Commission will appreciate the problematic nature of a regulatory body's inclusion of classified matters in a broad-based rulemaking effort such as the instant one.

[3] Federal electronic surveillance orders may be issued pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2522 (referred to herein as "Title III"). Title III electronic surveillance orders pertain to the content of communications. Orders for the use of pen register and trap and trace devices, which provide call-identifying information, are issued pursuant to 18 U.S.C. §§ 3121-3127. Electronic surveillance and pen register and trap and trace orders may also be issued pursuant to state electronic surveillance statutes. Throughout these comments, "electronic surveillance," "interception," and "intercept" are used interchangeably to refer to electronic surveillance activities.

[4] Aside from including law enforcement's electronic surveillance search authorities, both the Federal Title III and the pen register and trap and trace statutes (as well as most state statutes) contain long-standing statutory provisions mandating that telecommunications service providers and others shall furnish the applying law enforcement agency "forthwith *all* information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services...[accorded] the person whose communications are to be intercepted" (emphasis added). Law enforcement is also required under this pre-CALEA, Title III provision to compensate the carrier for reasonable expenses incurred in providing such facilities or assistance. 18 U.S.C. § 2518(4). Analogous provisions exist with regard to pen register and trap and trace efforts. 18 U.S.C. § 3124. (FISA -based assistance provisions are found at 50 U.S.C. § 1805(b)(2)(B)).

Today, the proliferation of carriers and increasing centralization of their security functions have made it considerably more difficult, from both a procedural and practical point of view, for law enforcement to conduct, or effect, electronic surveillance. Larger carriers also have tended to concentrate their security functions in a single office within the carrier's entire region, which complicates both the installation of the intercept and the delivery of surveillance information. For example, if a law enforcement officer in Bell Atlantic's New Jersey territory obtains a court order for electronic surveillance on a subject subscriber's telephone in New Jersey, he must contact the Bell Atlantic security office in Virginia. As a result, a number of carrier personnel and facilities can be involved in implementing an intercept, which, if not properly addressed, can add delay to the process.

4. Moreover, internal administrative procedures employed by telecommunications carriers tend to vary from carrier to carrier. The level of scrutiny applied to judicial orders in some instances is overly extensive. Indeed, review by carrier personnel has resulted in facially valid intercept orders being inappropriately delayed, frustrated, or rejected.

5. Further, in recent years, rapid advances in technology, such as the deployment of new switch- and network-based services and features and the dispersion of intelligence throughout carrier networks, have eroded law enforcement technical agents' ability to fully and properly effect intercepts themselves. It is becoming apparent that surveillance solutions must increasingly become switch- and network-based.

6. It is well known that advanced telecommunications technology has changed the way telephone calls are established, processed, and maintained. As stated above, telecommunications frequently are no longer the two-party POTS calls of the past; multiparty calls having several different "legs" have become common. Second, calls no longer rely on dialed digits as the exclusive means of processing, establishing, and maintaining such calls; other signaling is centrally involved. Third, with the advent of subscriber-initiated multiparty calls, law enforcement is able to intercept only *part* of the communications being supported by the subject-subscriber's telephone service (i.e., those occurring over the leg of the call that the subject-subscriber's terminal equipment is actually connected to at any point in time). Fourth, subscribers are being offered calling features and services (e.g., conference calling, call forwarding) that can rapidly change almost instantaneously the nature of the subscriber's service, which, in turn, could lead to insufficient acquisition of interception delivery channels and circuits by law enforcement.[5] For all these reasons, therefore, law enforcement has been

[5] Although law enforcement agencies check with telecommunications carriers before a Title III or pen register effort begins, absent a message advising law enforcement of new services, there could be significant delay in effecting added delivery channels. As a result, without adequate delivery circuits, a substantial amount of the intercepted information will go undelivered—figuratively "falling on the floor."

technologically impeded from intercepting all of the lawfully authorized communications content and call-identifying information connected with, and supported by, the subject-subscriber's telephone service.

7. Nevertheless, even though the telecommunications markets in which lawful intercepts are effected have changed dramatically, law enforcement's primary electronic surveillance concerns have not changed. These concerns are the timeliness, security, accuracy, and evidentiary integrity of all lawful electronic surveillance. The public safety and the criminal prosecutions that necessitate electronic surveillance depend for their success on strict attention to these concerns.

8. Generally, the longer it takes to effect an intercept order, the greater the possibility that critical evidence and information will be lost because a criminal subject has moved on or because the intercept order has expired.[6] The more carrier personnel involved in effecting an intercept, the more likely it is that the security of a particular surveillance may be compromised. Delays in reporting a technical or human compromise of an intercept, for example, may result in subjects becoming apprised that surveillance exists without law enforcement's knowledge of that compromise. In such a case, not only will the evidentiary value of the electronic surveillance be eroded, but the safety of undercover law enforcement officers or the intercept subjects may be endangered. Delays or flaws in a carrier's operational procedures for responding to surveillance orders can also threaten the accuracy and integrity of electronic surveillance.[7]

9. All of these issues bear generally on the evidentiary integrity of electronic surveillance information and could conceivably present a basis upon which to challenge the admissibility of evidence.[8] For this reason, Law Enforcement believes that the Commission's rules establishing carrier policies and procedures are a critically important piece of the CALEA implementation process. It would be in the best interests of the carriers charged with responding to law enforcement's valid electronic surveillance orders to implement policies and

---

[6] No Title III order is valid for more than 30 days, with the 30 days beginning to run on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or 10 days after the order is entered. 18 U.S.C. §2518(5).

[7] If an intercept subject changes his service or subscribes to a new feature offered by a carrier that enables him to reroute his communications, the law enforcement electronic surveillance effort may be bypassed, and important evidence lost, for an extended period before law enforcement becomes apprized.

[8] Since, under CALEA, the implementation of electronic surveillance orders will increasingly shift to telecommunications carriers, Law Enforcement's electronic surveillance activity could be rendered ineffectual if the evidence that results from lawful intercepts is subjected to court challenge based on lax carrier procedures.

procedures that safeguard and promote the timeliness, security, integrity, and accuracy of electronic surveillance activity.

10. Among the key issues addressed by CALEA are the telecommunications entities covered by the statute and the obligations these entities must meet to ensure they will be able to comply with electronic surveillance orders. Further, as telecommunications technology evolves and new services and capabilities are introduced into the market, the Commission's role in evaluating whether, and how, CALEA's obligations will extend to new services or providers will become increasingly important. Indeed, in the future, as telecommunications markets continue to grow and become more competitive, telecommunications providers are likely to become more differentiated in the range of services they offer.

11. Concepts such as number and service portability, as well as other advances in technology, likely will enable consumers to pick from a much broader range of services offered by multiple providers.[9] Indeed, as digitization, packet switching, bandwidth conservation methods, and innovative network management and switching techniques continue to redefine the traditional understanding of "telecommunications," the Commission will be asked to play a critical public safety role in ensuring that law enforcement can continue to fully and properly conduct lawful electronic surveillance.

12. For these reasons, Law Enforcement welcomes the Commission's efforts to address the issues raised by the mandates contained in CALEA, particularly those regarding the definition of telecommunications carrier and carrier systems security and integrity policies and procedures. The rules to be developed by the Commission with respect to these definitions and carrier policies and procedures will have a direct impact on Law Enforcement's future conduct of its investigative and evidentiary collection activities with respect to electronic surveillance. As such, although Law Enforcement recognizes the need to not unduly burden the administration of internal carrier systems and procedures, it is equally important that the Commission craft rules, procedures, and policies that will accommodate Law Enforcement's investigative efforts and public safety demands. An understanding of CALEA's legislative history may be helpful to the Commission's consideration of these issues.

III. LEGISLATIVE HISTORY

---

[9] *See generally* 47 U.S.C. § 153(30); *Telephone Number Portability*, [*Second Report And Order]*, CC Docket No. 95-116; 12 FCC Rcd 12281 (released August 18, 1997); and *Telephone Number Portability* [*First Report And Order]*, CC Docket No. 95-116; 11 FCC Rcd 8352 (released July 2, 1996) (discussions of number and service portability).

13. Congress passed CALEA and President Clinton signed it into law in October 1994. As the legislative history articulates, CALEA was passed "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."[10]

14. Passage of CALEA was not without precedent; it was a logical and necessary development of the Nation's electronic surveillance laws. Congress' enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 served as the foundation for defining communications privacy and law enforcement electronic surveillance authority. Subsequently, as telecommunications technology continued to change, Congress passed the Electronic Communications Privacy Act of 1986, which extended law enforcement intercept authority to new technologies and services, such as electronic mail, cellular telephones, and paging devices.[11]

15. However, telecommunications technology continued to change at an even more rapid pace in the years following 1986. This technological change resulted in unique challenges for law enforcement. FBI Director Louis J. Freeh, speaking on behalf of other Federal, state, and local law enforcement communities, expressed the effect of these changes on law enforcement when he testified before Congress in March and August 1994.[12] In his remarks – the first in a series of hearings on "Digital Telephony" – Director Freeh testified that a variety of advanced telecommunications services and features were eroding law enforcement's ability to enforce the law through the use of the authorities set forth in the Federal and state electronic surveillance laws and related pen register and trap and trace statutes.

16. Director Freeh testified that without remedial legislation "one of the most effective weapons against national and international drug trafficking, terrorism, espionage,

---

[10] H.R. Rep. No. 827, 103rd Cong., 2d Sess., 9, *reprinted in* 1994 U.S. Code Cong. & Ad. News 3489 (1994). It is important to note that the final version of CALEA was substantially rewritten by subcommittees of the House and Senate Commerce Committees. The House Report accompanied an earlier version of CALEA, sponsored by the Judiciary Committee. There are no Commerce Committee reports.

[11] *See* 18 U.S.C. §§ 2510-*et seq.*; 18 U.S.C. §§ 2701-*et seq.*; and 18 U.S.C. §§ 3121-*et seq.* *See also* H.R. Rep No. 103-827, at 12.

[12] *Joint Hearing on the Proposed Legislation,"Digital Telephony and Communications Privacy Improvement Act of 1994,"* Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 103rd Cong., 2d Sess. (Mar. 18, 1994) (hereinafter *Director Freeh's Statement*).

organized crime, and serious violent crimes [would] be severely and adversely impacted."[13] He stated, "The indisputable fact is that emerging and future technology will have a much greater and more devastating impact on law enforcement and the public safety unless Congress acts now to ensure that current impediments are removed and new ones are not introduced."[14]

17. Director Freeh stated that the purpose of the proposed legislation was ". . . to maintain technological capabilities *commensurate with existing statutory authority*—that is, to prevent advanced telecommunications technology from repealing *de facto* statutory authority already conferred by Congress" (emphasis added).[15] Director Freeh emphasized that the legislation ". . .deals with the advanced telephony problem *in an appropriately comprehensive fashion*—it does not simply 'band-aid-over' past problems; it also responsibly deals with new services and technologies (such as personal communications services) that likely will emerge. . . [o]n the other hand, the legislation is narrowly focused on where the vast majority of the problems exist—the networks of common carriers, a segment of the industry which historically has been subject to regulation" (emphasis added).[16] It clearly was not intended to preserve or maintain past ineffective electronic surveillance capabilities that were no longer working fully or properly.

18. Thus, in analyzing CALEA, it is important to recognize that Congress clearly understood the essence of CALEA to be the *comprehensive preservation and maintenance of electronic surveillance and related statutory search authority* granted to law enforcement agencies by law. These goals are to be achieved through whatever technical modifications are necessary.[17]

---

[13] Director Freeh's Statement at 2.

[14] Director Freeh's Summary Statement (Summary Statement of the full statement referred to in note 12) at 10.

[15] Director Freeh's Statement at 2-3.

[16] Director Freeh's Statement at 3-4.

[17] In his Statement, Director Freeh advised, "Over the last decade, it is conservatively estimated that several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated, in whole or in part, by various technological impediments. . . It is important to note that there have been many instances where court orders have not been sought or served on carriers due to law enforcement's awareness of these pre-existing impediments . . ." *Director Freeh's Statement* at 32-33. Indeed, in 1994, the FBI provided the House and Senate Judiciary Committees with an illustrative list of 183 instances where the law enforcement agencies informally surveyed by the FBI stated that they had been impeded in conducting electronic surveillance-related efforts, in whole or in part, by advanced telecommunications services or features.

19. When Congress passed CALEA in October 1994, it heeded Director Freeh's request to maintain court-authorized or otherwise approved electronic surveillance. Congress required that CALEA ensure that new technologies and services will not hinder law enforcement access to the communications content and call-identifying information occurring over the telecommunications service that is the subject of a court order authorizing electronic surveillance. At the same time, Congress sought to balance law enforcement's needs with the privacy interests of the American public and with the telecommunications industry's need to develop and deploy new services and technologies that benefit society. As the House Report states: "[t]he bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."[18] It is in this light that the Commission must exercise its mandate to implement those sections of CALEA over which it has jurisdiction.

IV. DEFINITION OF TELECOMMUNICATIONS CARRIER

20. Law Enforcement agrees that the Commission has drawn the correct conclusion that Section 601(c)(1) of the Telecommunications Act of 1996 (the "1996 Act") did not modify CALEA's definition of a "telecommunications carrier," or its definition of "information services." In addition, the 1996 Act by its own terms did not modify or supercede existing law, unless expressly so stated. The 1996 Act did not contain language indicating that it would modify the definitions of "telecommunications carrier" or "information service" for the purposes of interpreting CALEA.

21. Law Enforcement also agrees with the Commission's tentative conclusion that all entities defined as common carriers for purposes of the 1996 Act are telecommunications carriers subject to CALEA. Law enforcement also agrees with the Commission's determination that commercial mobile service providers fall within CALEA's definition of telecommunications carriers. In addition, Law Enforcement believes that any entity providing telecommunications services for hire to the public are subject to CALEA's requirements. This definition would include cable operators and electric and other utilities that provide telecommunications services for hire to the public.

22. Moreover, in the post 1996 Act environment, there may exist telecommunications companies that do not hold themselves out to serve the public indiscriminately that should

[18] H.R. Rep. No. 103-827 at 13. Because of the extreme importance of fully effective electronic surveillance capability to public safety and effective law enforcement, Congress conferred authority on the Attorney General to enforce the assistance capability requirements set forth in CALEA Section 103 and conferred jurisdiction over such cases on the Federal courts. Moreover, to underscore the potential impact of this matter on public safety, civil penalties of up to $10,000 per incident for each day in violation were included to ensure widespread carrier compliance with CALEA. *See* 18 U.S.C. § 2522.

also be treated as "telecommunications carriers" by the Commission.[19] Otherwise, companies that hold themselves out to serve particular groups may, intentionally or inadvertently, undermine CALEA. Law Enforcement believes that if the Commission adopts the definition of telecommunications carrier as a company that holds itself out to serve the public indiscriminately, it may add a level of unnecessary ambiguity to its coverage. If the Commission were to adopt such language, it may create a loophole whereby criminals could use telecommunications service providers that do not indiscriminately offer their services to the public, thereby thwarting CALEA. Thus, the Commission should not incorporate the word "indiscriminately" into the definition of telecommunications carrier because it may cause an unnecessary ambiguity regarding the reach of the term "telecommunications carrier" under CALEA.

23. Finally, Law Enforcement agrees with the Commission's conclusion that providers of pay telephones are not telecommunications carriers for purposes of CALEA. Pay telephones, for purposes of CALEA, have more to do with end-user terminal equipment than with telecommunications services. It is Law Enforcement's contention that the type of terminal equipment being used for the telecommunications service is irrelevant under CALEA. CALEA is concerned with the type of telecommunications service, not the manufacturer or owner of the physical phone or device.

24. Law enforcement agrees with the Commission's proposal not to adopt a specific list of the types of carriers that would be subject to the obligations of CALEA because over time new communications technologies will come into existence. Law enforcement, however, is concerned that any type of illustrative list could be considered all-inclusive. Thus, Law Enforcement advocates that the Commission in its final rules state that any communication service, either wireline or wireless, for hire by the public, is subject to the obligations mandated by CALEA.[20] But, if the Commission believes that it is in the public interest to have an illustrative list of the types of entities that are subject to CALEA, Law Enforcement believes that it would be a useful clarification to specify that the following additional telecommunications services are included—

- Paging technologies
- Facility-based and switch-based resellers
- Specialized mobile services
- Enhanced specialized mobile services
- Aeronautical radio.

---

[19] *See generally*, P. Pitsch and A. Bresnahan, *Common Carrier Regulation of Telecommunications Contracts and the Private Carrier Alternative*, 48 Fed. Com. L.J. 447 (June 1996).

[20] The definition adopted by the Commission should make it clear that *any* service offered in this manner by a carrier would be subject to CALEA, including, for example, packet mode over digital subscriber lines ("DSL") services offered by carriers.

25. Law enforcement contends that paging systems should be included in the definition of "telecommunications carrier" for the purposes of interpreting CALEA because paging systems generally fall within the definition of common carrier or, at minimum, rely on common carriers to be activated. Individuals must call the paging service and then punch in their alphanumeric messages, such as phone numbers to call or messages. In addition, most common carriers for hire now provide phone systems that offer paging channel access. Thus, Law Enforcement advocates that the definition of telecommunications carrier, and any illustrative list the Commission may choose to create, should include pagers.

26. Further, Law Enforcement believes that resellers should be included in CALEA's definition of telecommunications carrier. It is Law Enforcement's contention that a reseller is accountable to assist Law Enforcement in any way technically feasible under CALEA. If the reseller is using any equipment or facilities for telecommunications service, the reseller and the incumbent owner of the telecommunications equipment or facility should be required to ensure that law enforcement officials will have access to their equipment or facilities for the purposes of electronic surveillance under CALEA. Law enforcement also contends that the definition of telecommunications carrier should include resellers with prepaid calling card or other similar services.

27. Law enforcement agrees with the Commission's conclusion that CALEA affords the Commission the flexibility to classify new local exchange carriers and to include, as telecommunications carriers, entities that provide replacement for local exchange service but who otherwise do not fit neatly into the current definition of telecommunications carrier. In the future, however, Law Enforcement will seek to consult with the Commission with regard to persons or entities offering services that become a replacement for local exchange service. Moreover, Law Enforcement agrees with the Commission's conclusion to decline to exercise its discretion at this time to include within the definition of telecommunications carrier specific persons or entities providing wire or electronic communication or switching service that is a replacement for a substantial portion of the local exchange service. The Commission should continually monitor new services and technologies because Law Enforcement believes that they could become a substantial replacement for local exchange service in the future.

28. Law enforcement recommends that the Commission not exercise its discretion pursuant to Section 102(8)(C)(ii) of CALEA, which allows the Commission to exclude specific classes or categories of carriers from the obligations of CALEA after consultation with the Attorney General. In this regard, only explicit exclusions of specific classes and categories of telecommunications carriers are sufficient to exempt carriers from their statutory obligations. In addition, Law Enforcement agrees with the Commission's tentative conclusion that private mobile service providers are not subject to the requirements of CALEA as long as the provider of private mobile service does not become a telecommunications service provider for hire by the public or replace a substantial portion of local exchange service. Once the private mobile service provider offers any portion of its

services to the public for hire, or when such service offered on a private carriage basis substantially replaces any portion of the public switched network, it should be considered a telecommunications carrier as defined under CALEA.

29. Law enforcement agrees with the Commission's tentative conclusion that providers of exclusively information services are excluded from CALEA's requirements and are not required to modify or design their systems to comply with CALEA with regard to information services. Law Enforcement believes, however, that any portion of a telecommunications service provided by a common carrier that is used to provide transport access to information services is subject to CALEA's requirements. Thus, Law Enforcement advocates that the Commission should consider a conservative definition of information services because of the possible criminal uses of such services.

30. Moreover, Law Enforcement agrees with the Commission's tentative conclusion that calling features associated with telephone service should be classified as telecommunications services under CALEA. Thus, telecommunications carriers offering these types of services must be required to make all necessary network modifications to comply with CALEA. In addition, Law Enforcement regards the Commission's list of calling features to be illustrative and not exclusive. Law Enforcement believes that any attempt by the Commission to make a comprehensive and exclusive list of calling features would be counterproductive and detrimental to law enforcement. An exclusive list would also be counterproductive because of the regulatory burden associated with updating the list each time a technological advancement occurs.

V. CARRIER SECURITY POLICIES AND PROCEDURES

A. The Commission Should Make It Clear That Carriers' Duty Under CALEA to Ensure That Intercepts Are Appropriately Executed Applies to Its Personnel Designations, Employee Oversight, and Personnel Practices and Procedures

31. Law Enforcement concurs with the Commission that carriers have an affirmative duty under CALEA to assist law enforcement in its duly authorized electronic surveillance activities. The underlying source of this duty is found, for example, in 18 U.S.C. Section 2518(4), which provides for intercept orders to require the provision by carriers of "all information, facilities, and technical assistance" necessary to accomplish the interception.[21]

[21] Nearly identical assistance provisions are set forth in the pen register and trap and trace statutes. *See* 18 U.S.C. § 3124.

32. Law Enforcement also concurs with the Commission that the use of the word "authority" in Section 301 of CALEA (Section 229(b)(1) of the Communications Act of 1934) refers to the authority granted to a carrier's employee by the carrier to engage in interception activity. By contrast, the first possible construction identified by the Commission in paragraph 25 of the Notice of Proposed Rulemaking ("NPRM") would place carrier personnel in the position of reviewing the underlying validity and basis for a court order or, in the case of exigent circumstances, the authorization of a duly empowered law enforcement official.[22] Law Enforcement strongly believes that carriers are not vested with such *de novo* review authority under CALEA or the electronic surveillance laws. Nor does Law Enforcement believe that CALEA grants discretion to the Commission to confer such authority on carriers.

33. Indeed, there have been anecdotal reports of instances where carriers have refused to provide assistance to law enforcement even after being presented with a facially valid court order in circumstances where carrier personnel "did not recognize" a particular judge's signature or where the description of the carrier service to be included in the intercept did not precisely match the carrier's brand name for that service. Yet it is clear from the assistance provisions in the electronic surveillance laws that it is not within the purview of carriers to look behind court orders or authorizations with the intention of enforcing the criminal law. The Commission has the opportunity, in furtherance of public safety, to establish rules in this proceeding that will minimize the likelihood of such case-by-case anomalies in the future.

34. To ensure that intercepts are conducted in a timely, secure, and accurate manner, the review that a carrier gives to a court order or certificate of authorization (provided in cases of exigent circumstances) should be limited to whether (1) the court order or certification is valid on its face (i.e., that it is what it purports to be); and (2) the intercept is

[22] Law Enforcement agrees that carriers have a duty with regard to electronic surveillance effected within a carrier's switching premises. However, not *all* future interceptions will be conducted at a carrier's switching premise. There will continue to be instances where law enforcement elects to effect an intercept as it does currently: in the local loop, away from a carrier's switching premises. Law enforcement's service of process and conventional carrier assistance will continue for these local-loop-based activities.

capable of being implemented as a technical matter. Any further scrutiny by carrier personnel of the legal basis for the intercept would result in the judgment of a carrier's employee being substituted for the judgment of either the court (in the case of an order) or the law enforcement officer empowered to certify that exigent circumstances exist. Hence, the Commission should specify that the duty of the carrier upon receipt of a facially valid court order or statutorily-based authorization for an intercept extends only to the prompt and good faith implementation of such court orders or authorizations.

35. It has been argued that carriers may face potential civil or criminal liability if they implement a court order that later proves to be unlawful. It should be noted, however, that Section 105 of CALEA does not place any additional liability on carriers that does not already exist under common law or the provisions of applicable statutes (e.g., Title 18 of the United States Code). Indeed, the procedures under these existing criminal and civil statutes also provide avenues for responding to any abuse by law enforcement of its authority and discretion in cases of electronic surveillance. Moreover, Law Enforcement believes that the electronic surveillance laws make it clear that a carrier's good faith implementation of an intercept requested pursuant to a facially valid court order, or certification of exigent circumstances, all other things being equal, would provide the carrier a defense to claims of liability.[23] Of course, the good faith requirement might not be met in the event that unauthorized interceptions by carrier personnel resulted from a carrier's failure to exercise its duty to implement and enforce appropriate security policies and procedures.

[23] The duties imposed on carriers under Section 105 of CALEA do not expand the potential civil or criminal liability of carriers. Good faith reliance on a court order or a request of an investigative or law enforcement officer under 18 U.S.C. § 2518(7) is a complete defense to any civil or criminal action against a carrier. 18 U.S.C. § 2520(d)(1), (2). Further, in a criminal action, good faith reliance by a carrier would defeat the intent requirement of a *prima facie* case. Indeed, under 18 U.S.C. § 2511(2)(a), "no cause of action shall lie in any court" against a carrier providing information, facilities, or assistance in accordance with the terms of a court order or certificate of authorization. The same is true for derivative liability. *See also infra* note 24.

B. The Commission Should Require Carrier Procedures That Ensure the Timeliness, Security, and Integrity of Electronic Surveillance Conducted on Law Enforcement's Behalf

36. Law Enforcement strongly contends that any carrier activities that threaten to compromise the security of electronic surveillance activities could endanger lives and impede prosecutions. Thus, Law Enforcement agrees with the Commission's statement in Paragraph 26 of the NPRM that each carrier must ensure that the personnel it designates to implement and have access to interceptions perform only authorized interceptions, and that those personnel do not reveal the existence, or content, of those interceptions to anyone other than law enforcement personnel, except pursuant to valid court, legislative, or administrative order. The following comments are designed to ensure that carriers' personnel and administrative procedures regarding electronic surveillance include meaningful security protections.

1. Personnel Procedures.

37. Law Enforcement agrees with the Commission's statement in Paragraph 27 of the NPRM to the extent that civil liability may extend to a carrier under certain circumstances if its employees are found to have illegally intercepted communications.[24] Law enforcement is

---

[24] With respect to the Commission's statement concerning the extension of criminal liability, Law Enforcement believes that the risk of carrier liability is minimal. For a corporation to be convicted for the criminal act of its agent under a theory of *respondeat superior*, it must be found that the agent is acting within the scope of employment (i.e., the agent must be performing acts which he is authorized to perform for the corporation, and those acts must be motivated–at least in part—by an intent to benefit the corporation). *See U.S. v. Cincotta*, 689 F.2d 238, 241-42 (1st Cir. 1982). Law Enforcement believes that the duties imposed on carriers under Section 105 of CALEA do not add to a carrier's potential liability for criminal acts of its employees because Section 105 duties do not bear on employee motivation or whether the employee is acting within the scope of employment in connection with the underlying criminal act. As the Commission notes, 18 U.S.C. § 2520, paragraph (a), already provides civil remedies for persons whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of Title III. In such a civil action, the person may recover from the "person or entity" which engaged in the violation. 18 U.S.C. § 2520(a).

Law Enforcement believes that the duties assigned to carriers under Section 105 would not expand the potential for such liability because, under common law principles, employers are already required to act reasonably in hiring employees and in supervising their activities. Compliance by a carrier with the regulations implementing Section 105 evidences that the carrier acted reasonably and mitigates against imposing vicarious liability for the intentional act of its employee; if carriers fail to comply with the regulations, such noncompliance will be evidence of negligence, and will tend towards imposition of vicarious liability. Thus, to the extent a carrier is exposed to possible derivative liability under *respondeat superior* or a claim of negligence, the risk of exposure will be substantially mitigated, if not eliminated, by compliance with CALEA.

charged with the responsibility of protecting citizens against illegal invasions of privacy, including by carrier personnel. Illegal intercepts or disclosures of electronic surveillance could conceivably occur during the implementation and maintenance of a lawfully authorized intercept as a result of the improper or negligent conduct of carrier personnel. Appropriate carrier personnel policies and procedures are required, therefore, in order to protect the respective interests of the carrier, law enforcement, and the public.

38. Initially, carriers should be required to establish a "vetting" process for carrier personnel designated and authorized by the carrier to receive and implement intercept orders, or certifications, or who otherwise have access to electronic surveillance activity and information. While a carrier's normal hiring and other personnel processes would likely include some inquiry into the credit and criminal histories of any prospective employee, the Commission's rules should include carrier policies and procedures that recognize that those select employees who are designated to effect electronic surveillance should be of demonstrable trustworthiness. Hence, carrier policies and procedures should include a background check commensurate with the sensitivity of the activities in which the designated employee will be engaged. The Commission should be aware that such trustworthiness determinations and background checks are consistent with the existing practice of carriers with regard to security personnel who today handle and administrate electronic surveillance orders.

39. The Commission should specify that this information should be collected and included in individual records for all designated personnel who participate in intercepts or have access to electronic surveillance information. Policies of this sort not only help law enforcement in the event an intercept is compromised or electronic surveillance information is improperly disclosed, they should afford protection for the carrier in making personnel assignments to security functions, and demonstrate that reasonable steps have been taken.

40. To the extent that carriers become aware of information regarding any security personnel that would call the integrity of a particular designated employee into question, carriers should be required to take immediate steps outside the normal personnel review process to reassign that particular individual pending more thorough review. In addition, security personnel should be required to execute nondisclosure agreements, the terms of which would survive the employee's reassignment or departure from the company, that also certify that the employee has been apprised of the criminal and civil penalties applicable to the

improper disclosure of surveillance-related information. These agreements should remain with the employee's permanent records.

41. In addition to law enforcement's security interest in these procedures, it likewise is in a carrier's interest that these agreements be obtained and that related procedures be clearly stated and assiduously pursued. For example, in the event that claims are made against a carrier arising from an alleged illegal intercept or the unauthorized disclosure of electronic surveillance information, the existence of clear and specific policies and procedures and demonstrable evidence that they were followed in a particular case should provide the carrier with a defense to an action based on its non-negligent, good faith conduct. As noted above, the foregoing policies and procedures safeguard the interests of all concerned - - the carrier, law enforcement, and the public.

2. Reports of Violations.

42. Law Enforcement believes it is important for a carrier's duty to include the affirmative obligation to report violations of its security policies and procedures and compromises, or suspected compromises, of intercepts. Thus, in the event a carrier acquires information that leads it to suspect that its employee may have engaged in illegal surveillance activity on his own, that information should immediately be reported to the FBI or the cognizant law enforcement agency for further investigation. At a minimum, it also is presumed that the employee would immediately be reassigned pending the outcome of the investigation. It is understood that this practice has historically been followed by carriers.

43. Law Enforcement also strongly agrees with the Commission's suggestion in Paragraph 27 of the NPRM that carriers should be required to report any compromise, or suspected compromise, concerning the existence of an interception to the affected law enforcement agency, or agencies. Indeed, because of the potential threat to the safety of witnesses, undercover agents, and intercept subjects that a compromise could represent, carrier technical personnel should be required to report such compromises, or suspected compromises, to the carrier security office immediately upon discovery. At a minimum, the Commission should require that no more than 2 hours be allowed to elapse between the discovery that an intercept has been compromised, or is suspected of being compromised, and the report of that fact to the affected law enforcement agency or agencies.

44. The standard that should apply in determining whether an intercept may have been compromised should be the standard of reasonable suspicion. In this regard, carrier personnel should be required to report objective facts that would reasonably give rise to the suspicion that an intercept had been compromised. Upon discovery of such facts, carrier personnel should be required to report the suspected compromise to the security office, which, in turn, would report it to the law enforcement agency involved. The Commission should develop a standard for determining what preventative measures would reasonably be required to ensure that compromised intercepts do not go undiscovered or unreported. The existence of specific policies and the resulting demonstrable evidence should provide a carrier with a defense to an action based on its non-negligent good faith conduct.

45. Law Enforcement believes that reports of violations of carrier security policies and procedures and compromises of intercepts should be reported to the Commission on a regular basis. Such reports would enable the Commission to exercise more effectively its continuing jurisdiction over CALEA-related matters. But this reporting requirement should not be permitted to delay a carrier's obligation to immediately report to law enforcement illegal wiretap activity and compromises, or suspected compromises, of lawfully authorized intercepts.

C. The Commission Should Specify That Carriers Are Not Required to Review the Substantive Basis or Underlying Legal Authority for Facially Valid Intercept Requests

46. Law Enforcement agrees with the Commission's statement in Paragraph 28 of the NPRM that there are at least two valid authorities for the implementation of an intercept: (1) a court order signed by a judge, and (2) a certification in writing by a law enforcement officer, as defined in 18 U.S.C. § 2510(7), that no court order is necessary pursuant to 18 U.S.C. § 2518(7). In addition, one party to a conversation can consent to the interception by law enforcement of the content of his or her conversations with another party (call content) or to the installation of pen register or trap and trace devices on his or her service. *See, e.g.,* 18 U.S.C. §§ 2511(2)(c) and 3121(b)(3). In such cases, the electronic surveillance statutes

clearly indicate that no court order is required. Yet, instances have been reported of a carrier impermissibly refusing to provide the requested assistance in these circumstances, even where the proper subscriber consent has been presented.

47. It is not necessary for the Commission to adopt a rule that carriers include in their internal policies and procedures information provisions that would separately define the legal authorizations required for carriers to implement an intercept. In fact, carrier maintenance of such detailed authorization criteria could erroneously suggest to carrier personnel that they are entitled to substitute their review for that of a judge when a carrier is presented with a facially valid court order. Carriers are the implementers, not the enforcers, of lawful intercept orders or certifications under the electronic surveillance laws. The Commission should clarify that its rules do not purport to alter the electronic surveillance laws.

48. There are a number of specific points made in Paragraphs 28 through 31 of the NPRM concerning the requirements for electronic surveillance that warrant specific comment in order to ensure clarity. These points also illustrate the importance that Law Enforcement attaches to the proposition that the Commission should not require carriers to be responsible for interpreting the subtleties of Federal or state electronic surveillance laws.

49. First, we offer the following to clarify what the Commission has suggested as the proper basis for "appropriate authorization" in cases of orders, exigent circumstances, and consent. It should be clarified that "appropriate legal authorization," in cases of court orders, is not limited to those issues pursuant to 18 U.S.C. § 2518. For example, court orders also may be issued pursuant to the federal pen register and trap and trace statutes (18 U.S.C. §§ 3121, *et seq.*), analogous state law, and FISA. Hence, the discussion and emphasis placed exclusively on Title III law could well be confusing to carriers when discussing what constitutes "appropriate legal authorization."

50. Second, as the Commission has correctly recognized, telecommunications carriers are obligated to implement interceptions based upon "certifications" under emergency circumstances (*see, e.g.* 18 U.S.C. § 2518(7); 18 U.S.C. § 3125; and 50 U.S.C. § 1805(e)). It should be noted, however, that these certifications (grounded in emergency circumstances) precede, rather than obviate the need for, court orders. The foregoing statutes make clear that within 48 hours (or less) after emergency interceptions are instituted, an appropriate court order must be filed with the court. When a law enforcement agency certifies to a telecommunications carrier that an emergency situation exists under the law, the telecommunications carrier is duty-bound to implement the interception effort. Neither CALEA nor any electronic surveillance law authorizes a telecommunications carrier to adjudge whether a statutory-based emergency exists or not. That is, carriers have no right to attempt to discern the factual or legal basis of the statutory emergency or to probe into which statutory category supports the emergency. Further, emergency authority and varying

exigent circumstances related to emergency interceptions are found in a number of the electronic surveillance statutes, as discussed above, not just in Title III. Hence, Law Enforcement would recommend against the Commission's proposal that carriers incorporate into their policies and procedures a "list of exigent circumstances found in 18 U.S.C. § 2518 (7)."

51. Third, the "consent" of a party to a communication (under Title III) or of a user (under the pen register/trap and trace statutes) is also recognized under the foregoing statutes as a basis for lawful authority to conduct interceptions (see e.g., 18 U.S.C. § 2511(2)(c) and 18 U.S.C. § 3121(b)(3)).

52. Law Enforcement would like to state, however, that it concurs with the Commission's tentative conclusion that existing laws adequately protect citizen's privacy and security rights against improper electronic surveillance. CALEA, at its core, focuses on the *preservation* of law enforcement electronic surveillance *capabilities* commensurate with, and pursuant to, the authority found in existing law, in a way consistent with communications privacy rights and security.

D. The Commission Should Ensure That Internal Carrier Authorizations and Procedures Are Designed to Maintain the Timeliness, Security, and Accuracy of Intercepts

53. Law Enforcement agrees with the Commission's proposal in Paragraph 30 of the NPRM to require carriers to designate specific employees to assist law enforcement officials in implementing lawful interceptions. Those personnel should be subject to the personnel procedures previously discussed. Moreover, Law Enforcement believes that there should always be at least one designated employee who is available to respond to appropriate law enforcement requests.

1. Designated Personnel.

54. For evidentiary and security reasons, Law Enforcement is greatly concerned by the Commission's suggestion in Paragraph 30 of the NPRM that non-designated employees be permitted to effect certain surveillance work. Law Enforcement strongly believes that only specifically designated carrier personnel should be permitted to have any involvement in, knowledge of, or access to an electronic surveillance or information concerning it. This does not mean that only security personnel should be required for the installation of regular services, such as leased lines, to law enforcement, or that security personnel would be required to perform those functions from which it would be impossible even to infer that an intercept was involved.

55. Carriers must maintain records of all personnel who are involved in the installation and maintenance of intercepts. The reasons for maintaining such information include the fact that carrier personnel having any part in the installation of an intercept may be required to testify in a criminal prosecution as to how the intercept was installed and maintained. Without a clear "chain of custody" for the intercept, prosecutions might fail if law enforcement were unable to demonstrate Title III compliance.

56. Law Enforcement believes that all carrier functions involved in the installation or maintenance of an intercept should be implemented by designated personnel if, in the performance of any particular function, the carrier employee doing the work could acquire any knowledge, either express or implied, of the intercept. It is uncertain that a line could be drawn to isolate functions that could be performed by non-designated carrier personnel as part of their routine work assignments without those personnel becoming informed that the task at hand relates to a surveillance.

57. The procedures employed by any particular carrier pertaining to the issuance, assignment, and distribution of work orders must enable any such functions to be segregated in a secure way so that non-designated carrier personnel would be able to participate in a surveillance without knowing of that participation. Even the remote possibility that a non-designated employee might conclude that his work was in connection with a surveillance should be precluded. Otherwise, intercepts or the undercover accounts, identities, and locations used by many law enforcement agencies could be compromised if their existence were to become widely known.

58. Because all persons having knowledge of, or access to, all facets of an electronic surveillance must be accounted for, Law Enforcement believes that, for the security reasons stated above, only specifically designated carrier personnel should be permitted to have any involvement in effecting surveillance work where the function to be performed could enable such carrier personnel to know of the intercept. Carriers should be responsible for ensuring that any low-level tasks that might be identified as not requiring designated personnel are described, assigned, and performed in such a manner that no information is communicated from which the non-designated employee could even infer that an intercept is involved.

59. Law Enforcement also concurs with the Commission's general proposal in Paragraph 30 of the NPRM that only designated employees create records containing electronic surveillance information and that those records be kept separately. However, for the reasons stated above, Law Enforcement does not agree that a separate record keeping function performed by designated employees would be sufficient to eliminate the concerns posed by the prospect that non-designated employees could perform electronic surveillance functions.

60. In response to the Commission's request for comment, Law Enforcement offers the following with regard to the rules the Commission should consider in implementing Section 105 of CALEA. Such rules should specify—:

- Telecommunications carrier policies and procedures regarding designated (authorized) personnel, facilities, and security need to be in place and working in order to limit access to information concerning the existence of (including records concerning access and operation of) interception capabilities to those personnel authorized by the carrier. An audit trail regarding such information is also required.

- Carrier personnel designated to effect interceptions and to have access to information concerning interceptions must be carefully selected by a telecommunications carrier. A telecommunications carrier is, and should be, responsible for ensuring that its designated personnel are trustworthy (e.g., have no serious criminal convictions, pending criminal charges, or bad credit history) and that they would be suitable for processing and handling sensitive law enforcement interceptions and information.

- An official list of a telecommunications carrier's designated personnel should be created and available at all times to appropriate, designated law enforcement personnel, for any operational needs and any necessary security review or checks that may be required. Such list should include the individuals' names, personal identifying information (date and place of birth, SSN), official titles, and contact numbers (telephone and pager). Nondisclosure agreements should be executed by such personnel.

As noted above, such trustworthiness determinations, and background checks are consistent with carriers' existing practice with regard to their Security Office personnel who handle and administer electronic surveillance orders.

2. Intercept Authorizations.

61. Law Enforcement believes, as stated earlier, that a court order or a certification (or a consent) is required before a lawful intercept may be implemented. It should be reiterated that a carrier's review of the legal process should be limited to confirming the order's or certification's facial validity and technical feasibility. The Commission may also wish to note that the presentation by telecopier of a facsimile copy of a court order or an emergency certification is sufficient service of process to trigger the carrier's obligation to respond. This is a particularly critical point in the case of larger carriers that have centralized security offices.

62. Law Enforcement also agrees with the Commission's proposal in Paragraph 31 of the NPRM that each carrier employee and officer who oversees interception activity be required to execute a document containing each of the items listed by the Commission in its proposal, with one exception. Item 4 of the Commission's proposal should be deleted because it is impossible for carrier security personnel to know, in real time, when the interception must lawfully terminate.[25] To the extent that a carrier's burden might be lessened, it may be, however, that the execution of a certification would suffice in place of a more formal affidavit. In addition, Law Enforcement proposes that any such document have added to it an additional item stating that the signatory understands that unauthorized disclosure of intercept information is an actionable offense potentially subject to criminal or civil penalties, including imprisonment or fine, or both.

63. With respect to the first item on the list, the "telephone number(s) or the circuit identification number(s)," Law Enforcement believes that this category should be modified to include the telephone number(s) *and* the circuit identification number(s). This is the phrasing used by the Commission in connection with the record keeping requirement addressed in Paragraph 32 of the NPRM. In addition, Law Enforcement strongly urges the Commission to broaden the category to include the subscriber identifier(s) (IMSI or MIN number(s)) and the terminal identifier(s) (IMEI or ESN number(s)) that would apply to interceptions of wireless communications. These identifiers should be included because, in

[25] *See infra* note 26.

wireless networks, routing numbers and line identities may be insufficient to connect a particular telephone number to a specific subscriber.[26]

64. Law Enforcement also appreciates that the paperwork burden on carriers should be minimized to the greatest extent possible, especially for large carriers or carriers that are involved in a substantial number of intercepts, while still maintaining all necessary safeguards. Law Enforcement wishes to ensure that the paperwork burden is never permitted to impede the timeliness with which intercept requests are implemented. The proposal that an affidavit or certification be prepared only by the employee or officer responsible for overseeing the interception activity is, thus, supported. That document, however, should set forth the identities and functions of all carrier personnel who have knowledge of, or access to, information or facilities associated with the intercept. If, as Law Enforcement has suggested in its response to Paragraph 30 of the NPRM, each of those employees is a designated person, the individual personnel records of those individuals should contain the requisite certification concerning non-disclosure of intercept information.

3. **Record Keeping.**

65. In response to Paragraph 32 of the NPRM, Law Enforcement believes that ensuring the integrity of the records of electronic surveillance maintained by carriers is critical to the security and evidentiary concerns of Law Enforcement and the public safety.

66. Law Enforcement, therefore, concurs with the Commission's general proposal that carriers be required to keep records of the conduct of surveillance, and that those records be compiled contemporaneously with the start of each interception.[27] In addition, the

---

[26] IMSI numbers are "International Mobile Subscriber Identities;" MIN numbers are "Mobile Identity Numbers;" IMEI numbers are "International Mobile Equipment Identities;" and ESN numbers are "Electronic Serial Numbers." *See* Cellular Radio Telecommunications Intersystem Operations Signaling Protocols (Interim Standard), TIA/EIA/IS-41.5-C (February 1996).

[27] As an operational matter, the Commission should require that the actual initiation and termination of an electronic surveillance be manually effectuated by carrier personnel, rather than programmed into the switch beforehand. For example, even though Law Enforcement is authorized to conduct interceptions up to a 30-day period, it is required by law to terminate the interception sooner if the goals of the interception have been attained. Also, in a number of states, the 30-day interception period is computed beginning at 12:00 a.m. of the day on which the court signs an order, which would typically then lead to an interception being terminated at midnight. Such circumstances could lead to a problem if programming is exclusively relied upon in situations where, for example, an extension or emergency authorization may have been obtained before the

Commission may wish to require the carriers to add the name of the issuing court in the case of a court order, which would assist both carriers and law enforcement in retrieving information when necessary. To ensure the integrity of the electronic surveillance effort, carriers should be required to maintain separate records of each surveillance activity, and those records should be maintained in a separate (including from FISA records) and secure storage area, access to which should be limited to a small number of designated carrier personnel.

67. It is essential to the admissibility of evidence that Law Enforcement be able to maintain these records for the same 10-year period required in 18 U.S.C. § 2518(8)(a). In that regard, Law Enforcement believes carriers should be required to transmit the originals, or certified original copies, of all electronic surveillance records to the cognizant law enforcement agency by no later than ten (10) days following the conclusion of an intercept. Law Enforcement understands that, while not necessarily required, carriers may wish to retain copies of those records. In such an event, the Commission should require that any records retained by a carrier after the originals or certified originals have been delivered to Law Enforcement be maintained in the same separate and secure manner as described above. Law Enforcement believes that these records are subject to the nondisclosure provision set forth in 18 U.S.C. § 2511(2)(a)(ii).

68. To the extent that a carrier has permitted a third party to have access to its switches or other facilities from which electronic surveillance could be detected, such carrier shall maintain records that will include the date, time, purpose, and identity of the third party personnel involved for each access permitted.[28]

4. <u>Timeliness</u>.

---

expiration of the original order, but potentially after normal security office business hours (or where the order expires during a weekend). The presence of carrier personnel would provide assurance that there would be no interruption in a surveillance in such a circumstance.

[28] For example, small carriers often have maintenance agreements with their manufacturers which could permit such activities to take place. In such cases, a carrier's service contract may include such record keeping provisions.

69. As Law Enforcement has stated in its comments on the specific requirements addressed in Paragraphs 29—33 of the NPRM, one of the critical factors affecting the efficacy of electronic surveillance is the timeliness with which intercepts are implemented. This factor is a theme throughout the Commission's discussion of carrier security policies and procedures. Section 103 of CALEA requires carriers to be capable of "*expeditiously* isolating, and enabling the government to intercept, all wire and electronic communications within that carrier's network . . ." and "*rapidly* isolating, and enabling the government to access, call identifying information that is reasonably available to the carrier." 47 U.S.C. § 1002. The more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays.

70. Therefore, to facilitate the CALEA requirement that carriers respond promptly to interception orders and provide information "expeditiously" and "rapidly," the Commission should require that carriers receiving interception orders or certifications complete their internal approval and documentation process and implement the interception within 8 hours of receiving the court order, certification, or consent. For exigent circumstances, for example, in cases under 18 U.S.C. §§ 2518(7), 3125, no more than 2 hours should be allowed to elapse before an interception, pen register, or trap and trace is implemented. These time periods warrant the further requirement that carriers have a designated security officer and designated technical personnel available, either on duty or on call by pager, 24 hours a day, 7 days a week.

71. Law Enforcement also believes that the accelerated 2-hour time period that should apply to the duty of carriers to report compromises of intercepts to law enforcement should also apply to reporting intercept malfunctions following their discovery. As discussed above, the compromise of an intercept poses an immediate danger to the safety of any undercover personnel who may be involved in the investigation and perhaps to the subjects of the intercept as well. So too, malfunctioning intercepts can not only result in the loss of critical evidence, but also endanger public safety by inhibiting law enforcement's ability to respond in emergency circumstances. A time period longer than 2 hours would result in a needless waste of the law enforcement resources being dedicated to an inoperative electronic surveillance.

72. In Paragraph 33 of the NPRM, the Commission asks for comment on additional information that carriers should be required to provide to law enforcement. Law Enforcement believes carriers should be required to maintain and have accessible to Law Enforcement a point or points of contact available twenty-four (24) hours a day, seven (7) days a week to ensure Law Enforcement access to the installation, monitoring, and maintenance of pen register, trap and trace, communications content, and other related electronic surveillance functions. Law Enforcement supports the efforts by the carriers and Commission to meet this obligation in the least burdensome manner possible.

E. No Distinction Is Made for Small Carriers Under CALEA

73. Law Enforcement strongly disagrees with the notion that CALEA contains any specific provision providing for the establishment of lesser requirements for small carriers insofar as their obligations concerning the implementation of CALEA's requirements is concerned. Nor do the electronic surveillance laws make such a distinction. From Law Enforcement's perspective, no sound policy reason exists for making a distinction between large and small carriers. Indeed, the assistance requirements set forth in the criminal statutes regarding electronic surveillance make it clear that law enforcement's ability to respond to important investigations, and frequently to life and death circumstances, cannot be dependent on the size of the carrier in the particular location where criminal activity may take place.

74. Law enforcement has no wish to burden small carriers unnecessarily, but the integrity and security of interceptions, and the impact that the loss of vital evidence may have on public safety and the successful conduct of criminal prosecutions, is unrelated to size. Under CALEA, a small carrier has the same obligation as a large carrier to respond to the dictates of the electronic surveillance laws and ensure that there are no unauthorized intercepts or disclosures of intercept information. There may be a practical correlation between the size of the carrier and the number of designated personnel that will be required by that carrier to fulfill its CALEA requirements. But new carrier entrants in critical geographic areas, even though they may be smaller, could conceivably receive a disproportionately large number of intercept requests.

75. Nonetheless, both Title III and CALEA apply across the board. Law enforcement's public safety and security concerns do not vary according to geography or size. In the first instance, therefore, the CALEA regulatory requirements being developed by the Commission should be made to apply equally to all CALEA-covered entities, and a multi-tiered regulatory scheme, whether based on carrier revenues or number of subscribers, should be rejected by the Commission.

76. For these reasons, Law Enforcement disagrees with the proposal stated in Paragraph 35 of the NPRM to define a category of "small telecommunications carriers" based on $100 million annual operating revenues. Likewise, Law Enforcement has several concerns about the Commission's proposal in Paragraph 35 to permit "small carriers" to elect to file a certification that its procedures are consistent with Commission rules regarding CALEA. Such a proposal likely would quickly become unworkable and, indeed, could lead to the imposition of an even greater administrative burden on carriers and the Commission.

77. Will penalties apply if a compliance certificate proves to be invalid due to the failure of an individual small carrier's policies and procedures to comply with Commission rules? Who would enforce the security policies, processes and procedures requirements in such cases? What safeguards for law enforcement would exist to ensure that intercepts could be implemented in a prompt, secure, and reliable manner while enforcement actions were pending? Would the Commission ultimately find itself in the position of providing detailed management and organizational directions to specific carriers? Furthermore, the $100 million cutoff would effectively eliminate all but about 21 of the thousands of telecommunications carriers covered by CALEA from the more stringent regulatory requirements.[29]

78. The Commission states in Paragraph 36 of the NPRM that smaller and newer carriers will be the least likely to be able to meet CALEA's requirements because they are unlikely to have the resources that are available to larger carriers. Law Enforcement does not

[29] In 1994, approximately 21 local exchange carriers had revenues above $100 million. *See* 1995 America's Network Directory (*citing* USTA 1994 Holding Company Report).

believe this proposition necessarily withstands scrutiny. Rather, the resources necessary to develop procedures to comply with CALEA under the rules to be adopted in this proceeding are likely to be smaller for small carriers. It stands to reason that simpler procedures will be required for small carriers with less expansive or complex networks, fewer facilities, and smaller staffs. The expense of compliance likely to be borne by large carriers, whose networks cover more territory, offices, switches and staff, does not necessarily translate, dollar for dollar, to a small carrier whose personnel are likely to serve multiple functions in substantially simpler organizational bureaucracies.

79. In response to the Commission's request for proposals contained in Paragraph 36 of the NPRM, it should be clarified that CALEA's objectives extend far beyond law enforcement's mere ability to receive pen register, trap and trace, and interception services, upon request, from all carriers subject to CALEA. CALEA's objectives, at least in the context of security policies and procedures, include all of the ancillary protections discussed in the preceding comments by Law Enforcement that will ensure the timeliness, accuracy, security, and evidentiary integrity of those services and the information they produce. Moreover, laxity in following rules established by the Commission will ultimately lead to public harm because unlawful and unauthorized interceptions could more easily take place.

80. The Commission should not, directly or otherwise, take any action that results in small carriers, as defined according to some competition-based criteria or an arbitrary revenue cutoff, being relieved of their responsibilities under CALEA. Instead of instituting a certification procedure, which would be exceedingly difficult to monitor and lead to gaps in compliance, the Commission may wish to develop standardized forms to assist small carriers with compliance. These forms could be designed to elicit all the information that large carriers will be asked to provide. They could even be issued with a manual containing a template set of security policies and procedures, which the adoption of and adherence to could be deemed by the Commission to be CALEA compliant. But, should the Commission choose to pursue such a course to assist small carriers, the content of the forms and the manual should specifically be designed to ensure that identical standards are applicable to large and small carriers alike.

81. Law Enforcement would be willing to work with Commission staff to develop the appropriate forms, but wish again to emphasize that their primary concerns are that the timeliness, accuracy, security, and evidentiary integrity of surveillance information be protected. Beyond that, it may be more appropriate for the Commission, together with interested trade associations and individual carriers, to lead such an effort.

F. Commission Procedures

82. Law Enforcement agrees with the Commission's tentative conclusion in Paragraph 37 of the NPRM that 90 days from the effective date of the rules adopted in this proceeding is sufficient time within which the carriers should file their initial procedures with the Commission. Law Enforcement also agrees that the Commission's general rules concerning compliance with its rules are applicable to compliance with CALEA. The procedures and penalties in those rules should be applicable to all entities that are subject to CALEA. To the extent that, as part of an enforcement proceeding, the Commission requires production of records relating to electronic surveillance policies and procedures, it should take care to ensure that the security of law enforcement practices and methods is not compromised.

83. In the case of mergers or divestitures, Law Enforcement believes that statements concerning CALEA policies and procedures should be included with the applications filed with the Commission seeking license transfers and other prerequisite approvals before a merger or divestiture may be consummated. These statements should address how the affected carriers will implement requests for intercepts during any post-transaction period preceding a consolidation or divestiture. Following the Commission's approval of a transaction, the surviving entity, in the case of a merger, or the new owner, in the case of a divestiture, should then have 90 days within which to file with the Commission any modifications to its procedures.

84. For reasons stated previously regarding the definition of telecommunications carrier, Law Enforcement concurs with the Commission's tentative conclusion in Paragraph 38 of the NPRM that the rules promulgated in this proceeding should apply to all telecommunications carriers, as defined by CALEA. To the extent that future determinations of substantial replacement, or the advent of new services, result in additional entities being included under the CALEA definition of telecommunications carrier, the rules should immediately become applicable to those entities.

VI. JOINT BOARD

85. The NPRM issued by the Commission to address cost recovery issues for non-reimbursed CALEA expenditures was issued in connection with the Federal-State Joint Board convened pursuant to Section 229(e)(3) of the Communications Act to consider changes to the Commission's Part 36 and Part 21 rules related to charges, practices, classifications, and regulations for cost recovery in light of CALEA. Law Enforcement believes that the Commission should use its current methodologies, to the fullest extent possible, for making determinations on how non-reimbursed CALEA costs should be allocated. Law Enforcement will comment in the separations proceeding in the event that submissions from other interested parties require further comment.[30]

VII. ADOPTING TECHNICAL STANDARDS

86. Law Enforcement concurs with the Commission's stated intention in Paragraph 44 of the NPRM not to address in this proceeding the issues raised in the petition by the Cellular Telecommunications Industry Association ("CTIA") regarding the technical standard for assistance capability envisioned by CALEA. The Commission is to be applauded for urging law enforcement and industry to continue their efforts to develop the necessary requirements, protocols, and standards.

87. Law Enforcement has the following specific comments on the points made by the Commission in its description of the standards issue set forth in Paragraphs 41 through 43 of the NPRM. In Paragraph 41, it should be clarified that the obligation to consult on standards issues falls equally on the Justice Department, carriers and manufacturers. *See* 47 U.S.C. § 1005 (manufacturers) and 47 U.S.C. § 1006 (Justice Department and carriers).[31] In addition, it should be noted that, although carriers may be deemed to be in compliance with CALEA

---

[30] *See Jurisdictional Separations Reform and Referral to the Federal-State Joint Board*, CC Docket No. 80-286 (released October 7, 1997).

[31] Manufacturers and support services providers "have a critical role in ensuring that lawful interceptions are not thwarted." H.R. Rep. 103-827, 103d Cong., 2d Sess., at 26 (October 4, 1994).

if they comply with publicly available technical requirements, the technical requirements must meet the capabilities set forth in Section 103 of CALEA. The electronic surveillance requirements under Section 103 of CALEA and the underlying electronic surveillance statutes are not subject to modification by carriers. Rather, technical requirements contained in an industry standard should concern only the means by which those electronic surveillance requirements are to be met.[32]

88. Law Enforcement believes that the promulgation of technical requirements or standards to implement the assistance capability requirements of the CALEA is vital to the preservation of law enforcement's electronic surveillance capability in an ever-changing telecommunications environment. Law Enforcement further believes that CTIA's industry consensus document proposing a standard (Standards Proposal [SP] 3580A) is technologically deficient because it lacks certain requisite functionality to fully and properly conduct lawful electronic surveillance. Law Enforcement had proposed amendments to SP-3580A to include additional functionalities, thereby creating a technical standard that would fully meet the assistance capability requirements of Section 103 of CALEA and satisfy the investigative, operational, and evidentiary needs of law enforcement. Because this is an ongoing process, which the Commission acknowledges, Law Enforcement concurs that it would be inappropriate to address these issues in this proceeding.[33]

89. Congress believed it beneficial to use "publicly available technical requirements or standards adopted by an industry association or standard-setting organization . . . to *meet* the [assistance capability] requirements of Section 103" (emphasis added). To give impetus to such efficient and industry-wide standards efforts, Congress offered a so-called "safe harbor" to those carriers, manufacturers, and support service providers that comply with

---

[32] We would like to clarify the Commission's statement in the NPRM (the Commission states: "[w]ith respect to information acquired solely through pen registers or trap and trace devices, the call-identifying information cannot include any information that may disclose the physical location of the subscriber, except to the extent that the location may be determined by the telephone number alone.") *See* NPRM, ¶¶ 7 and 40. The CALEA section to which the Commission is referring, Section 103(a)(2), in fact contains language that specifies that location-related call-identifying information may not be acquired by law enforcement "solely pursuant to the authority for pen registers and trap and trace devices . . ." The distinction is that the CALEA constraint involved is not one tied to the use of the device or the equipment, but rather to the *legal authority required to be provided*. CALEA Section 103(a)(2) specifies that the legal authority cannot be that set forth solely under the federal pen register and trap and trace statutes. Location-related call-identifying information can be lawfully acquired by Federal authorities by *other* legal authority (e.g., Title III, the court order specified in 18 U.S.C. § 2703(d), or a search warrant, etc.). This is an important distinction both legally and operationally. Aside from the legal authority specified to acquire location-related call-identifying information noted above, law enforcement recognizes, especially in kidnaping and extortion cases, that operationally the location of the kidnapper or extortionist (and the hostage victim) is often of prime or singular importance -- more important, for example, than intercepting the content of the criminal's communication.

[33] On December 5, 1997, Telecommunications Industry Association and Alliance for Telecommunications Industry Solutions published an interim standard, J-STD-025, entitled Lawfully Authorized Electronic Surveillance.

publicly available standards or technical requirements that fully meet the statutory mandates of Section 103.

90. Carrier compliance with the assistance capability requirements of Section 103 is required whether or not industry-wide technical requirements or standards are actually used, or ever promulgated. The "safe harbor" provision applies only where the technical requirements or standards *fully meet* the assistance capability requirements of Section 103.

VIII. REQUESTS UNDER THE REASONABLY ACHIEVABLE STANDARD

91. At Paragraphs 45 through 48 of its NPRM, the Commission requests comments on "Requests Under the 'Reasonably Achievable' Standard." Under Section 109 of CALEA, telecommunications carriers or any other interested party may petition the Commission to determine whether compliance with the assistance capability requirements of CALEA Section 103 is reasonably achievable with respect to equipment, facilities, or services installed or deployed after January 1, 1995. CALEA sets forth a number of factors the Commission must take into consideration when making its determination regarding whether compliance is reasonably achievable. Law Enforcement believes that these factors need to be weighed and applied in light of the critical importance to public safety of preserving law enforcement's electronic surveillance capabilities in a modern, mobile, information-based, and communications-driven society.

92. Before commenting directly on the Commission's request for comment on this issue, Law Enforcement wishes to note two sources of potential misunderstanding in these paragraphs. First, at footnote 155, the Commission states "Equipment, facilities, and services deployed on or before January 1, 1995 need not comply with the capability requirements of Section 103." While it is true that such equipment, facilities, and services will be "grand fathered" if the Attorney General chooses not to reimburse carriers for the necessary modifications, it is more appropriate to state that these equipment, facilities, and services will be deemed to be in compliance with CALEA until such time as the Attorney General agrees to reimburse or until a significant upgrade or major modification is made. At that point, the equipment, facilities and services will have to meet the requirements of Section 103 of CALEA.

93. Additionally, Paragraph 47 of the Commission's NPRM discusses reimbursement for meeting the capacity requirements set forth in accordance with Section 104 of CALEA. Law Enforcement wishes to note that the reasonably achievable standard of CALEA does not apply to capacity compliance or reimbursement; rather, it applies solely to compliance with the assistance capability requirements of CALEA Section 103. This distinction is made clear

in CALEA.[34]

94. With regard to petitions for determinations of reasonable achievability, Law Enforcement suggests the following procedural requirements. First, because cost will clearly play a significant role in the Commission's determinations, Law Enforcement suggests that the Commission require that individual carrier petition submissions include an estimate of the reasonable costs directly associated with the modifications under consideration. The showing should be required in the initial carrier petition in order to provide the Commission (and the Attorney General through notice from the Commission) with the information necessary to its determination at the initial stage of the process. Further, requiring such a showing will also allow the Attorney General to make a prompt decision regarding reimbursement of additional reasonable costs in the event that the Commission determines that some, or all, of the costs associated with necessary modifications are not reasonably achievable.

95. Law Enforcement also requests that the Commission present its determinations in terms of dollar amounts. Specifically, should the Commission determine that a modification is not reasonably achievable, Law Enforcement suggests that the Commission make the further determination as to what portion of the costs are reasonably achievable for the carrier. Again, presenting the Commission's findings in this manner will expedite the Attorney General's decisions regarding reimbursement of additional reasonable costs. Should the Commission state only that a modification is or is not reasonably achievable without addressing the issue of which costs should be assumed by the carrier, and which costs should be considered for reimbursement by the Government, the CALEA implementation process will be significantly delayed.

96. With respect to the factors listed in Paragraph 45 of the NPRM, Law Enforcement believes that the first factor on the list in Paragraph 45 pertaining to the effect of compliance on public safety and national security should be deemed to be the paramount consideration in the Commission's determination of reasonable achievability. CALEA states in its preamble that it is an act "to make clear a telecommunications carrier's duty to

---

[34] The Commission (in footnote 163) characterizes the FBI's capacity requirements as based on a "percentage of engineered capacity." Although the FBI issued its *Initial Notice of Capacity* that expressed future estimated actual and maximum capacity requirements in terms of "percentage of engineered capacity", after full consideration of all submitted comments, the FBI issued a *Second Notice of Capacity* that expressed future estimated actual and maximum capacity requirements in terms of geographically-based numbers of communications content, pen registers, and trap and trace devices. Neither the *Initial* nor *Second Notice of Capacity* was initiated under a rulemaking proceeding. *See Implementation of the Communications Assistance for Law Enforcement Act, Second Capacity Notice,* 62 Fed.Reg. 1902 (1997).

cooperate in the interception of communications for law enforcement purposes." *Id.* This clear expression of legislative policy should inform the Commission's decision on how each of the statutory factors is weighted and applied to requests pertaining to reasonable achievability. This process should be conducted on a case-by-case basis.

IX. EXTENSIONS OF COMPLIANCE DATE

97. Law Enforcement concurs with the Commission's decision in Paragraph 50 of the NPRM to not promulgate specific rules regarding requests for extensions of time to comply with CALEA in this proceeding. With respect to the Commission's proposal to consider petitions for extensions of time on the basis of the criteria specified in Section 109 to determine if it is reasonably achievable for a carrier, for "any equipment, facility, or service installed or deployed after January 1, 1995" to comply with the assistance capability requirements of Section 103 of CALEA, it should be noted that the issue of reasonable achievability requires consultation with the Attorney General. In this regard, it may be that the different issues presented by the question of whether an extension should be granted and the question of whether reimbursement is required might require a significantly different weighing of the reasonable achievability factors set forth in Section 109 of CALEA.

98. For example, development, manufacturing, and deployment schedules in the industry might lead to a request for extension on grounds of reasonable achievability. The grant of such a request would not necessarily mean that compliance with the assistance capability requirements of Section 103 of CALEA is not "reasonably achievable" under Section 109 such that the Attorney General would be required to reimburse a carrier lest it be "deemed" to be in compliance with CALEA under Section 109(b)(2)(B).

99. The former is an issue of timing; the latter is an issue of technical capability. It should also be noted that there may also be network-based, or other non-switch-based, solutions that would enable a carrier to provide certain surveillance services to law enforcement under Section 103 of CALEA that would preclude the grant of an extension. Law Enforcement looks forward to working with the Commission and industry on the development of applicable rules in both circumstances.

X. REPORTING AND RECORD KEEPING

100. Law Enforcement agrees in part with the Commission's tentative conclusion that some carriers may have in place practices for proper employee conduct and record keeping. However, Law Enforcement also believes that the different approaches to electronic

surveillance presupposed by CALEA, that is, switch- or network-based solutions, may render these existing procedures inadequate.

101. In the past, for example, a director of carrier security, pursuant to legal process, might advise law enforcement of the line appearance and cable and pair information necessary for an intercept. Law enforcement technical personnel would actually implement the intercept. In the future, CALEA solutions, which may be largely switch- or network-based, contemplate more extensive and direct involvement by carrier personnel. As a result, the manner in which interceptions are conducted and the number of carrier personnel involved may be substantially different. Consequently, even for carriers with whom law enforcement has worked in the past, there may need to be an increase in the level of attention paid to designated carrier personnel and their activities regarding interceptions, as well as an enhanced level of record keeping. It may be that carriers with extensive experience in working with Law Enforcement in this area will be able to make these procedural and management changes more easily than others.

X I. CONCLUSION

102. Law Enforcement urges the Commission to adopt a fair, balanced, and reasonable approach to the requirements of CALEA that is consistent with the Act's overall purpose of preserving law enforcement's electronic surveillance capabilities in today's technologically advanced U.S. telecommunications markets. Congress understood that the need for the expeditious and rapid delivery of surveillance information would be critical to the fulfillment of Law Enforcement's public safety mandate. The accuracy, security, and evidentiary integrity of that information must also be safeguarded and ensured for it to be effectively used in criminal prosecutions.

103. Law Enforcement urges the Commission to keep the purpose of CALEA in mind:

> 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, feature and services.[35]

The proposals and suggestions in these comments meet the interests of Law Enforcement in ensuring the security, accuracy, integrity, and timely effectuation of electronic surveillance.

---

[35] H.R. Rep. 103-827, 103rd Cong., 2d Sess., at 9 (October 4, 1994).

The comments offered by Law Enforcement regarding the definitions presented by the Commission in this NPRM will likewise enable Law Enforcement to keep pace with rapidly advancing technology in today's telecommunications markets.

104. None of the proposals, suggestions, and definitions in these comments, if they are adopted by the Commission, will impede the development and introduction of new technologies. Nor will their adoption unduly burden the service provider community. Moreover, none of the proposals, suggestions, and definitions in these comments will adversely impact the communications privacy or security of the public. Indeed, they should enhance communications privacy and security. The Commission's ongoing role in fulfilling the fundamental public safety purposes of CALEA is critical, and Law Enforcement appreciates the Commission's efforts in this matter.

Respectively submitted,
FEDERAL BUREAU OF INVESTIGATION

Carolyn G. Morris
Assistant Director
U.S. Department of Justice
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535