**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

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

Dated: February 11, 1998

**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 |
| | ) | |
| | ) | |

**Reply Comments of the FBI Regarding**
**Implementation of the Communications**
**Assistance for Law Enforcement Act (CALEA)**

## I. INTRODUCTION

1. The Federal Bureau of Investigation (FBI) respectfully submits its reply 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]

[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 reply 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.

## II. CALEA'S TECHNICAL STANDARD AND SAFE HARBOR PROVISIONS[2]

2. The Telecommunications Industry Association ("TIA") has recommended that the Commission refrain from establishing, by rule, under section 107(b), technical requirements or a standard to meet the requirements of section 103 of CALEA, in light of the recently promulgated TIA interim standard J-STD-025.[3] Although Law Enforcement strongly maintains that the TIA interim standard is deficient because it lacks certain key capabilities, Law Enforcement has not yet petitioned the Commission to establish a new standard to meet the requirements of section 103. Hence, we concur with TIA that, at this time, the Commission's undertaking of a rulemaking action regarding a CALEA standard in *this* NPRM would be unwarranted.[4] Indeed, we believe that it would not be legally supportable under CALEA.[5] Under section 107(b), the proper procedure, now that the J-STD-025 interim standard has been issued, is for a government agency or a person to file a petition with the Commission which claims that the standard, as promulgated, is deficient. To date, no party has petitioned the Commission regarding this interim standard.[6] Absent the requisite statutory

---

[2] Law Enforcement has followed the structure of the comments filed by industry for the Commission's ease of review. It should be noted, however, that the issues upon which industry focuses the most attention — the technical standard, extensions, and safe harbor provisions — are not the subject of this proceeding.

[3] *See* TIA Comments.

[4] *Id.*

[5] *See* 47 U.S.C. 1006(b) and the Commission's CALEA analysis in its NPRM at 28. *Accord*, TIA.

[6] Several commenters have encouraged the Commission to rule on Cellular Telecommunications Industry Association's (CTIA) pre-J-STD-025 petition, which had requested the Commission to adopt and establish, as a CALEA technical standard, the then working (but unfinalized) TIA SP-3580 document. CTIA asserted in its petition that no standard existed, and went on to inaccurately allege that the FBI would effectively block the promulgation of a final standard. It thus argued that the Commission should jump into the breach and act. CTIA's central arguments in that petition, of course, have been proven wrong — TIA has issued the J-STD-025 standard. Moreover, the FBI

predicate of a deficiency petition being filed regarding J-STD-025, the Commission lacks the statutory authority to engage in such rulemaking.

3. TIA also has requested the Commission to clarify the safe harbor provisions found in section 107(a) of CALEA with reference to the J-STD-025 interim standard.[7] Law Enforcement strenuously objects to this request. Law Enforcement finds no statutory support in CALEA for any party to so petition the Commission or for the Commission to entertain a petition to make determinations about, or render a legal opinion concerning, safe harbor. The statutory authority conferred upon the Commission under section 107(b) of CALEA is specific and limited.[8] It extends to establishing, if petitioned to do so, technical requirements or a standard, if none exists, and technical requirements or a standard where those in existence are claimed to be, and are determined by the Commission to be, deficient. Under such circumstances, the Commission may provide a reasonable period of time and conditions for compliance. During the period of transition, the Commission may also set forth new technical requirements for carriers or craft a new standard that would fully meet the requirements of section 103. Although Congress presumably could have empowered the Commission to make determinations about, and confer, safe harbor, the absence of any such language in CALEA clearly indicates that Congress did not intend to grant such authority to the Commission.

---

obviously did not *prevent* (and never could have *prevented*) the promulgation of an industry standard. Therefore, under the express and limited conditions specified under CALEA, which allow for the submission of a standards-related petition to the Commission, CTIA's pre-standard petition fails to comply with CALEA and lacks validity. It is clear then that, as a matter of law, absent the requisite statutory compliance, the Commission cannot act upon CTIA's petition.

[7] *See* TIA Comments.

[8] TIA concurs: Congress provided the Commission with only a limited role in establishing technical compliance standards. TIA Comments at 6.

4. Further, the Commission should also reject TIA's request to render advisory opinions in *this* NPRM regarding carrier and manufacturer liability during the period that the interim standard is in place or during the pendency of a deficiency petition. Similarly, the Commission should refuse to address in *this* NPRM how much time it would allow for compliance if a new standard were established.[9] Obviously, the Commission cannot make such determinations absent a deficiency petition properly before it. Moreover, it would be premature and improper to address these fact-based issues absent a fully-developed record. Resolution of these issues would necessarily be tied directly to determinations of case-specific factual circumstances associated with the nature of, and the reasons for, the deficient standard, and how long it would take the various manufacturers, carriers, or others to redress the deficiencies identified. Therefore, Law Enforcement strongly urges the Commission to decline to address these issues before they are properly presented to the Commission.

5. The Commission already has wisely decided that it will address any petition regarding a CALEA standard and requests for extensions of time for compliance separately in another rulemaking.[10] Law Enforcement supports the Commission's stated position and urges the Commission not to reverse itself in that prudent decision.

6. Finally, Law Enforcement would be remiss if it failed to note some imprecise assertions made by United States Telephone Association (USTA) and CTIA suggesting that the *mere existence* of the published J-STD-025 interim standard satisfies the safe harbor requirements of section 107(a).[11] In fact, as the Commission has previously noted in its

---

[9] *See* TIA Comments.

[10] Commission NPRM at 30.

[11] USTA Comments at Summary 2, and at 10, respectively: ("The Commission should be aware that the industry standards setting body has adopted an interim standard which provides a 'safe harbor' for carriers pursuant to section 107") ("The TIA and Committee T1 subsequently jointly published the standard on an interim/trial use basis. This satisfies

NPRM, safe harbor under section 107(a) can only potentially exist where the carrier or manufacturer is *in compliance with* publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under section 107(b) that meet the requirements of section 103.[12] Since carriers and trade associations assert in their NPRM comments that the technical solutions (software, equipment, etc.) to meet the section 103 requirements are yet to be completed and deployed, it is clear that the statutory requirements for safe harbor have not been met. Current carrier equipment, facilities, and services simply are not in compliance with the interim standard.

## III. EXTENSIONS FOR CALEA COMPLIANCE

7. TIA, USTA, and Personal Communications Industry Association (PCIA) have requested the Commission to grant a two-year blanket extension of the CALEA compliance date for all telecommunications carriers, from October 25, 1998 till October 24, 2000.[13] Law Enforcement strongly believes that the Commission must reject the requests of these trade associations for a blanket two-year extension for compliance for all telecommunications carriers for the numerous reasons set forth below. Most importantly, CALEA does not permit such petitions from trade associations,[14] nor does it permit petitions for industry-wide

---

the 'safe harbor' provisions of section 107..."). CTIA Comments at TAB B (CTIA letter to TIA, dated Nov. 20, 1997) ("The TR45.2 Subcommittee decided long ago that it would seek ANSI approval for then PN-3580 to meet the section 107 'safe harbor' provisions of ...[CALEA], which requires that technical standards be publicly available and adopted by an industry association or standard-setting organization").

[12] Commission analysis of CALEA in its NPRM at 27.

[13] *Accord*, CTIA.

[14] The Commission has already correctly noted in its NPRM at 33-34 that, under CALEA, it is "a telecommunications carrier" who is authorized to petition the Commission for an extension under section 107(c) ("We propose to permit carriers to petition the Commission for an extension of time ... to determine whether it is reasonably achievable

blanket extensions.

8. First, recognizing that technological impediments to electronic surveillance capabilities pose an extremely serious risk to the public safety, effective law enforcement, and the Nation's security, Congress intended to keep the window of societal vulnerability as small as reasonably possible. Noting that Law Enforcement, carriers, manufacturers, and others had been engaged in extensive, ongoing technical discussions regarding Law Enforcement's technological interception requirements for several years before CALEA was enacted,[15] Congress concluded, and all parties to the legislation agreed, that the four-year CALEA compliance period within which to meet the section 103 capability requirements was reasonable.

9. Second, although Congress encouraged the use of standards-setting organizations as a means of ensuring efficient and cost-effective implementation of the section 103 requirements, Congress made it clear, in section 107(a)(3), that "[t]he absence of technical

---

for the petitioning carrier with respect to any equipment, facility, or service ... to comply with the assistance capability requirements of section 103 within the compliance time period") (emphasis added). Congress expressly limited who could petition for an extension under section 107(c) to a "telecommunications carrier." In contrast, section 109(b) provides that "a telecommunications carrier or any other interested person" may petition the Commission regarding a determination of reasonable achievability under section 109.

.

[15] *See* H.R. Rep. No. 827, 103rd Cong., 2d Sess., 15, *reprinted in* 1994 U.S.C.C.A.N. 3495 (1994). The FBI and telecommunications industry efforts, described in the House Report, under the Electronic Communications Service Provider Committee (ECSPC), began in May, 1992 with frequent meetings occurring from 1992 through 1994. After CALEA was enacted these meetings intensified and were later subsumed into the TIA standards forum. With law enforcement interception requirements being broadly understood very early on, based upon prior ECSPC "Action Teams'" efforts and otherwise, there was little reason to believe that a CALEA industry standard would justifiably take over two-and-one-half years to complete.

requirements or standards for implementing the assistance capability requirements of section 103 shall not . . . relieve a carrier, [or] manufacturer . . . of the obligations imposed by section 103."[16] Stated differently, Congress envisioned the use of, and compliance with, an industry standard as but *one of the means* to the *end* of complying with section 103 within the compliance period. If anything, Congress could have assumed that the standards-setting process *means* would have hastened -- not delayed -- CALEA compliance. The standards-setting process -- a process dominated and controlled by the telecommunications industry -- was never intended to operate as an end in itself. Nor would industry delay in promulgating a standard, in and of itself, justify an extension. Congress never intended one of the industry's means of implementing CALEA to effectively operate as a trump card in the industry's hands to repeal *de facto* CALEA's compliance date at the industry's discretion.

10. Indeed, Congress was prescient in its awareness that, absent statutory language affirmatively directing carrier compliance within four years, an industry-dominated standards process could easily drag out technical discussions and solutions development indefinitely -- a prospect in conflict with Congressional intent. Moreover, Congress anticipated that an industry-based standard might be challenged as deficient and provided a statutory mechanism to deal with such challenges.

11. Third, the delay in promulgating an industry standard has arisen essentially because the industry has refused to include all of the technical functionality, consistent with the section 103 assistance capability requirements, that Law Enforcement has consistently stated it requires to effectively, properly, and lawfully conduct electronic surveillance. Law Enforcement has repeatedly advised TIA's standards-setting body *what* interception capabilities Law Enforcement requires, based upon its vast operational and courtroom experience, to properly conduct electronic surveillance in a way that meets evidentiary, security, and integrity needs.

---

[16] *See* the Commission's concurring CALEA analysis in its NPRM at 28.

12. In CALEA, Congress recognized that law enforcement officers are the experts in, and end-user recipients of, the electronic surveillance solutions being developed. The industry has wrongfully excluded these necessary end-user law enforcement interception capability requirements from the interim standard.[17] Although carriers, manufacturers, and others, under CALEA, are certainly equipped and entitled to make determinations about *how* best to implement Law Enforcement's requirements technologically, CALEA does not empower the industry to veto in the standard those section 103 capability requirements that Law Enforcement has consistently stated it needs to do its job properly and lawfully.[18]

13. Fourth, trade association requests for a blanket extension of time for compliance are grounded in the flawed rationale that, since the J-STD-025 interim standard has only recently come into existence, it would be impossible for equipment to exist that would meet the section 103 assistance capability requirements or the J-STD-025 interim standard by the October 25, 1998 compliance date.[19] Further, these requests misleadingly represent, based on normal industry practice, that it will take manufacturers 24-30 months from the

---

[17] The House Report on CALEA states that telecommunications carriers "will have a 'safe harbor' and be considered in compliance with the capability requirements if they comply with publicly available technical requirements or standards designed in good faith to implement the assistance requirements." H.R. Rep. No. 827, 103rd Cong., 2d Sess., 26, *reprinted in* 1994 U.S.C.C.A.N. 3506 (emphasis added).

[18] The House Report on CALEA indicates the nature of the industry's proper role in implementing CALEA within standards forums. "The legislation provides that the telecommunications industry itself shall decide *how* to implement law enforcement's requirements ." (emphasis added), H.R. Rep. No. 827, 103rd Cong., 2d Sess., 19, *reprinted in* 1994 U.S.C.C.A.N. 3499 (1994). The point is: the requirements are law enforcement's, and *how they are to be implemented* is for the telecommunications industry to decide. But, the industry cannot decide not to implement important portions of Law Enforcement's interception requirements.

[19] *See, e.g.*, CTIA Comments at 8: "The absence of a standard a fortiori means that compliance is not 'reasonably achievable through application of technology available within the compliance period.'"

promulgation of the J-STD-025 interim standard to produce CALEA compliant solutions.[20]

14. Based upon direct discussions with manufacturers, Law Enforcement has learned that most manufacturers have been developing technological solutions for some time to address the section 103 requirements. Further, while there are several important technical interception capabilities that have not been incorporated into the J-STD-025 interim standard, Law Enforcement and the industry have been in full agreement for quite some time with regard to the inclusion of all of the other technological capabilities set forth in the interim standard. As to these agreed-to items, which constitute the great majority of the overall requirements, most manufacturers long ago began designing and developing solutions even to some interception capabilities excluded from the standard. In fact, several manufacturers are well along the way. Moreover, a number of the manufacturers have developed many of the needed CALEA solutions in their switching platforms in order to meet CALEA-like solutions required of them by statute or otherwise by law enforcement or national security entities in a number of foreign countries.

15. Based on progress that the industry has already reported making, it is likely that certain manufacturers will have developed technological solutions to meet most (if not all) of the section 103 requirements by October 25, 1998, or shortly thereafter.[21] Thus, a blanket two-year extension for compliance would be unjustified, particularly given the serious risk to the public safety, effective law enforcement, and the Nation's security posed by ongoing technological impediments to electronic surveillance.

---

[20] *See, e.g.*, TIA's Comments.

[21] *See* the attached FBI report filed with U.S. House of Representatives Appropriations Committee Chairman Rogers, dated Jan. 26, 1998, (Appendix A). In this report, it is stated that a Bell Emergis network-based CALEA solution will be available to carriers before the October 25, 1998 compliance date, and that the commonly-used Nortel DMS-100 switches will be substantially CALEA-compliant by the 4th quarter of 1998.

16. Fifth, under section 107(c)(2), "Grounds for Extension," the statutory language of CALEA states that a request for an extension of the compliance date must be based upon a determination that compliance with the assistance capability requirements under section 103 is not reasonably achievable through application of technology available within the compliance period. The language of the statute indicates that such an extension should be grounded on the *technological feasibility* of meeting these requirements within the compliance period. CALEA, section 107(c)(2), does not envision industry delay in promulgating a standard as proper "grounds" for the Commission's granting extensions.[22]

17. There is little doubt that had the industry proceeded expeditiously to design and develop technical solutions that would meet Law Enforcement's articulated interception requirements under section 103 -- either within the industry-controlled J-STD-025 interim standard or otherwise -- that section 103-compliant technology would widely exist and have been implemented within the compliance period. In the context of CALEA's treatment of enforcement orders against carriers for failing to meet the requirements of section 103, Congress specified that such orders may be issued by courts if compliance is "reasonably achievable through the application of available technology ... *or would have been reasonably achievable if timely action had been taken*" (emphasis added).[23] Moreover, in assessing enforcement actions for CALEA noncompliance and the time to be granted for achieving compliance, Congress specified, among the factors to be weighed, good faith efforts to comply in a timely manner and the culpability or delay in undertaking efforts to comply.[24]

---

[22] As noted above, it appears certain technological solutions will be available by October 25, 1998 to meet the section 103 requirements. Therefore, it cannot seriously be maintained, under section 107(c)(2), that compliance is "not reasonably achievable through application of technology available within the compliance period."

[23] 47 U.S.C. 1007(a)(2).

[24] 47 U.S.C. 1007(b).

Law Enforcement strongly believes that the Commission should not reward the industry for its delay in the standards-setting process where such delay is responsible for the unavailability of certain technological solutions within the compliance period.[25] This is particularly so, since technological complexity has not been asserted as the grounds for not achieving timely CALEA compliance.

18. Sixth, section 107(c) expressly provides that only a telecommunications carrier may petition the Commission for an extension. Thus, there is no statutory authority for trade associations or others, outside of telecommunications carriers, to petition the Commission for an extension of the compliance date. Correspondingly, there is no statutory authority for the Commission to entertain petitions filed by entities having no statutory standing to petition the

---

[25] Some commenters (e.g., USTA, SBC) have suggested that the absence of a final capacity notice precludes manufacturers and carriers meeting the CALEA compliance date, and that this provides a basis for granting a blanket two-year extension for compliance (*e.g.*, USTA at 14; SBC at 24). Such assertions are misleading on a number of counts. The argument that switch manufacturers cannot proceed to implement the CALEA capability requirements without a set of *finalized* capacity numbers is erroneous. First, the Second Notice of Capacity, which sets forth detailed capacity numbers throughout the United States for every wireline carrier (county) and wireless carrier (service area) was issued on Jan. 14, 1997. Law Enforcement has assured the industry that these capacity numbers would not change in the Final Notice of Capacity. These hard, location-specific capacity numbers have undoubtedly enabled manufacturers to use them as guidance in the design and development process. Second, although there are some aspects of a manufacturer's solution that are capacity-dependent, the majority of the section 103 capability requirements are not. Thus, manufacturers could have progressed substantially without the Final Capacity Notice being issued, as long as a range of capacity numbers was known. More specifically, a manufacturer could proceed in developing methodologies to access call content and call-identifying information without regard to the capacity. Also, a manufacturer could proceed in identifying delivery protocols without regard to the capacity.

Importantly, Congress properly understood that capability and capacity have only a limited interrelationship. Accordingly, it specified in CALEA that the capability requirements were to be met by October 25, 1998, whereas the capacity requirements were to be met within three years of the final capacity notice.

Commission under section 107(c). This is because this CALEA section was intended to exclusively address carrier-specific factors that, if warranted, may support an individual carrier's extension request.

19. Seventh, Law Enforcement believes that CALEA does not permit blanket extensions of time to comply with CALEA. Congress recognized that each carrier's compliance issues, solution(s), and developmental efforts for modifying its equipment, facilities, and services (either independently or in conjunction with its switch manufacturer(s) and support service provider(s)) would vary. Congress, in section 107(c), sought to ensure case-specific equity and fairness for an *individual* carrier and Law Enforcement. Given the severe threats to effective law enforcement, public safety, and the Nation's security, section 107(c)(2) mandates that the Commission consult with the Attorney General in order to assess whether a particular telecommunications carrier's request for an extension is warranted given *its* particular equipment, facilities, or service. As noted above, Congress intended to keep the window of societal vulnerability as small as reasonably possible.

20. Because Congress intended these assessments to be made *on a case by case basis*, it enacted language specifically stating that it must be a telecommunications carrier which may petition the Commission for any justifiable extension of time to comply with section 103. Indeed, under section 107(c)(4), any extension granted must be specific and tailored in its application and shall apply to only that part of the carrier's business on which the new equipment, facility, or service is used.[26]

---

[26] Several telecommunications carriers (e.g., Bell South, Bell Atlantic) have encouraged the Commission to act upon CTIA's July 1997 petition to the Commission as it relates to granting an industry-wide two-year extension for compliance. Bell South Comments at 16; Bell Atlantic Comments at 8-9. However, as discussed *supra*, Law Enforcement believes that CTIA's petition lacks vitality since an interim standard has been published which supersedes CTIA's petition to establish a technical standard. Moreover, the Commission would not be empowered to grant such a "blanket" extension for all carriers, even if brought by carriers, since a proper telecommunications carrier petition must be

21. Congress prudently recognized that the factual basis for a particular carrier's petition must be tied directly to the particular circumstances of the petitioning carrier and to specific components of that carrier's network in question.[27] Given the serious impact upon the public safety, effective law enforcement, and the Nation's security, the Commission should decline to rewrite CALEA in a fashion inconsistent with the language used, and the intent evidenced, by Congress as it narrowly tailored the provisions regarding who could seek extensions, their breadth, and the grounds for them under law.

22. Finally, the Commission should consider the fact that the FBI and the Department of Justice recently have extended an offer to the leading manufacturers (and derivatively to their client carriers) to enter into agreements under which the Department of Justice would not pursue enforcement actions against the manufacturer or its carriers where compliance within the compliance date was in doubt because the particular manufacturer had not made available a technological solution fully compliant with CALEA section 103 requirements. Such agreements would cover specific switching platforms (or other non-switch solutions) and would include reasonable deployment schedules and verifiable milestones.

23. The Department of Justice also indicated, in this initiative, that it would support a carrier's petition to the Commission for an extension of the compliance date for the specific equipment named in the agreement and for the length of time specified in the agreement. Law Enforcement strongly believes that extensions, such as noted here, that are tailored to specific

---

specific and exclusive as to that carrier's own equipment, facilities, or service, as required under section 107. And, we do not believe that Bell South's, Bell Atlantic's or any other carrier's Comments were intended to be, or could properly be construed as constituting, a section 107 extension petition as to *their* particular equipment, facilities, or service.

[27] *See* H.R. Rep. No.827, 103rd Cong., 2d Sess., 18-19, *reprinted in* 1994 U.S.C.C.A.N. 3498-99, ("[The legislation] allows any company to seek from the FCC up to a two-year extension of the compliance date if retrofitting *a particular system* will take longer than the four years allowed for compliance" (emphasis added)).

carriers, specific equipment, and specific deployment schedules are consistent with the carrier- and case-specific treatment Congress required under section 107(c).[28] Proceeding with this Department of Justice initiative will obviate wholesale industry-wide extension petitions to the Commission. Where petitions are filed, they can be decided expeditiously because the Department will have endorsed them.[29]

## IV. REASONABLE ACHIEVABILITY UNDER SECTION 109 AND ITS INAPPLICABILITY UNDER SECTION 107

24. Law Enforcement previously responded to the Commission's request for comments as to whether the section 109 "reasonable achievability" criteria could be applied appropriately to a carrier petition for an "extension" under section 107.[30] In our Comments, we noted that sections 107 and 109 serve distinctly different purposes under CALEA, and that each addresses distinctly different issues.[31] Upon further consideration, and after reviewing the comments of AT&T[32] and others, Law Enforcement has now concluded that the reasonable achievability criteria of section 109 definitely should not be applied to, or considered in, section 107 extension petitions, nor should the Commission otherwise conflate these distinctly different provisions.

---

[28] Moreover, the Department of Justice's approach outlined here should be extremely effective in addressing and resolving the concerns of a substantial number of carriers and manufacturers with regard to specific equipment, facilities, and services, and it clearly does not constitute a legally impermissible and highly objectionable industry-wide "blanket" extension.

[29] Department of Justice initiative is set forth in a letter addressed to the Telecommunications Industry Association. *See* Letter of January 22, 1998 from Attorney General Janet Reno to Matthew Flanagan, President, TIA, attached hereto as Appendix B.

[30] The Commission's NPRM at 33-34.

[31] FBI Comments at 41-42.

[32] *See* AT&T Comments generally at 21-27.

25. As Law Enforcement noted in its prior Comments, section 107 essentially relates to the timing of compliance: that is, whether meeting the assistance capability requirements by October 25, 1998 is "reasonably achievable through application of technology available within the compliance period (emphasis added)."[33] By contrast, determinations of reasonable achievability under section 109 pertain to the broader aspects of technical and cost feasibility: that is, "whether compliance would impose significant difficulty or expense on the carrier or the users of the carrier's systems,"[34] and *presupposes that technological solutions are available to a carrier*. A careful reading of section 109 reveals that Congress envisioned that a section 109 petition would follow, only if required, a section 107 carrier petition for an extension.

26. As can be seen from the AT&T comments and otherwise,[35] if section 109 criteria and factors are applied to section 107 extension requests, confusion will needlessly abound, and Congress' original intent will be significantly distorted. For example, AT&T notes that section 109 allows up to one year for the Commission to make a determination about a reasonable achievability petition under section 109. While this is true, AT&T then links the time period for a section 109 reasonable achievability determination with its assertion that "[t]he industry is less than one year away from the CALEA compliance deadline and hardware or software to implement the industry standard is not available yet." (Emphasis added.)[36]

27. Aside from the irrelevance of an industry standard to meeting CALEA's

---

[33] 47 U.S.C. 1006(c)(2).

[34] 47 U.S.C. 1008(b)(1).

[35] AT&T argues that "carriers should be able to petition for a section 109(b) determination in conjunction with a section 107(c) determination." *Id.* at 27.

[36] *Id.* at 21.

compliance date, AT&T appears to be using the threat or prospect of multiple section 109 reasonable achievability petitions as a lever to force the Commission into "toll[ing] the compliance deadline automatically,"[37] which would in effect create a *de facto* automatic extension, prohibited by CALEA, by suggesting that failing to do so would cause "gaps" and "carrier doubts."[38] In addition, if, as suggested by AT&T, carriers could seek to evade compliance altogether under the section 109 reasonable achievability regime (and its mechanism for *deeming equipment to be compliant* under certain circumstances), when the only genuine issue may be whether compliant equipment is available by October 25, 1998 or shortly thereafter, it could only result in further distortion of Congressional intent.[39]

---

[37] *Id.* at 22.

[38] *Id.*

[39] *Id.* at 23. In addition, several commenters, including AT&T, misstate the meaning of the term "installed or deployed" as used in section 109 of CALEA. *See, e.g.*, AT&T Comments at 20. The CALEA Cost Recovery Rules, 28 C.F.R. part 100, define "installed or deployed" as follows: "'Installed or deployed' means that, on a specific switching system, equipment, facilities, or services are operable and available for use by the carrier's customers." (28 C.F.R. 100.10). When the FBI proposed this definition in the May 10, 1996 Cost Recovery NPRM (61 FR 21396), no commenters raised concerns about this definition of "installed or deployed." However, when the FBI published its Advance Notice of Proposed Rulemaking requesting *only* proposed definitions of the term "significant upgrade or major modification" (61 FR 58799), some commenters took that as an opportunity to argued that "deployed" should mean "commercially available prior to January 1, 1995" and should, therefore, be defined separately from the term "installed." The commenters in this proceeding before the Commission seek to make the same false distinction. The FBI believes that this belated attempt to interject a "commercially available" definition, as argued by these commenters in this NPRM, is both procedurally improper and substantively inconsistent with CALEA. In CALEA section 109(e)(3), the Submission of Claims provision, reads: "Such [Cost Control] regulations shall require any telecommunications carrier that the Attorney General has agreed to pay for modifications pursuant to [section 109] *and that has installed or deployed such modification* to submit to the Attorney General a claim for payment ...." (emphasis added). It is unlikely that Congress intended that carriers would be able to submit claims for payment simply because a piece of equipment was commercially available. It is also unlikely that Congress intended that the Attorney General agree to reimburse carriers for commercially available equipment sitting in their warehouses. Rather, it seems clear that Congress intended that

28. Law Enforcement believes that it is critical to look to Congressional intent, as embodied in these provisions. Had Congress intended to permit the criteria and "factors" specified in section 109 to be applied to section 107 extension petitions, it could have easily done so, but it did not. Similarly, it is clear that Congress did not intend for these very different provisions to be merged and intermingled. Instead, as noted above, Congress strictly limited evaluations of petitions for extensions under section 107 to the *availability* of technical solutions *within the compliance period*. Moreover, Congress made clear that only a carrier could petition for an "extension" under section 107. Under section 109, however, a carrier or other interested party can petition the Commission, based upon factors delineated in section 109(b)(1), which are unrelated to the timing of compliance. The Commission should defer to the CALEA-regime as Congress created it; the Commission should resist being persuaded into rewriting it.

## V. DEFINITION OF TELECOMMUNICATIONS CARRIER

29. Law Enforcement, along with TIA, The Center for Democracy and Technology (CDT), The Electronic Frontier Foundation (EFF), and Computer Professionals for Social Responsibility (CPSR), agrees with the Commission's 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, Law Enforcement continues to support the interpretation that the 1996 Act by its own terms did not modify or supersede existing law, unless expressly so stated. Moreover, GTE states that "CALEA is designed to protect the American public from criminal activity." Law

---

claims be submitted only for such equipment for which the CALEA solution was "operable and available for use" or "deployed."

Enforcement agrees and continues to advocate that all entities defined as common carriers for purposes of interpretation of the 1996 Act are telecommunications carriers subject to CALEA. Thus, when drafting its final rules, the Commission should not modify the definition of "a telecommunications carrier" or "information services" for the purposes of interpreting CALEA.

30. In the post 1996 Act environment, Law Enforcement believes that there may exist telecommunications companies that do not hold themselves out to serve the public indiscriminately that should also be treated as "telecommunications carriers" by the Commission. Otherwise, companies that hold themselves out to serve particular groups, may, intentionally or inadvertently, undermine CALEA. Thus, Law Enforcement, TIA and AT&T, for unrelated reasons, believe that the Commission should not incorporate the word "indiscriminately" into the definition of a telecommunications carrier.[40] Law Enforcement continues to advocate that the term "indiscriminately" may cause an unnecessary ambiguity regarding the reach of the term "telecommunications carrier" under CALEA.[41] Law Enforcement, however, agrees with the definition, articulated by USTA, CTIA and AT&T, that CALEA applies to all classes of telecommunications carriers that offer telecommunications services to the public for hire and provide the subscriber with the ability to originate, terminate, or direct communications. Law Enforcement concurs with this definition because it is consistent with the statutory language of section 103 of CALEA.[42]

---

[40] TIA and AT&T believe that the definition proposed by the Commission is too broad in nature. Law Enforcement disagrees and believes that the definition should be as expansive as possible. Thus, Law Enforcement advocates that the word "indiscriminately" should not be used in the Commission's final rules.

[41] If the Commission were to adopt the term "indiscriminately," 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.

[42] *See* CALEA section 103, *codified at* 47 U.S.C. § 1002 (stating that "a telecommunications carrier shall ensure that its equipment, facilities, or services that

31. Furthermore, 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 is concerned specifically that any type of illustrative list could mistakenly be interpreted as all-inclusive. Thus, Law Enforcement disagrees with TIA and Motorola's assertion that the definition of a telecommunications carrier should be interpreted narrowly based upon the limited list of entities noted in the House Judiciary Committee Report.[43] This report states that:

> This definition encompasses *such service providers as* local exchange carriers, interexchange carriers, competitive access providers (CAPS), cellular carriers, providers of personal communications services (PCS), satellite-based service providers, cable operators and electric or other utilities that provide telecommunications services for hire to the public, and *any other common carrier* that offers wireline or wireless service for hire to the public. (emphasis added).

The House Judiciary Committee Report's use of the phrase "such service providers as," clearly indicates that the above list was merely meant for illustrative purposes. Moreover, the Report's indication that other unspecified carriers were to be included is made clear by its use of the phrase "any other common carrier." Further it is obvious that the House Judiciary Committee recognized the fact that it could not foresee and list all of the possible telecommunications providers that would be subject to CALEA. Thus, Law Enforcement believes that TIA and Motorola's asserted reliance upon the legislative history in order to narrowly interpret the definition of a telecommunications carrier under CALEA is misguided. Rather, Law Enforcement considers the definition of a telecommunications carrier under

---

provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of ...").

[43] *See* H.R. Rep. No. 103-827 at 20 (1994).

CALEA to be broad in nature because the definition encompasses not only common carriers for hire to the public, but "cable operators and electric or other utilities[44] that provide telecommunications services for hire to the public."[45]

32. Law Enforcement continues to recommend that the Commission not exercise its discretion pursuant to section 102(8)(C)(ii) of CALEA, which allows the Commission to exclude specific classes and categories of carriers from the obligations of CALEA after consultation with the Attorney General. AT&T agrees and currently believes that it is unnecessary for the Commission to exempt any category of telecommunications providers, but if the Commission were to exempt a category of telecommunications providers, it should do so pursuant to a petition or upon its own motion.[46] In addition, AT&T and BellSouth agree that the Commission currently does not need to establish procedures for exempting categories of telecommunications providers. Law Enforcement agrees with both AT&T and BellSouth. The Commission should also monitor continually new services and technologies because Law Enforcement believes that they could become a substantial replacement for local exchange service in the future.[47] Law Enforcement will, in the future, consult with the Commission with regard to persons or entities offering services that become a replacement

---

[44] *See* 47 U.S.C. § 224(a)(1) (defining the term utility, in relation to pole attachments, as "any person who is a local exchange carrier or an electric, gas, water, steam, or other public utility "). By adding the term "utility" the definition of a telecommunications carrier was significantly broadened, thus, adding additional support to Law Enforcement's contention that the definition of a telecommunications carrier was meant to be construed broadly under CALEA.

[45] *Id.* Furthermore, SBC and Bell Atlantic Mobile concur with Law Enforcement that the definition of a telecommunications carrier under CALEA should include cable operators and electric and other utilities that provide telecommunications services to the public.

[46] *See* section 102(8)(C)(ii) of CALEA.

[47] As a recent example, the Commission has undertaken a proceeding dealing with Local Multipoint Distribution Services (LDMS), one facet of which pertains to nonmobile wireless local loop service, a replacement for local wireline exchange service.

for local exchange service.

33. Law Enforcement maintains that paging systems are clearly included within the definition of "a telecommunications carrier" for the purposes of interpreting CALEA because paging systems generally fall within the definition of a common carrier. Individuals must call the paging service and then communicate their alphanumeric or voice messages, such as phone numbers to call, or other content-based messages. Moreover, most common carriers for hire now provide phone systems that offer paging channel access. Thus, Law Enforcement believes that the definition of a telecommunications carrier, and any illustrative list the Commission may choose to create, must include pagers.

34. Law Enforcement would like to clarify the record with regard to the comments on pagers offered by PCIA and AirTouch. PCIA in its comments has stated that "with the passage of the Clone Pager Authorization Act" that any CALEA-based rule promulgated by the Commission would add an unnecessary level of cost and complexity to carrier operations. PCIA acknowledges, however, that Congress has not yet enacted this legislation.[48] Nonetheless, passage of this act would not, and is not intended to, address CALEA compliance. Its chief feature is the treatment of the legal standard that would be required for (only numeric) pager interceptions. It is not legislation for pagers that addresses advanced communications technologies, services, and features -- which is the central subject matter of CALEA.

35. AirTouch, in explaining its current procedures for pager interceptions, notes that it provides Law Enforcement with a "clone" pager to receive messages simultaneously with the paging customer who is the subject of a court order. AirTouch thus appears to suggest

---

[48] Only the Senate has passed it (S. 170, 105th Cong. 1st Sess. (1997)); the bill is currently pending in the U.S. House of Representatives.

that because, in its estimation, it is already meeting CALEA's assistance capability requirements there is no need for it (or paging companies generally) to be treated by the Commission as a telecommunications carrier. Unfortunately, "clone" pager-based interceptions have only limited effectiveness and utility, and fail to fully meet CALEA's section 103 requirements. Consequently, inclusion of pagers under CALEA is absolutely imperative for law enforcement and public safety purposes.

36. Finally, the Commission should understand that a significant number of electronic surveillance efforts conducted by Law Enforcement involve pagers.[49] Indeed, pager interceptions are extremely frequent in drug-trafficking investigations -- the highest category of Federal and State electronic surveillance activity.

37. Law Enforcement, along with USTA, CTIA, PCIA, SBC, GTE, BellSouth, and Ameritech, advocates that resellers should be included in CALEA's definition of a telecommunications carrier. Moreover, PCIA states that classifying resellers as common carriers for purposes of CALEA is consistent with the manner in which the Commission and the courts have traditionally categorized resellers.[50] Thus, it is Law Enforcement's contention that a reseller is accountable to assist Law Enforcement in any way technically feasible under CALEA. Law Enforcement agrees with Paging Network's statement that a carrier that packages or offers services that are provided over another network is not in a position to effect an interception in the other carrier's network. However, Law Enforcement agrees with

---

[49] In 1996, 17 percent (171 cases) of intercepts involved electronic devices, including digital display pagers and voice pagers. STATISTICS DIVISION, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, "1996 Wiretap Report," Table 6.

[50] *See The Resale and Shared Use Order*, 60 FCC 2d 261, para. 8 (1976)(stating that "an entity engaged in the resale of communications service is a common carrier, and is fully subject to the provisions of Title II of the Communications Act"). *See also National Association of Regulatory Utility Commissioners v. FCC*, 525 F.2d 630, 641; 553 F.2d 601, 608 (D.C. Cir. 1976).

SBC and BellSouth that if a 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.[51] Finally, Law Enforcement also contends that the definition of a telecommunications carrier should include resellers with prepaid calling card or other similar services. Law Enforcement increasingly is confronted with criminals using prepaid calling cards; absent coverage, loop holes may be created.

38. Law Enforcement concurs with Bell Atlantic, SBC, BellSouth, and Ameritech in supporting the Commission's determination that commercial mobile service providers fall within CALEA's definition of telecommunications carriers. Nextel in its comments, however, contends that CALEA would have a serious adverse technical, operational, and financial impact on specialized mobile radio (SMR) systems that do not utilize intelligent switching capability and offer seamless handoff to customers and push-to-talk dispatch services that are offered on a stand alone basis or as a unique feature in a package of interconnected services. In addition, Nextel believes that by applying CALEA to SMRs the Commission would run counter to its goals of promoting advanced technologies and creating a competitive marketplace. Nextel, however, admits that it is a "common carrier to the extent it provides interconnected two-way mobile phone service to which CALEA obligations should apply."[52]

39. Nextel asserts, however, that the Commission cannot impose CALEA upon non-interconnected services because there is no existing wiretap or interception technology. However, the prior existence of wiretap or interception technology is irrelevant and is not

---

[51] In all likelihood, the network carrier would be necessary for the interception, while the resale carrier would supply the customer information.

[52] Nextel Comments at page 7.

dispositive. Rather, the standard for determining "a telecommunications carrier" is measured or defined by the type of telecommunications services provided by the entity. Once an entity is deemed to be a covered "telecommunications carrier" under CALEA, it is obligated to provide the CALEA section 103 assistance capabilities to Law Enforcement.

40. While Law Enforcement appreciates Nextel's concerns, Nextel itself has correctly stated that commercial mobile radio service (CMRS) providers are included in the definition of a telecommunications carrier under section 102(8) of CALEA. In addition, the Commission has concluded that the CMRS classification encompasses all cellular, PCS, and those SMRs that are interconnected to the public switched telephone network.[53] Since Nextel is connected to the public telephone-switched network and is a telecommunications service provider for hire by the public, Law Enforcement strongly believes that the Commission must deem Nextel to be a telecommunications provider under section 102(8) of CALEA. Relatedly, 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 a private mobile service does not become a telecommunications service provider for hire to the public or replace a substantial portion of local exchange service. Once the private mobile service provider offers any portion of its service 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.

41. Law Enforcement, along with SBC, Ameritech, USTA, and BellSouth, agrees with the Commission's conclusion that providers of pay telephones are not telecommunications carriers for purposes of CALEA. SBC, Ameritech, and BellSouth

---

[53] *Second Report and Order*, GN Docket No. 93-252, 9 FCC Rcd 1411 (1994) at paras. 82 *et seq.*

contend that pay telephone providers should be excluded from the definition of CALEA because they do not provide transport or switching services. Law Enforcement agrees and further believes that pay telephones have more to do with end-user terminal equipment than with telecommunications services. Moreover, any type of terminal equipment 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*.

42. Law Enforcement, along with other commenters,[54] agrees with the Commission's tentative conclusion that exclusive providers of 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. Metricom states that the language of section 103(b)(2) is ambiguous as to situations where a company is an information service provider and a telecommunications service provider. Thus, Metricom and Law Enforcement agree that the express definition of a telecommunications carrier contemplates that an entity could be subject to CALEA only for its services that are not information services.

43. In addition, Law Enforcement concurs with BellSouth, which states that when pure information service providers begin offering telecommunications services to the public, and in general begin holding themselves out as providers of common carrier services, the Commission should then deem them to be telecommunications carriers and require them to comply with CALEA. Although information service providers are exempted under CALEA, this does not relieve them of their responsibilities under other applicable electronic surveillance laws. Thus, Law Enforcement continues to advocate that the Commission adopt a narrow definition of information services to ensure that Law Enforcement is capable of intercepting criminal use of such services.

---

[54] *Accord* USTA, NTCA, U S West, SBC, Ameritech, and Metricom.

## VI. CARRIER SECURITY POLICIES AND PROCEDURES

44. The industry comments on the issue of the security policies and procedures that carriers should be required to adopt reflect a misunderstanding of CALEA, and the ways in which advances in technology have shifted the nature of the roles that Law Enforcement and telecommunications providers must play to implement lawful electronic surveillance. As stated in the FBI's original comments, past electronic surveillance was conducted almost exclusively in the local loop on two-party, plain old telephone service (POTS) communications, and law enforcement technical agents generally were able to effect authorized intercepts themselves at locations in the "local loop" removed from the carrier's central office or switch. In this manner, Law Enforcement was able efficiently and successfully to intercept *all* of the communications content and call-identifying information supported by a subject-subscriber's POTS telephone service.[55] This is no longer the case; due to technological changes, Law Enforcement is often impeded from intercepting all of the lawfully authorized communications content and call-identifying information from a subject-subscriber's telephone service.[56]

---

[55] Law Enforcement did serve a secondary "assistance order" on a carrier to obtain relevant line and appearance information and delivery circuits. 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 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). § 18 U.S.C. § 2518(4).

[56] Telecommunications frequently are no longer the two-party POTS calls of the past; multiparty calls having several different "legs" have become common. With the advent of subscriber-initiated multiparty calls, Law Enforcement is able to intercept only *part* of the communications occurring over the subject-subscriber's telephone service—those occurring over the leg of the call that the subject-subscriber's terminal equipment is actually connected to at any point in time. The subject-subscriber may, in fact, be using another terminal device. 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,

45. Just as there has been a need to shift from "local loop" interceptions to central office or network-based interceptions, there necessarily will be a corresponding shift away from law enforcement personnel to telephone carrier personnel in the implementation of sensitive electronic surveillance efforts. Previously, Law Enforcement could assure itself that guarantees of trustworthiness and accountability existed for the personnel who conducted these sensitive (and often classified) interception efforts because it was law enforcement personnel who were directly responsible for their implementation. Now, with carrier personnel being responsible to implement electronic surveillance, equivalently strong guarantees must exist. These guarantees are absolutely essential to preserve the security and integrity of surveillance information, and its reliability in criminal prosecutions where the carrier personnel responsible for implementing an intercept are often required to testify in court.

46. Notwithstanding the change in how interceptions are executed, and the change in who executes them, Law Enforcement's essential electronic surveillance requirements have not changed. These requirements 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 upon these requirements being met.

47. As such, although Law Enforcement recognizes the need not to unduly burden the administration of internal carrier systems and procedures, it is not within the discretion of Law Enforcement to forego extremely important security, integrity, and evidentiary requirements necessitated by statute, by the courts, and the Rules of Evidence. Therefore,

---

subscribers are being offered calling features and services (e.g., conference calling, call forwarding) that can rapidly change the nature of the subscriber's service, almost instantaneously, which if unaddressed, in turn, could lead to the loss of evidence, confusion with regard to evidence, and the insufficient procurement of interception delivery channels and circuits by Law Enforcement.

it is imperative that the Commission craft rules, procedures, and policies that will accommodate Law Enforcement's investigative and evidentiary needs and address public safety demands.

48. In analyzing CALEA, it is important to recognize that Congress 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, through whatever technical modifications necessary.[57] Congress did not intend to preserve or maintain past ineffective electronic surveillance capabilities that were no longer working fully or properly. Moreover, Congress clearly anticipated that just as technological changes would have to be made so too would there have to be changes in way surveillances are executed -- with much of the responsibility shifting to carrier personnel in the carriers' switching premises.[58]

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

#### 1. Intercept Authorizations

49. 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. § 2518(4), which requires the provision by carriers of "all information, facilities, and technical assistance"

---

[57] *See* FBI comments to NPRM at 10 n.17 (*filed* Dec. 12, 1997).

[58] *See* 47 U.S.C. § 1004 ("interception[s] and... access... effected within its switching premises can be activated only... with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.").

necessary to accomplish the interception. Nearly identical assistance provisions are set forth in the pen register and trap and trace statutes.[59]

50. 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, as amended) refers to the authority granted to a carrier's employee by the carrier to engage in interception activity.[60] By contrast, the first possible construction identified by the Commission in paragraph 25 of the 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.[61] Law Enforcement strenuously asserts that there is absolutely no language in CALEA or its legislative history that suggests that CALEA was intended to alter a carrier's response to a facially-valid court order or other lawful authorization. That is, there is absolutely nothing in CALEA suggesting that the Act intended to confer some new, enhanced, and *de novo* review authority on carrier personnel regarding the legal process it receives from Law Enforcement. Nor does Law Enforcement believe that CALEA grants discretion to the Commission to confer such authority on carriers.

51. Indeed, Law Enforcement reiterates that there have been anecdotal reports of

---

[59] *See* 18 U.S.C. § 3124.

[60] *Accord* US West, BellSouth.

[61] Law Enforcement agrees that carriers have a specific CALEA-based 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.

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.

52. It is unnecessary and highly problematic, therefore, for the Commission to adopt a rule that carriers include in their internal policies and procedures information provisions that separately define the legal authorizations required for carriers to implement an intercept. In fact, carrier maintenance of such detailed authorization criteria would inevitably and erroneously suggest to carrier personnel that they are supposed to test the legal process against some "look up table" of statutes which are often somewhat complex, and then 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, authorizations, and certifications under the electronic surveillance laws in this regard. The Commission should clarify that its rules do not purport to alter the electronic surveillance laws.

53. Law Enforcement agrees with PageNet's statement that lawful electronic surveillance can be initiated under circumstances other than those identified by the Commission, *i.e.*, in the emergency situations enumerated under 18 U.S.C. § 2518(7).[62]

---

[62] *Accord* GTE, BellSouth. Law Enforcement strongly disagrees with PageNet, Omnipoint, GTE, and BellSouth that the Commission should clarify its proposed rules to include these means of legal process.

Omnipoint believes that the Commission should not require carriers to incorporate policies and procedures relating to exigent circumstances found in 18 U.S.C. § 2518(7) because incorporating this legal standard into carrier policies and procedures will only confuse the carrier personnel responsible for surveillance assistance. Moreover, SBC and GTE agree with Law Enforcement 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.[63] Law Enforcement strongly agrees, but would go further and urge the Commission to state that a carrier need only receive a facially valid court order, exigent circumstances certification, or other lawful authorization to be required to provide electronic surveillance assistance to Law Enforcement.

54. The Commission should also include in its final rules that the presentation by telecopier of a facsimile copy of a court order or an emergency certification is sufficient 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. Furthermore, Law Enforcement agrees with PageNet that if a carrier complies with these forms of authorization, carriers should be shielded from liability if they initiate an interception at the behest of any law enforcement agency.

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

55. 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

[63] SBC and GTE believe that their respective employees should not be required to look behind orders which initiate valid electronic surveillance.

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 carrier personnel and administrative procedures regarding electronic surveillance implement meaningful security protections.

### 1. Illegally Intercepted Communications

56. 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 intentionally illegally intercepted communications.[64] USTA argues that CALEA section 105 does not extend vicarious criminal and civil liability to a carrier and that the Commission does not have authority to extend liability in this manner.

57. Law Enforcement is charged with the responsibility of protecting citizens against

---

[64] 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 may result in a finding of vicarious liability. Thus, to the extent a carrier is exposed to possible derivative liability under *respondeat superior*, the risk of exposure will be substantially mitigated, if not eliminated, by compliance with CALEA.

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. Thus, Law Enforcement agrees with SBC and BellSouth that carriers must ensure that only surveillance in accordance with a court order or other lawful authorization is performed within a carrier's switching premises. Prohibitions against illegal wiretapping and disclosure by carrier employees of the existence or content of intercepted communications are contained in 18 U.S.C. § 2511.[65]

### 2. Designated Personnel

58. Law Enforcement continues to agree with the Commission's proposal in Paragraph 30 of the NPRM which requires carriers to designate specific employees to assist law enforcement officials in implementing lawful interceptions.[66] Indeed, it is clear that by use of the terms "authorized" and "designated" in its explanation of CALEA's systems security and integrity provisions, Congress presupposed that electronic surveillance would be entrusted by carriers to a small group of select employees.[67] BellSouth concurs and states that it is sound practice for carriers to designate specific employees, officers, or both, to assist Law Enforcement in implementing lawful interceptions. What should separate this group of

---

[65] 18 U.S.C. § 2511. Both carriers state that no such restrictions are contained in CALEA.

[66] Omnipoint in its comments states that it concurs with the Commission's proposed rule and already has such procedures in place.

[67] *See* H.R. Rep. No. 103-827, at 26 (1994).

designated personnel from the broad mass of carrier employees is a higher guarantee of trustworthiness given the great sensitivity of conducting electronic surveillance. In this manner, safeguards can be built into the system that protect the integrity, security, and evidentiary validity of electronic surveillance information.

59. In its initial comments, Law Enforcement contended that for evidentiary and security reasons, it was greatly concerned by the Commission's suggestion that non-designated employees be permitted to effect surveillance work. Law Enforcement believed that only specifically designated carrier personnel should be permitted to have any involvement in, knowledge of, or access to electronic surveillance or information concerning it. BellSouth and Teleport disagree because it would require them to designate every network technician in the company. Thus, they believe that the Commission, in its final rules, should allow non-designated personnel to effectuate electronic surveillance provided that they do so unknowingly. Law Enforcement concurs with BellSouth and Teleport that, in these limited circumstances, it would be acceptable for non-designated personnel to participate in the implementation of electronic surveillance, provided they did so unknowingly.

60. Accordingly, Law Enforcement believes that the procedures employed by a 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 must be precluded. 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.

61. SBC, for example, has procedures in place, which ensure that a dedicated

organization in its company is responsible for ensuring the following:

- that assistance to Law Enforcement in electronic surveillance is well-managed, protects privacy and the confidentiality of the intercepted communications and the activity itself;
- that surveillance devices are lawfully authorized and that, when detected, unlawful devices are removed and reported to Law Enforcement; and
- that court orders or other lawful authorization are presented by law enforcement agents.

These types of procedures, in Law Enforcement's view, constitute a sound framework upon which to base a complete set of CALEA-compliant security policies and procedures, as discussed below.[68]

62. Law Enforcement wishes to reiterate that, 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

[68] SBC proposes that rules be adopted by the FCC only if and when a carrier is found to have been repeatedly unable or unwilling properly to preserve the goals of CALEA and the related provisions of 18 U.S.C., stating that carriers who have provided assistance to Law Enforcement in the past already have in place practices for proper employee conduct and record keeping. The FCC acknowledges in para. 74 of the NPRM that many carriers currently have in place practices for proper employee conduct and recordkeeping. For this reason, US West, BellSouth, and Ameritech agree with SBC that the FCC need only provide general guidance regarding the conduct of carrier personnel. Since carriers are in some fashion already using security guidelines, it can hardly be argued that uniform and comprehensive guidance from the Commission would be burdensome.

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.

63. 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.

64. Law Enforcement agrees with Teleport that designated personnel should be limited to a core group of point-of-contact personnel who have the primary responsibility for carrying out surveillance.[69] In addition, Law Enforcement and Teleport agree that a list of the core group of designated personnel be kept confidential and provided to Law Enforcement only upon request. Law Enforcement believes that it is important to maintain such information because carrier personnel may be required to testify in a criminal prosecution as to how the intercept was installed and maintained. Absent a clear "chain of custody" for the intercept, the electronic surveillance information upon which successful prosecutions depend might be found deficient under Title III.

---

[69] *See* GTE agrees that it is appropriate for there to be a designated "single" point of contact for every carrier.

65. Further, Law Enforcement 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 recordkeeping 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. In addition, a record of the personnel involved in the implementation of intercepts must be maintained by the carrier and available in the event that Law Enforcement requires such information in order to support the surveillance's implementation obtained under a specific electronic surveillance order or if a question arises as to the integrity of the implementation.

66. Law Enforcement offers the following with regard to the rules the Commission should consider in implementing CALEA section 105. 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 for 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, social security number), official titles, and contact numbers (telephone and pager). Nondisclosure agreements should be executed by such personnel.

67. 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.

68. Finally, another key requirement is Law Enforcement's need to have access to assistance from carriers with respect to the implementation or maintenance of electronic surveillance intercepts on a 24-hour per day, seven-day a week basis. This is simply the practical, operational reality that Law Enforcement faces in the conduct of its activities. If, for example, an intercept ceases to function or an emergency intercept is required outside of normal business hours, Law Enforcement must be able to restore or implement such an intercept without delay. In an environment where electronic surveillance is switch based, and carrier involvement is therefore required, assistance from carrier security personnel must be available to Law Enforcement on the same, full-time basis.

### 3. Recordkeeping

69. 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. Law Enforcement and Omnipoint both concur with the Commission's general proposal that carriers should be required to keep records of the conduct of surveillance, and that those

records be compiled contemporaneously with the start of each interception.[70] Omnipoint states that it already keeps the records, as proposed by the Commission. In addition, the Commission may wish to require that the carriers 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 (including FISA-related materials) should be maintained in a separate and secure storage area, access to which should be limited to a small number of designated carrier personnel.

70. Upon review of all the comments, Law Enforcement agrees with Bell Atlantic Mobile that carriers should not be required to retain electronic surveillance-related records for ten (10) years. While the Commission is correct that, under Title III, electronic surveillance records must be maintained for a 10-year period, CALEA does not impose a record retention obligation directly on carriers.[71] Law Enforcement is already required to

---

[70] 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 for 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, even though, for example, an extension or emergency authorization may have been obtained before the expiration of the original order, but potentially after normal security office business hours (or the order may expire during a weekend). The presence of carrier personnel would provide assurance that there would be no interruption in a surveillance in such a circumstance.

[71] *Accord* AirTouch, PrimeCo, PageNet, Sprint Spectrum, USTA, and Ameritech.

retain records for a ten (10) year period under 18 U.S.C. § 2518(8)(a), and a duplicative retention obligation for carriers would not be necessary. However, for evidentiary and record retention purposes it is important and necessary that Law Enforcement be able to maintain the essential details related to each electronic surveillance effort, including information regarding which carrier personnel effected the surveillance, etc.

71. Therefore, Law Enforcement believes that carriers should be required to create records and transmit the originals, or certified copies, of all electronic surveillance records to the cognizant law enforcement agency by no later than five (5) days following the conclusion of an intercept. This way the record retention obligation can be handled properly by Law Enforcement. Law Enforcement understands that, while not necessarily required by law, carriers may wish to retain copies of those records.[72] In such event, the Commission should require that any records retained by a carrier after the originals or certified copies have been delivered to Law Enforcement be maintained in the same separate and secure manner as described above. Law Enforcement emphasizes that these records are subject to the nondisclosure provision set forth in 18 U.S.C. § 2511.

72. 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 carriers shall maintain records that will include the date, time, purpose, and identity of the third party personnel involved for each access permitted.[73]

---

[72] AirTouch and PrimeCo state in their comments that they currently retain their records for three years because the statute of limitations for civil suits against carriers and their employees is two years.

[73] 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 these recordkeeping provisions.

**4. Affidavits**

73. Law Enforcement agrees with the Commission that, for evidentiary purposes, carrier-based electronic surveillance must be implemented in a manner that enables the cognizant law enforcement agency to identify the relevant factual circumstances of the particular intercept. The Commission has proposed that each employee involved in an interception prepare and execute an affidavit each time they perform an interception and that such affidavits be prepared no later than 48 hours from the time of the interception.

74. According to a majority of carriers, this requirement is unnecessary.[74] Based on the above carriers' comments and Law Enforcement's prior experience, Law Enforcement agrees that a less stringent means than an affidavit would suffice to show the validity of the implementation of an electronic surveillance. A method, such as a single certification executed by the security officer in charge, that captures the relevant factual information required by Law Enforcement would be appropriate and consistent with CALEA. The execution of a single certification for each surveillance effort would suffice in place of a more formal affidavit executed by all of the carrier personnel involved and would reduce a carrier's paperwork burden.

75. As to the contents of a certification, Law Enforcement agrees with Omnipoint that the Commission's proposal in Paragraph 31 of the NPRM that the carrier employee or officer who oversees interception activity should be required to execute a document containing each of the items listed by the Commission in its proposal.[75] Law Enforcement

---

[74] *See* Ameritech, BellSouth, Bell Atlantic Mobile, 360 Degree Communications, AT&T, GTE, SBC, and PrimeCo.

[75] Omnipoint states that it already keeps such records.

appreciates AirTouch's concern that the paperwork burden on carriers should be minimized as much as possible. Law Enforcement is well aware of the possible paperwork burden placed upon carriers by the Commission's proposed rules, and thus has sought to minimize them to the extent possible. Law Enforcement, however, believes that evidentiary requirements far outweigh the burdens here. In order to effectuate a valid electronic surveillance, Law Enforcement must ensure that the intercept meets the evidentiary threshold needed to introduce the electronic surveillance evidence into a court of law. Thus, the proposal that certification be prepared only by the employee or officer responsible for overseeing the interception activity is both reasonable and appropriate.

76. The certification should also 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 or officers is a designated person, the individual personnel records of those individuals should contain the requisite certification concerning non-disclosure of intercept information. Moreover, Law Enforcement proposes that any such document include an additional item stating that the signatory understands that unauthorized disclosure of intercept information is an actionable offense, potentially subjecting its perpetrator to criminal or civil penalties, including imprisonment or fine, or both.

77. Law Enforcement, however, still differs with the Commission's proposed Item 4. Law Enforcement continues to believe that Item 4 should be deleted because it is impossible for carrier security personnel to know, in real time, when the interception must lawfully terminate. Moreover, 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 slightly 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 wireless networks, routing numbers and line identities may be insufficient to connect a particular telephone number to a specific subscriber.[76]

78. Finally, Law Enforcement wishes to reiterate that the paperwork burden should never impede the timeliness with which intercept requests are implemented. The timeliness with which Law Enforcement receives such information is critical to the maintenance of the integrity and evidentiary validity of electronic surveillance information.

### 5. Reports of Violations-Compromises

79. Law Enforcement, SBC, GTE, Ameritech, BellSouth, and Bell Atlantic Mobile all concur that it is a carrier's affirmative obligation to report violations of its security policies and procedures and compromises, or suspected compromises, of authorized electronic surveillance to the affected law enforcement agency, or agencies, when the compromise is related to the potential unauthorized disclosure of a surveillance or other law enforcement activity. Law Enforcement considers this to be essential 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

---

[76] 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).

suspected compromises, to the carrier security office immediately upon discovery. At a minimum, Law Enforcement strongly urges that the Commission require that no more than two (2) hours be allowed to elapse between the time of 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.

80. Law Enforcement also advocates that 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 be reported immediately to the FBI or the cognizant law enforcement agency for further investigation.[77] At a minimum, Law Enforcement presumes that the employee would be reassigned immediately pending the outcome of the investigation. Law Enforcement, based upon past experience, understands this to be the practice now followed by most carriers.

81. Law Enforcement believes that the standard that should be applied in determining whether an intercept may have been compromised is 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 has 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.

82. Law Enforcement, however, believes that such violations and compromises of

---

[77] To allay the concerns of NTCA, Law Enforcement is only proposing, in this context, that carriers report illegal electronic surveillance. Specifically, under 18 U.S.C. § 2511, illegal electronic surveillance requires intentional, as opposed to negligent or inadvertent, conduct. *See also* 18 U.S.C. § 2520 (providing a good faith defense).

intercepts should be reported to the Commission every two years when a carrier must re-certify that it is complying with the security policies and procedures mandated by CALEA and its implementing regulation.[78] In addition, Law Enforcement and SBC agree that reports made to the Commission relating to compromises should be strictly confidential, and not put in the public record. Law Enforcement believes that such reports would enable the Commission to exercise more effectively its continuing jurisdiction over CALEA-related matters.

### 6. Timeliness

83. Law Enforcement continues to believe that one of the most critical factors affecting the efficacy of electronic surveillance is the timeliness with which intercepts are implemented. 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. Thus, Law Enforcement disagrees with SBC's comments that the Commission should refrain from adding administrative rules relating to timeliness of effectuating a court ordered electronic surveillance.

84. Law Enforcement is well aware that the more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays. 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

[78] *See infra* "Certification of CALEA Requirements."

complete their internal approval and documentation process and implement the interception within eight (8) hours of receiving the court order, certification, or consent. For exigent circumstances, in cases under 18 U.S.C. §§ 2518(7), 3125, no more than two (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, seven (7) days a week.

85. Law Enforcement still 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 not only result in the loss of critical evidence, but they also endanger public safety by inhibiting Law Enforcement's ability to respond in emergency circumstances. Moreover, a time period longer than two (2) hours would result in a needless waste of the law enforcement resources being dedicated to an inoperative electronic surveillance.

86. 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 reiterates that 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, communication content, and other related electronic surveillance functions. Such a point of contact is commonly in place today with regard to carriers and law enforcement officers specializing in electronic surveillance. Law

Enforcement supports the efforts by the carriers and Commission to meet this obligation in the least burdensome manner possible.

### 7. Certification of CALEA Requirements

87. Law Enforcement still contends that both Title III and CALEA apply across the board to small and large carriers alike. Law Enforcement also believes that public safety and security concerns should not vary according to the geography or the size of the carrier. Therefore, the CALEA regulatory requirements 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.

88. For these reasons, Law Enforcement continues to disagree with the Commission's proposal, stated in Paragraph 35 of the NPRM, which defines 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. 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.[79]

---

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

89. A majority of commenters contend that all competitive carriers, not just small carriers with revenues less than $100 million, should have the opportunity to take advantage of the self-certification procedures that the Commission has proposed.[80] The commenters premise their arguments on the belief that streamlined procedures would promote the public interest, thereby reducing the administrative burden and expense and thus increasing efficiency. In addition, AirTouch asserts that it is not clear how competition would be enhanced if market participants were required to divulge their internal policies and practices.[81] Based upon the carriers' submissions, Law Enforcement now agrees that all carriers, regardless of their size, need only certify initially that they are in compliance with the security policies and procedures mandated by CALEA and its implementing regulation, and then re-certify to such compliance every two (2) years thereafter. Requiring only such certification will substantially decrease the proposed reporting burdens placed on carriers. Moreover, Law Enforcement agrees with PageNet that carriers should only provide their internal security compliance manuals upon request by the Commission or Law Enforcement.

90. In order to ensure standard security policy procedures, Law Enforcement advocates that the Commission develop standardized forms to assist carriers in designing CALEA compliance manuals.[82] This would ensure that identical standards would be applicable to large and small carriers alike. The Commission could even issue a manual containing a template set of security policies and procedures, which the adoption of and

---

[80] *Accord* PageNet, 360 Degree Communications, PrimeCo Personal Communications, and PCIA, CTIA, and AirTouch.

[81] AirTouch further states that given the fact that carriers have a long history of meeting Law Enforcement's interception requirements without invading customers' substantial privacy interests, there is no reason to now require competitive carriers to submit their internal compliance manuals to the Commission for review.

[82] *Accord* PowerTel.

adherence to could be deemed by the Commission to be CALEA compliant.

91. Law Enforcement is willing to work with Commission staff to develop the appropriate forms, but wishes to emphasize that their primary concerns are that the timeliness, accuracy, security, and evidentiary validity 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.

## VII. CONCLUSION

92. Law Enforcement commends the efforts of all commenters to this NPRM and respectfully requests that the Commission consider carefully our positions herein submitted on many of the comments made by others. We also respectfully request that the Commission adopt the additional measures proposed in our original comments to the NPRM.

Respectfully submitted,

FEDERAL BUREAU OF INVESTIGATION

Carolyn G. Morris
Assistant Director
Information Resources Division
14800 Conference Center Drive Suite 300
Chantilly, Virginia 20151

# APPENDIX A

# APPENDIX B