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

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

COMMENTS REGARDING FURTHER NOTICE OF PROPOSED RULEMAKING

Louis J. Freeh, Director
Federal Bureau of Investigation

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

Honorable Janet Reno
Attorney General of the United States

Donald Remy
Deputy Assistant Attorney General

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

TABLE OF CONTENTS

SUMMARY

The Commission's Further Notice of Proposed Rulemaking represents a significant step forward in the process of implementing the Communications Assistance for Law Enforcement Act. The Department of Justice and the Federal Bureau of Investigation thank the Commission for its exhaustive efforts to resolve the legal and technical issues concerning CALEA's assistance capability requirements that have been presented in this proceeding. With the Commission's further assistance in the remainder of this proceeding, we are confident that the goals that Congress set out to achieve when it enacted CALEA can be successfully realized.

The Commission has tentatively identified a number of deficiencies in the J-Standard, the industry "safe harbor" standard that is the subject of this proceeding. The Notice seeks comments on the Commission's tentative conclusions regarding the specific provisions of the J-Standard. The Notice also seeks comments on general issues relating to the assistance capability requirements of Section 103 of CALEA and the Commission's discharge of its responsibilities under Section 107(b).

With respect to the general issues identified in the Notice, we encourage the Commission to keep the following points in mind. First, once the Commission has determined that the J-Standard is deficient, the question under Section 107(b) is how to correct the deficiencies, not whether to correct them. If a particular deficiency may be corrected in more than one way, the Commission is free to select the particular means that best furthers the statutory criteria of Section 107(b). But Section 107(b) does not provide a mechanism for industry to be excused from meeting the assistance capability requirements of Section 103. If individual carriers find compliance with Section 103 infeasible, CALEA provides relief through the "reasonable achievability"mechanism of Section

109(b), which -- unlike Section 107(b) -- is carefully tailored to allow the Commission to take account of the circumstances of individual carriers.

Second, the Commission must give close attention to the role that cost considerations should -- and should not -- play in this proceeding. In reasonable achievability proceedings under Section 109(b), the cost of compliance for an individual carrier is relevant to whether the carrier should be required to modify its equipment, facilities, and services. But in proceedings to correct deficiencies in general industry "safe harbor" standards under Section 107(b), cost is relevant only as a basis for choosing among alternative means of meeting CALEA's assistance capability requirements -- not as a basis for excusing compliance with those requirements. To the extent that cost considerations are relevant under Section 107(b), the Commission must look to manufacturers and carriers for such information, and it should insist that any manufacturer and carrier cost estimates be adequately documented and substantiated before placing reliance on them.

Third, the Commission must resolve the general question of when call-identifying information is "reasonably available" to carriers. "Reasonable availability" is a technical concept that focuses on network design, not a financial concept involving carrier balance sheets. The J-Standard offers a proposed industry definition of "reasonably available," but the industry definition contains serious flaws that must be corrected if CALEA's provisions regarding call-identifying information are not to be undermined.

Fourth, the Commission needs to give careful consideration to how its decision in this proceeding will be implemented. The Commission has proposed to enlist the aid of an industry standard-setting body in drafting revisions to the J-Standard. We have reservations about the legal basis for such a disposition, but those reservations can be dealt with by providing that the

Commission will play a continued role following the completion of the standard-setting body's efforts. The Commission should also adopt concrete measures to ensure that proceedings before the standard-setting body move forward expeditiously and that the ultimate deadline for complying with CALEA's assistance capability requirements is not affected by any delays in those proceedings.

Turning from the general issues identified in the Notice to the specific issues surrounding the provisions of the J-Standard, we are in substantial agreement with many of the Commission's tentative conclusions. We agree with the deficiencies that the Commission has tentatively identified in the J-Standard, and we believe that those deficiencies can be (and must be) readily corrected in this proceeding. We encourage the Commission to reconsider its tentative conclusion that Section 103 of CALEA does not require the J-Standard to incorporate "surveillance integrity" features. We agree with the Commission's tentative conclusion that the J-Standard's location information provision is consistent with Section 103 of CALEA, and we stress that the location information provision entitles law enforcement to receive location information only when it has appropriate judicial authorization. Finally, with respect to packet mode communications, we do not believe that the specific packet mode provision of the J-Standard that has been challenged by CDT is deficient, and we urge the Commission to tread carefully in addressing more general packet mode issues that are beyond the immediate scope of this proceeding.

DISCUSSION

The Department of Justice and the FBI submit the following comments in response to the Further Notice of Proposed Rulemaking released by the Commission on November 2, 1998 ("Notice"). The Notice was issued by the Commission pursuant to Section 107 of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1006, and other applicable provisions of the Communications Act of 1934. See Notice ¶¶ 23, 148.

Section 103 of CALEA requires telecommunications carriers to meet specified "assistance capability" requirements relating to the performance of authorized electronic surveillance by federal, state, and local law enforcement agencies. 47 U.S.C. § 1002. Section 107(a) of CALEA permits industry associations or standard-setting organizations to adopt "technical requirements or standards * * * to meet the [assistance capability] requirements of section 103." Id. § 1006(a)(2). Section 107(b) of CALEA provides that, if a government agency or other person believes that industry technical standards adopted under Section 107(a) are deficient, it may petition the Commission to "establish, by rule, technical requirements or standards" that meet the requirements of Section 103. Id. § 1006(b).

In March 1998, the Department of Justice and the FBI ("the government") filed a petition under Section 107(b) ("Government Petition") for the Commission to issue technical standards in connection with J-STD-025 ("J-Standard"), an industry technical standard intended to implement Section 103 of CALEA for wireline, cellular, and broadband PCS telecommunications carriers. The Government Petition identified a number of specific respects in which the government believes the J-Standard to be deficient as a means of ensuring that carriers meet their assistance capability obligations under Section 103 of CALEA. The petition proposed specific additions and revisions to

the J-Standard that were intended to cure these deficiencies. The Commission also received petitions relating to the J-Standard from the Center for Democracy and Technology ("CDT") and the Telecommunications Industry Association ("TIA"). See Notice ¶¶ 16-20.

The Notice released on November 2 identifies various respects in which the Commission has tentatively concluded that the J-Standard is deficient. The Notice identifies other respects in which the Commission has tentatively concluded that the J-Standard is not deficient. The Notice requests comments on these tentative conclusions. The Notice also requests comments on a number of other matters relating to CALEA's assistance capability requirements and the Commission's performance of its responsibilities under Section 107(b) of CALEA.

These comments are submitted in response to the Commission's Notice. The comments are divided into three parts. Part I addresses general issues, both substantive and procedural, that are raised in the Notice. Part II addresses specific issues relating to the individual "punch list" items presented in the government's rulemaking petition (see Notice ¶¶ 67-128). Part III addresses the location information and packet-mode issues presented in CDT's rulemaking petition (see Notice ¶¶ 48-66).

The government has previously filed comments relating to CALEA's assistance capability requirements in response to the Commission's earlier public notice of April 20, 1998, in this proceeding. See DOJ/FBI Comments Regarding Standards for Assistance Capability Requirements, CC Docket No. 97-213 (filed May 20, 1998) ("Government May Comments"); DOJ/FBI Reply Comments Regarding Standards for Assistance Capability Requirements, CC Docket No. 97-213 (filed June 12, 1998) ("Government June Reply Comments"). In some instances, matters raised in the Notice have already been addressed in these prior comments. In the discussion that follows, we

refer the Commission to relevant portions of our earlier comments and incorporate them here by reference.

When the Commission considers our present comments and the corresponding comments by other parties, we urge the Commission to view them in the broad context of CALEA's underlying statutory objectives. As we have explained previously, CALEA was enacted to "insure that law enforcement can continue to conduct authorized wiretaps" in the face of rapid technological changes in the telecommunications industry. H. Rep. No. 103-827, 103d Cong., 2d Sess. 9 (1994) ("House Report"), reprinted in 1994 U.S. Code Cong. & Admin. News ("USCCAN") 3489. The outcome of this proceeding will determine whether that critical statutory goal will actually be accomplished. As Congress recognized in enacting CALEA, legally authorized electronic surveillance is a vital law enforcement tool, and law enforcement's ability to investigate, prosecute, and prevent crimes will be compromised if the deficiencies in the J-Standard are not corrected. Thus, the Commission's decisions in this proceeding will have a direct effect on the public interests in enforcing criminal laws and preserving public safety -- interests of the highest possible magnitude.

I. General Comments

A. The Nature of the Present Proceeding

We begin with three general comments concerning the nature of this proceeding. These comments concern the relationship between J-Standard itself and the "technical requirements or standards" that Section 107(b) requires the Commission to establish if the Commission finds the J-Standard to be deficient.

First, by virtue of Section 107(a)(2), CALEA's "safe harbor" provision, a carrier that is in compliance with the J-Standard is deemed to be in compliance with Section 103. See 47 U.S.C.

§ 1006(a)(2). The safe-harbor feature of Section 107(a)(2) makes the Commission's exercise of its authority under Section 107(b) critical to the intended operation of CALEA. If an industry standard such as the J-Standard is deficient -- that is, if it does not ensure that all covered carriers will in fact meet the assistance capability requirements imposed by Section 103 -- then Congress's goal of providing law enforcement with the technical capabilities needed to carry out legally authorized electronic surveillance will be directly compromised unless the standard is modified to eliminate the deficiencies. Congress has vested the Commission with the authority to establish technical requirements and standards under Section 107(b) precisely to ensure that law enforcement's ability to protect public safety and national security through lawful electronic surveillance is not frustrated in this fashion.

Second, to the extent that the Commission finally determines that the J-Standard is deficient, the sole remaining issue in this proceeding is how to correct the deficiencies, not whether to correct them. If a particular deficiency in the J-Standard may be cured by more than one means, the Commission is entitled to select from among the available means on the basis of the statutory criteria set forth in Section 107(b). But as discussed further below, the Commission may not excuse industry from correcting the deficiency altogether. See pp. 27-28 infra. If the Commission regards one proposed means of correcting a deficiency as unsuitable, it may turn to another means -- but in the end, it must designate some means of curing the deficiency and ensuring that the underlying assistance capability obligations of Section 103 will be met.

Third, carriers are not legally obligated to employ the particular means of satisfying Section 103 that are set forth in a "safe harbor" standard, regardless of whether the safe-harbor standard is set by industry or by the Commission. As we have explained previously, and as the Commission has

recognized, the safe-harbor mechanism created by Section 107(a)(2) of CALEA is a voluntary one; if a carrier can satisfy its underlying assistance capability obligations under Section 103 by other means, it is free to do so. See Notice ¶¶ 7, 32; Government May Comments at 14-15; Government June Reply Comments at 13-14. Because the specific means prescribed by a safe-harbor standard are voluntary, the Commission need not pursue a "lowest common denominator" approach to standard-setting that attempts to accommodate the potentially differing circumstances of each individual carrier and each platform. Since carriers are under no obligation to use the particular means set forth in the Commission's standards, the Commission can develop standards that "meet the assistance capability requirements of section 103" (47 U.S.C. § 1006(b)(1)) without having to attempt to tailor those standards to the peculiar circumstances of individual carriers and platforms. Moreover, as discussed below, CALEA contains other mechanisms for accommodating the particular circumstances of individual carriers.

B. Cost Considerations

At a number of points in the Notice, the Commission has requested comments regarding the costs associated with the implementation of CALEA's assistance capability requirements. See, e.g., Notice ¶ 30; see also Separate Statement of Commissioner Furchtgott-Roth. To the extent that we have comments concerning the costs of particular "punch list" items, we present those comments in Part II below. However, we have several comments regarding cost considerations at a more general level.

1. Statutory Framework

Congress was aware that implementing CALEA's assistance capability requirements would require telecommunications carriers to incur potentially substantial costs. Congress therefore

incorporated specific provisions in CALEA addressing the issue of implementation costs. It is critical at the outset to understand the role that cost considerations do -- and do not -- play in the statutory framework of CALEA.

a. For purposes of cost, CALEA draws a basic distinction between equipment, facilities, and services installed or deployed on or before January 1, 1995, and equipment, facilities, and services installed or deployed after that date. Generally speaking, the government must bear the reasonable costs directly associated with the modifications required for pre-1/1/95 equipment, facilities, and services to meet CALEA's assistance capability requirements. See 47 U.S.C. §§ 1007(c)(3), 1008(a). A carrier is not obligated to meet the assistance capability requirements with respect to pre-1/1/95 equipment, facilities, and services unless the Attorney General has agreed to pay those costs or the equipment, facility, or service has been "replaced or significantly upgraded or otherwise undergoes major modification." Id. §§ 1007(c)(3)(A)-(B), 1008(d). Thus, costs associated with modifying pre-1/1/95 equipment, facilities, and services should not be of concern here.

In contrast, the costs associated with modifying post-1/1/95 equipment, facilities, and services generally must be borne by telecommunications carriers themselves. Congress understood, however, that in some instances, costs and other factors might make it infeasible for individual carriers to meet CALEA's assistance capability requirements even with respect to post-1/1/95 equipment, facilities, and services. To deal with that problem, Congress enacted Section 109(b) of CALEA, 47 U.S.C. § 1008(b).

Under Section 109(b), a carrier or other interested person may petition the Commission to determine whether compliance with CALEA's assistance capability requirements is "reasonably achievable" with respect to any "equipment, facility, or service installed or deployed after January 1,

1995. " Id. § 1008(b)(1). If the Commission determines in such a proceeding that compliance is not "reasonably achievable" for a particular carrier, the Attorney General may agree, subject to the availability of appropriations, to pay the carrier for "the additional reasonable costs of making compliance with such assistance capability requirements reasonably achievable." Id. § 1008(b)(2)(A). If the Attorney General does not agree to pay such costs, the carrier is "deemed to be in compliance" with Section 103 with respect to the equipment, facilities, or services in question, and thus is excused from having to bear those costs until the equipment, facilities, or services undergo a major modification. Id. § 1008(b)(2)(B).

Congress explicitly made cost considerations part of the calculus for determining whether compliance is "reasonably achievable" under Section 109(b). In determining whether compliance is "reasonably achievable" for a particular carrier, the Commission must determine "whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier's systems * * * ." 47 U.S.C. § 1008(b)(1). The Commission also must consider "[t]he effect on the nature and cost of the equipment, facility, or service at issue" (id. § 1008(b)(1)(E)), and "[t]he financial resources of the telecommunications carrier" (id. § 1008(b)(1)(H)). These cost considerations are weighed along with a number of other factors, including "[t]he effect on public safety and national security" (id. § 1008(b)(1)(A)) and "[t]he need to achieve the capability assistance requirements of [Section 103] by cost-effective methods" (id. § 1008(b)(1)(D)), in determining whether compliance is "reasonably achievable."

b. The present proceeding is taking place not under Section 109(b), but rather under Section 107(b). See Notice ¶ 144 (dismissing, without prejudice, the portion of CDT's rulemaking petition seeking relief under Section 109(b)). Section 107(b) likewise takes account of cost considerations.

It does so, however, in a different and substantially more limited fashion. The difference in treatment of cost under Section 107(b) and Section 109(b) follows directly from the different objectives of those provisions.

Section 109(b) is designed to identify circumstances in which, absent government cost reimbursement, individual carriers may be excused from compliance with CALEA's assistance capability requirements. Section 107(b), in contrast, is designed to bring carriers into compliance with CALEA's assistance capability requirements, by correcting deficiencies in industry standards that would otherwise provide a "safe harbor" under Section 107(a)(2) of CALEA. The object of proceedings under Section 107(b) is not to decide whether carriers must comply with the assistance capability requirements of Section 103, but how they are to comply.

To that end, Section 107(b) identifies a number of factors to be taken into account by the Commission in promulgating "safe harbor" standards that meet the assistance capability requirements of Section 103. See pp. 27-30 infra. Among other things, Section 107(b) directs the Commission to establish standards that "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)) and that "minimize the cost of such compliance on residential ratepayers" (id. § 1006(b)(3)).

In keeping with the overall purpose of Section 107(b), these provisions direct the Commission to take account of cost in determining how the assistance capability requirements are to be met, not whether they are to be met: the Commission is to look for "cost-effective means" of "meet[ing] the assistance capability requirements" and to "minimize the cost of * * * compliance" with those requirements (emphasis added). Thus, if there is more than one means of complying with CALEA's assistance capability requirements, the Commission may take account of relative costs (along with

the other factors in Section 107(b)) in choosing among the alternatives. What the Commission may not do -- and what the cost provisions of Section 107(b) do not authorize the Commission to do -- is to adopt technical standards that stop short of "meet[ing] the assistance capability requirements of section 103" because of concerns about cost. Section 109(b), with its precisely articulated factors for determining whether compliance is "reasonably achievable," is the only avenue provided by Congress for the Commission to excuse carriers from compliance. Congress has made a global determination that the benefits of requiring carriers to meet Section 103's assistance capability requirements exceed the costs; Section 107(b) is not intended to invite an administrative reconsideration of that legislative cost-benefit determination.

It should be noted in this regard that Section 109(b), in contrast to Section 107(b), directs the Commission to take account of "[t]he effect on public safety and national security." See 47 U.S.C. 1008(b)(1)(A). If Section 107(b) were meant, like Section 109(b), to be a vehicle for excusing carriers from compliance with their assistance capability obligations, Congress would have included the same directive in Section 107(b), in order to ensure that the private costs of compliance are balanced against the public costs of non-compliance. Because Section 107(b) is <u>not</u> designed to excuse carriers from compliance with CALEA's assistance capability requirements, there was no need for Congress to direct the Commission to consider the costs to "public safety and national security" from non-compliance.

As noted above, the technical standards established by the Commission under Section 107(b) are simply a "safe harbor" for carriers that are seeking to comply with Section 103. Thus, if a particular carrier is able to comply with Section 103 by alternative means that are less costly than those entailed in the safe-harbor standard, the Commission's actions in this proceeding will not stand

in its way. And if "the total cost of compliance" for an individual carrier "is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features" (House Report at 28, reprinted in 1994 USCCAN at 3508), the carrier may seek relief under Section 109(b).

c. In earlier stages of this proceeding, industry commenters have asserted that cost considerations are incorporated in the capability assistance requirements of Section 103 itself. Specifically, they have argued that Section 103(a)(2), which requires carriers to provide access to "reasonably available" call-identifying information, excuses carriers from providing call-identifying information if doing so would involve undue expense. In response to these suggestions, the Commission has asked commenters to address "how cost should be considered in our determination of reasonable availability." Notice ¶ 26. We address the meaning of Section 103(a)(2)'s "reasonably available" language further below, but we comment here on the relationship between "reasonable availability" and cost.[1]

The language and subject matter of Section 103(a)(2) indicate that "reasonable availability" is a technical concept, not a financial one. The availability of call-identifying information to a carrier depends on the carrier's network architecture, the network elements where the information resides, the accessibility of the information within those network elements, and other technical considerations. It is these technical considerations, not cost considerations, that should determine whether particular call-identifying information is "reasonably available."

---

[1] As the Commission has recognized, the "reasonably available" proviso applies only to call-identifying information. There is no corresponding limitation on the obligation to deliver call content under Section 103(a)(1) of CALEA.

Because Congress has explicitly incorporated cost considerations into the determination of "reasonable achievability" under Section 109(b), there is no need to also read cost considerations into "reasonable availability" under Section 103(a)(2). Section 109(b) reflects a careful appraisal by Congress of the criteria, including but not limited to cost, that should be taken into account in deciding whether to excuse a particular carrier from bearing the costs required to modify its equipment, facilities, and services to implement CALEA's assistance capability requirements. Reading cost into "reasonable availability" would be at best redundant and at worst a form of double-counting.

Moreover, reading cost considerations into "reasonable availability" under Section 103(a)(2) would create a potential obstacle to law enforcement's ability to perform legally authorized electronic surveillance that is not created by Congress's incorporation of cost factors into "reasonable achievability" under Section 109(b). If delivery of particular call-identifying information is found not to be "reasonably achievable" under Section 109(b), the Attorney General has discretionary authority under Section 109(b)(2)(A) to obtain it at public expense by reimbursing the carrier "for the additional reasonable costs of making compliance * * * reasonably achievable," thereby obligating the carrier to provide access to the information (pursuant to appropriate legal authorization). 47 U.S.C. § 1008(b)(2)(A); see also id. § 1008(e)(2)(A)(i). But if particular call-identifying information is deemed to be not "reasonably available" under Section 103(a)(2), the information is entirely outside the scope of the carrier's assistance capability obligations under Section 103. Thus, if particular call-identifying information is deemed not to be "reasonably available" under Section 103(a)(2) because of cost, the carrier would not be obligated to provide it under CALEA even if law

enforcement would be willing to assume the cost of obtaining access to it.[2] The Commission should not -- and, in light of Section 109(b), need not -- read "reasonably available" to bring about such a result, a result that would be plainly contrary to what Congress was attempting to accomplish through CALEA.

2. Cost Information

a. To the limited extent indicated above (see pp. 11-12 supra), cost considerations have a role to play under Section 107(b) of CALEA. Unfortunately, the government is severely limited in its ability to provide the kind of detailed cost information that the Commission is seeking.

The principal potential source for CALEA cost information is the telecommunications manufacturers who will provide the equipment upgrades needed to implement CALEA. Section 106(b) of CALEA (47 U.S.C. § 1005(b)) requires "manufacturer[s] of telecommunications transmission or switching equipment" to provide the carriers using their equipment with "such features or modifications as are necessary to permit such carriers to comply" with the assistance capability requirements of Section 103 and the capacity requirements established under Section 104. Section 106(b) further provides that manufacturers must provide the required modifications "on a reasonably timely basis and at a reasonable charge." Ibid. (emphasis added).

---

[2] It is unclear whether a carrier would be obligated by any other federal law to modify its network to provide access to call-identifying information in this circumstance. Title III provides that carriers may be ordered by a court to "furnish * * * all information, facilities, and technical assistance necessary to accomplish [an] interception * * * ." 18 U.S.C. § 2518(4); see United States v. New York Telephone Co., 434 U.S. 159, 177 (1977). However, "the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated." House Report at 13, reprinted in 1994 USCCAN at 3493. One of the reasons that Congress enacted the assistance capability requirements of Section 103 was to eliminate this uncertainty.

In connection with Section 106(b), the FBI has engaged in extensive consultations with manufacturers regarding potential CALEA solutions. However, these consultations have not involved any significant sharing of cost information by the manufacturers with the government. For obvious reasons, manufacturers regard cost data as highly confidential proprietary information, and with a single exception, they have declined to provide cost information to the FBI even on a confidential basis.

A number of manufacturers have given the FBI proposed prices, as distinct from underlying manufacturer costs, for "CALEA solutions" covering the J-Standard and the additional capabilities sought by law enforcement. However, the price proposals that the FBI has received from manufacturers have been made pursuant to non-disclosure agreements (NDAs) that prohibit the government from disclosing propriety information, including price information, without the consent of the manufacturers. The NDAs permit disclosure in limited circumstances, but none of those circumstances appears to apply here. As a result, we regretfully cannot disclose to the Commission any price information obtained from manufacturers.

b. We anticipate that carriers and other commenters will provide the Commission with their own estimates of the costs associated with implementing CALEA's assistance capability requirements. We will respond to those estimates in our reply comments. As a general matter, however, the Commission should keep the following considerations in mind when reviewing cost estimates provided by carriers.

First, the Commission should require carriers to distinguish between the total cost of meeting Section 103's assistance capability requirements and the incremental cost of implementing the "punch list" capabilities at issue in this proceeding. Carriers who choose to rely on the safe harbor created

by the J-Standard must bear the costs associated with modifying post-1/1/95 equipment, facilities, and services to comply with the J-Standard, regardless of the outcome of this proceeding. The costs of implementing the J-Standard are, for present purposes, "fixed costs": industry has undertaken to incur these costs by adopting the J-Standard, and they will be incurred whether or not the Commission modifies the J-Standard to add capabilities from the government's punch list. As a result, those costs are irrelevant to the Commission's exercise of its authority under Section 107(b). To the extent that Section 107(b) provides for the Commission to take account of costs, the only relevant costs are the additional costs that may be incurred in implementing the capabilities added by the Commission.

Second, for purposes of this proceeding, carriers have an obvious incentive to maximize the claimed costs of implementing CALEA's assistance capability requirements and to minimize their professed ability to meet those requirements in a cost-effective manner. The Commission therefore must be vigilant in requiring carriers to substantiate and document their cost estimates. The Commission should ask carriers to spell out in detail the assumptions that underlie their cost estimates, such as their assumptions about anticipated price discounts. The Commission should also ask carriers to identify historical examples of software and hardware upgrades that the carriers regard as comparable in magnitude to those that may be required by the Commission here, and to identify precisely the costs attributable to such upgrades and the reasons for regarding them as comparable. Cost estimates that are not substantiated in this manner are entitled to little weight in the Commission's deliberations.

C. Reasonable Availability

As noted above, Section 103(a)(2) of CALEA obligates all telecommunications carriers to provide law enforcement agencies, pursuant to appropriate legal authority, with access to all

call-identifying information that is "reasonably available to the carrier." 47 U.S.C. § 1002(a)(2). CALEA does not provide an express definition of "reasonably available" (see id. § 1001 (CALEA definitions)), and the term is not used elsewhere in the Communications Act. The Notice therefore requests comments relating to the meaning and application of "reasonably available" in Section 103(a)(2). Notice ¶¶ 25-27. We have already commented above on the relationship between "reasonable availability" and cost; we now offer the following additional comments regarding other considerations.

1. As we have explained previously, the question whether a particular kind of call-identifying information is "reasonably available" is one that does not necessarily lend itself to across-the-board, industry-wide answers. See Government June Reply Comments at 37-38. As the Commission itself has noted, the availability of particular call-identifying information "is * * * likely to vary from carrier to carrier." Notice ¶ 26. Providing law enforcement agencies with access to particular call-identifying information may be technically straightforward with respect to one platform or network architecture and considerably more difficult and complex with respect to another. Thus, particular call-identifying information may prove to be "reasonably available" to one carrier and not "reasonably available" to another. Moreover, particular information that is not now "reasonably available" may become reasonably available as telecommunications technology and network architectures change over time.

Because of the inherently platform-specific and carrier-specific nature of reasonable availability questions, it would be fruitless for the Commission to try to determine whether a particular item, such as (for example) party status information (Notice ¶¶ 80-87), is "reasonably available" to telecommunications carriers as a class. And as a practical matter, it would not be

feasible for the Commission to determine the availability of particular call-identifying information separately with respect to each platform and carrier covered by the J-Standard.

Fortunately, there is no need for the Commission to make such determinations. Instead, the Commission can set forth a general definition of "reasonably available" and allow that definition to be applied by carriers and law enforcement agencies on a case-by-case basis in the future. That is the approach taken by the J-Standard itself, and there is no reason why the Commission should not follow suit in this regard.

Because the industry understood that reasonable availability may vary from platform to platform, the J-Standard does not undertake to determine whether any particular kind of call-identifying information is or is not "reasonably available." See J-STD-025, § 4.2.1 ("The specific elements of call-identifying information that are reasonably available * * * may vary between different technologies and may change as technology evolves"). Instead, the J-Standard offers a general definition of "reasonably available," one that is to be applied on a case-by-case basis to each item of call-identifying information. Ibid. The items of call-identifying information listed in the J-Standard (see J-STD-025, §§ 5.4.1-5.4.10) are therefore not limited to information that the industry has determined to be "reasonably available." Instead, the J-Standard lists all items of information that the industry deems to be call-identifying information, and relies on the industry's general definition of "reasonably available" to excuse carriers from having to deliver call-identifying information that is not reasonably available in a particular instance.

For reasons explained below, we have serious objections to the definition of "reasonably available" adopted by the J-Standard. However, we agree with industry that formulating a general definition of "reasonably available," and having the applicability of that definition to particular call-

identifying information dealt with on a case-by-case basis in the future, is preferable to attempting to determine ex ante whether a particular item of call-identifying information is "reasonably available" on an industry-wide basis. The Commission therefore should address the issue of "reasonable availability" in the same general fashion as the J-Standard itself does, by framing a working definition of "reasonably available" for the parties to apply in the future. Just as the J-Standard includes all items that industry has deemed to be call-identifying information, so too should the Commission include all additional items that the Commission determines to be call-identifying information. The Commission need not determine that a particular item is "reasonably available" before adding it to the J-Standard, any more than the industry itself did with respect to the items already in the J-Standard.

2. The J-Standard provides that call-identifying information will be deemed "reasonably available" to a carrier if, but only if, "the information is [1] present at an Intercept Access Point (IAP) [2] for call processing purposes." J-STD-025, § 4.2.1 (brackets added). The J-Standard's definition of "reasonably available" further provides that network protocols "do not need to be modified solely for the purpose of passing call-identifying information." Ibid.

The government strongly disagrees with this definition of "reasonably available." If the definition is left unchanged, it has the potential to interfere significantly with Congress's goal of closing the gap between law enforcement's legal authority to conduct electronic surveillance and industry's technical capability to assist that undertaking. The definition therefore should be modified in the Commission's final Report and Order.

The J-Standard's definition of "reasonably available" suffers from two basic problems. The first involves the requirement that call-identifying information be "present at an Intercept Access Point (IAP)" and the related provision that network protocols need not be modified to facilitate the

transmission of call-identifying information. The second concerns the categorical exclusion of call-identifying information that is not present at an IAP "for call processing purposes." We address these problems in turn.

a. As used in the J-Standard, "Intercept Access Point" or "IAP" refers to "a point within a telecommunications system where some of the communications or call-identifying information of an intercept subject's equipment, facilities, and services are accessed." J-STD-025, § 3. A carrier's network may (and ordinarily will) have more than one IAP. See id. § 4.2.2 ("The Access Function[] consist[s] of one or more Intercept Access Points"). However, the J-Standard imposes no requirements regarding where or how IAPs are to be situated within a network. Instead, it leaves the choice of IAPs entirely to the discretion of individual carriers and manufacturers. The J-Standard thus permits a carrier to situate IAPs without regard to the impact on the carrier's ability to "expeditiously isolat[e] and enabl[e] the government * * * to access" call-identifying information (47 U.S.C. § 1002(a)(2)).

By permitting a carrier to situate IAPs without having to take account of the resulting effect on law enforcement's ability to carry out lawful electronic surveillance, the J-Standard's definition of "reasonably available" threatens to defeat the central purpose of the statutory scheme. A carrier may select IAPs that seriously limit, or even prevent altogether, the collection of call-identifying information that law enforcement is legally authorized to acquire. Indeed, the J-Standard explicitly contemplates that IAPs may be placed within network elements that "provide reduced [surveillance] functionality." J-STD-025, Annex A, § A.1; see also id. § 4.2.2 ("The IAPs may vary between [carriers] and may not be available on all systems"). This flies in the face of Congress's goal of "insur[ing] that law enforcement can continue to conduct authorized wiretaps," and it frustrates

Congress's mandate that carriers "are required to design and build their switching and transmission systems to comply with the legislated requirements" of CALEA. House Report at 18, reprinted in 1994 USCCAN at 3498.

The problems created by this approach to the selection of IAPs are compounded by the J-Standard's unqualified position that network protocols do not have to be modified for the purpose of transmitting call-identifying information. In some instances, call-identifying information that is located elsewhere in a network could readily be made available through relatively minor modifications in network protocols.[3] We do not mean to suggest that carriers are obligated to modify network protocols in every instance where doing so would make it possible to provide law enforcement with otherwise inaccessible call-identifying information. But it is equally untenable to take the position, as the J-Standard does, that there is never any need to modify network protocols, even when the modification in question would be technically straightforward and would provide access to call-identifying information without imposing significant burdens on the network.

b. The J-Standard's requirement that call-identifying information be present at an IAP "for call processing purposes" is likewise problematic. It should be recalled that the statutory definition of "call-identifying information" (47 U.S.C. § 1001(2)) already serves to limit the scope of a carrier's obligations under Section 103(a)(2) to "dialing and signaling information that identifies the origin,

---

[3] Other recent Commission proceedings have resulted in the modification of telecommunication network protocols. For example, to comply with the Commission's Local Number Portability mandate, industry has had to make modifications to the SS7 network protocol. And the Commission's E911 initiative has required modifications of IS-41, a network protocol that allows interoperability between two wireless networks. More generally, it should be noted that protocols are significantly modified and expanded on a routine basis by standards organizations each year without concerns about "breaking" either the nodes that must generate the network protocol messages or the signaling network that must carry them.

direction, destination, or termination" of communications generated or received by a subscriber. To further require that such information be present at a particular point in the network "for call processing purposes," and to exclude categorically all call-identifying information that is not present at an IAP for such purposes, is to engraft a limitation on CALEA's assistance capability requirements that cannot be found in the statute itself or justified by reference to the statute's requirements. As long as call-identifying information is otherwise reasonably available, the fact that it is not present at an IAP for call processing purposes should be of no consequence.

It should be noted that requiring call-identifying information to be present at an IAP "for call processing purposes" would effectively excuse originating carriers from providing access to post-cut-through dialing, which is a particularly crucial source of call-identifying information for law enforcement. See Notice ¶¶ 123-128. The Commission has tentatively concluded -- in our view, correctly -- that "post-cut-through digits representing all telephone numbers needed to route a call * * * are call-identifying information." Id. ¶ 128; see pp. 66-70 infra. Neither the statutory definition of "call-identifying information" nor the statutory obligation to provide access to call-identifying information is tied to whether the originating carrier, as opposed to another carrier, uses the post-cut-through digits to complete the call. Yet the J-Standard's definition of "reasonably available" would effectively excuse originating carriers from providing access to post-cut-through digits -- not just in some cases, but in all cases. For reasons discussed in our earlier filings, it is not feasible for the government to look to long-distance providers or other "recipients" of post-cut-through dialing to find out the number of the party that the subject is calling. See Government June Reply Comments at 41-42 & n.24; see also pp. 68-69 infra. The J-Standard's "call processing purposes" proviso would

eliminate the only practical means of obtaining this critical information reliably and expeditiously. The Commission should not construe "reasonably available" to ratify that result.

c. To deal with these problems, the J-Standard's definition of "reasonably available" needs to be modified in the following respects. First, the requirement that call-identifying information be present "for call processing purposes" should be dropped. Second, the categorical exclusion of network protocol modifications should be removed. Third, the set of IAPs employed by a carrier must reflect a reasonable effort to provide access to the call-identifying information carried by the "equipment, facilities, or services that provide [the] customer or subscriber with the ability to originate, terminate, or direct communications" (47 U.S.C. § 1002(a)). We therefore suggest that the current language in the J-Standard be replaced with the following language:

> Call-identifying information is reasonably available if (1) it is present in an element in the carrier's network that is used to provide the subscriber with the ability to originate, terminate, or direct communications and (2) it can be accessed there, or can be delivered to an IAP located elsewhere, without unreasonably affecting the call processing capabilities of the network.

Construing "reasonably available" in this manner would protect a carrier's legitimate interests in the underlying integrity of its network operations and services while ensuring that law enforcement actually receives all call-identifying information that is reasonably available to the carrier.

3. In connection with the issue of "reasonable availability," the Commission has asked commenters to evaluate the types of information that have been "traditionally available under pen register and trap-and-trace authorizations * * * ." Notice ¶ 27. The Notice asks for comments on "whether the provision of such information to LEAs, in light of the statutory definitions of 'pen register' and 'trap and trace device,' and judicial interpretations of them, provide guidance or represent possible factors for determining 'reasonable availability.'" Ibid.

As we have explained in earlier filings, electronic surveillance in the analog POTS (Plain Old Telephone Service) environment traditionally has been carried out by intercepting communications on the analog "local loop" between the subscriber's telephone and the central office that handles the subscriber's outgoing and incoming calls. See Government Petition at 8-9; House Report at 13-14, reprinted in 1994 USCCAN at 3493-94. Generally speaking, electronic surveillance in this setting has been performed by establishing a physical connection to the wire carrying the subscriber's calls. The signals that are carried across the local loop between the subscriber's telephone and the central office are then transmitted to a remote surveillance site where law enforcement's monitoring activities take place.

When a law enforcement agency is conducting surveillance pursuant to pen register authority (see 18 U.S.C. §§ 3121-3127), the intercepted signals are typically routed through a device called a Dialed Number Recorder (DNR). The DNR prints a record of all dialing and signaling activity transmitted across the local loop. This includes not only the digits dialed by the subject, but also signaling information such as ringing, off-hook and on-hook signals, busy signals, and the like. In short, when acting pursuant to pen register authority, law enforcement traditionally has been able to access all dialing and signaling information transmitted to and from the subscriber.

Although the underlying definition of "pen register" in 18 U.S.C. § 3127(3) speaks in terms of signaling that identifies the "numbers" transmitted over the subscriber's line, CALEA itself makes clear that law enforcement's legal authority under the pen register statute encompasses all dialing and signaling information used in call processing. Section 207(b) of CALEA amended the pen register statute to provide that law enforcement agencies "authorized to install and use a pen register" must use "reasonably available" technology that "restricts the recording or decoding of electronic or other

impulses to the dialing and signaling information utilized in call processing." 18 U.S.C. § 3121(c) (emphasis added). The underscored language reflects Congress's own understanding of the information that it has authorized law enforcement to obtain pursuant to pen register authority.

In response to the Commission's question, we would not go so far as to suggest that all information that has traditionally been available to law enforcement pursuant to its pen register authority is ipso facto "reasonably available." CALEA contemplates that the locus of electronic surveillance will move from the local loop to switches or other network elements under the control of the carrier. Information that has traditionally been available on the local loop may not invariably be reasonably available to the carrier when surveillance is implemented at the switch. Conversely, some kinds of signaling information that have not traditionally been available over the local loop, such as "party hold" information (see pp. 44-47 infra), may now be readily available in a switch-based surveillance environment.

Nevertheless, the dialing and signaling information that traditionally has been available to law enforcement in the POTS environment does provide, in our view, a useful reference point in resolving disputes over reasonable availability. As explained in our earlier filings, Congress's underlying purpose in enacting CALEA was to "ensure that new technologies and services do not hinder [authorized] law enforcement access" to wire and electronic communications. House Report at 16, reprinted in 1994 USCCAN at 3496; see Government June Reply Comments at 10-11. Any reading of "reasonably available" that would significantly curtail access to the kinds of call-identifying information traditionally available to law enforcement is inconsistent with this legislative goal. And if a carrier contends that particular call-identifying information is not "reasonably available" to it, the

fact that such information has traditionally been available to law enforcement in pen register cases should be given considerable weight in evaluating that contention.

D. Section 107(b) Criteria

As noted above, Congress has identified specific criteria to be used by the Commission in establishing "technical requirements or standards" under Section 107(b). The Commission is directed to establish standards that: " (1) meet the assistance capability requirements of section 1002 of this title by cost-effective methods; (2) protect the privacy and security of communications not authorized to be intercepted; (3) minimize the cost of such compliance on residential ratepayers; [and] (4) serve the policy of the United States to encourage the provision of new technologies and services to the public * * * ." 47 U.S.C. § 1006(b)(1)-(4). In addition, the Commission must "provide a reasonable time and conditions for compliance with and the transition to any new standard," including "defining the obligations of telecommunications carriers * * * during any transition period." Id. § 1006(b)(5).

We have commented on these statutory criteria previously, and rather than repeat those comments, we incorporate them here by reference. See Government Petition at 59-63. We also address the statutory criteria in Part II below in connection with our comments about individual assistance capabilities. However, we have several additional comments about the statutory criteria at a more general level, and we present those comments here.

First, as indicated above in connection with our discussion of cost considerations (see pp.11-12 supra), the criteria set forth in Section 107(b) concern how the assistance capability requirements of Section 103 are to be met, not whether they are to be met. By its terms, Section 107(b) directs the Commission to establish technical requirements or standards that "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1) (emphasis added). To

the extent that the assistance capability requirements can be met in more than one way, the Commission may (indeed, must) take account of the criteria in Section 107(b) in choosing among the available alternatives. But any comments that purport to invoke the statutory criteria in order to excuse carriers from meeting their assistance capability obligations have no foundation in the statute.

Second, the Commission has asked commenters to address "the extent to which the capacity requirements of section 104 [47 U.S.C. § 1003] should affect our determinations under section 107(b)." Notice ¶ 31. The Commission notes that several commenters have suggested that "capability standards cannot be completed without first knowing the capacity that those capability standards must support." Ibid.

Those suggestions are fundamentally mistaken. Resolution of capacity issues might affect the implementation of assistance capability standards by manufacturers, but the existence of outstanding capacity issues is irrelevant to the establishment of standards by the industry and the Commission. The standards set forth in the J-Standard are generic standards that do not dictate the specific design modifications required for particular network platforms and do not depend on the capacity requirements that will be reflected in those modifications. Just as the absence of a final notice of capacity did not prevent the industry from selecting the assistance capabilities embodied in the J-Standard itself, neither should any outstanding capacity issues prevent the Commission from establishing additional assistance capabilities or delay the performance of that task.

Third, the Commission has indicated that it intends to establish a separate deadline for compliance with any "new" assistance capabilities added to the J-Standard in this proceeding, one that is later than the deadline of June 30, 2000, that the Commission has established for implementation of the "core" J-Standard requirements. Notice ¶ 133. Given the current timetable of this proceeding,

the government recognizes that compliance with new provisions that are added to the J-Standard may not be feasible by June 30, 2000. We believe, however, that compliance is feasible, and should be required, no later than 18 months after the new standards are published pursuant to this proceeding.

Therefore, if the Commission directs the industry to promulgate new standards within 180 days of the Report and Order, as the Commission has proposed to do, the Commission should provide that the deadline for compliance with the new standards will be no later than 24 months after the release of the Report and Order. Moreover, if carriers are able to implement particular capabilities in less than 24 months, they should be required to do so. To that end, the Commission should provide that the compliance deadline for each carrier will be the earlier of 24 months after release of the Report and Order or the date that the carrier has installed and deployed the modifications required to implement the capability in question. Finally, as discussed below, the Commission should also provide that the compliance deadline will not be extended in response to any delays in the industry standard-setting process.

E. Implementation

As explained above, the J-Standard must be revised to eliminate all deficiencies identified by the Commission in its Report and Order. The Notice states that the Commission intends to "permit[] Subcommittee TR45.2 of the TIA to develop the necessary [technical] specifications in accord with our determinations," rather than having the Commission itself draft specific changes to the J-Standard. Notice ¶ 132. The Notice states that TIA will be expected to "complete any such modifications * * * within 180 days of release of the Report and Order in this proceeding." Id. ¶ 133. We have the following comments on this proposal.

1. The government understands and appreciates the Commission's desire to have the assistance of an industry standard-setting body in developing the necessary modifications to the J-Standard. However, simply turning over the task to TR45.2, without providing for any further involvement by the Commission, might expose the Commission's action to a legal challenge -- a challenge that, if successful, might require the Commission to take on precisely the drafting tasks that it understandably would prefer not to perform. As we have explained previously, when the Commission determines that industry standards are deficient, Section 107(b) of CALEA provides for "the Commission to establish, by rule, technical requirements or standards" required to implement Section 103 of CALEA. 47 U.S.C. § 1006(b) (emphasis added). The underscored language suggests that the Commission is obligated to perform this task itself, rather than turning it over to the standard-setting body that developed the original, deficient standards. See Perot v. FEC, 97 F.3d 553, 559 (D.C. Cir. 1996) ("when Congress has specifically vested an agency with the authority to administer a statute, [the agency] may not shift that responsibility to a private actor"); Sierra Club v. Sigler, 695 F.2d 957, 962 n.3 (5th Cir. 1983) (agency "may not delegate its public duties to private parties"); Association of American Railroads v. Surface Transportation Board, 1998 WL 852532, at *13 (D.C. Cir. Dec. 11, 1998) (Sentelle, J., concurring).[4] Thus, the Commission's Report and Order could be challenged in the courts on the ground that the Commission has engaged in an unauthorized and impermissible delegation of regulatory authority.

---

[4] The Notice states that "CALEA contemplates that standards will be developed either 'by an industry association or standard-setting organization, or by the Commission.'" Notice ¶ 132 (quoting 47 U.S.C. § 1006(a)(2)). CALEA unquestionably contemplates that standards may be developed by industry, as well as the Commission, in the first instance. But when industry has already developed standards, and the Commission has determined those standards to be deficient, the language of Section 107(b) of CALEA indicates that the ultimate responsibility for modifying the standards to eliminate the deficiencies rests with the Commission itself.

To minimize this risk, the Report and Order should provide that the revised J-Standard will be presented to the Commission, immediately upon its adoption, for review and (if necessary) modification by the Commission itself. The Commission should allow a strictly limited period, such as 30 days after submission of the revised J-Standard, for submission of comments (if any) regarding the revisions. The Commission should then undertake to approve or disapprove the revisions within a correspondingly expedited time, such as within 60 days thereafter.

If the Commission approves the revisions, it should issue a further order establishing the revised J-Standard as a valid "safe harbor" standard. See CC Docket No. 97-213, CTIA Reply Comments at 4 (filed June 12, 1998) ("the Commission, if it deems necessary, can adopt the resulting industry consensus document by rule"). If the Commission finds the revisions deficient in any respect, it can correct the deficiencies and issue an order establishing the corrected standard as a safe harbor. By providing for the Commission to review the revised J-Standard and to issue an order establishing it (with any required corrections) as a safe harbor standard, the Commission's Report and Order would avoid being vulnerable to a legal challenge based on Section 107(b)'s requirement that the Commission "establish, by rule," the requisite technical standards.

2. The Notice proposes that TR45.2 be required to complete the necessary revisions to the J-Standard within 180 days. We agree with the Commission that 180 days is sufficient time to complete the necessary revisions. As we have noted in earlier filings, all of the capabilities in the government's punch list were originally included by industry itself in the initial working draft documents for the industry standard. See Government June Reply Comments at 15-16. Moreover, industry and law enforcement have been working together for the past year, under the aegis of TR45.2's ESS ad hoc group, to develop technical standards for implementing the punch list. As a

result, the industry standard-setting process that is contemplated by the Notice is already well underway.

Neverthless, relying on TR45.2 for assistance in the standard-setting process creates a risk of delay that could prejudice the timely implementation of CALEA's assistance capability requirements. Therefore, in addition to providing for Commission review and approval or disapproval of the revised J-Standard, the Report and Order should take additional steps to avoid unnecessary delay and to ensure that industry's standard-setting efforts lead to a satisfactory outcome.

First, the Commission should make clear that it will require strict compliance with the proposed 180-day time limit. The Report and Order should state that the 180-day deadline will not be extended. TR45.2 should be directed to notify the Commission immediately if and when it anticipates that it will not meet the deadline. The Report and Order should further provide that if TR45.2 fails to submit the required revisions to the Commission within 180 days, the Commission will accept proposed technical standards from law enforcement as the basis for the Commission's further proceedings.

Second, the Report and Order should reiterate that TR45.2 must "complete any such modifications" within 180 days. Notice ¶ 133 (emphasis added). Before the industry standard-setting process is complete, revisions to the J-Standard will be submitted for balloting. The Commission therefore should make clear that industry must finish the balloting process within the 180-day period. If TR45.2 were merely required to put the revisions out for balloting within 180 days, the balloting process itself could be stretched out almost indefinitely -- as it was during the development of the J-Standard itself, when balloting took nearly a full year.

Third, the Report and Order should make clear that the deadline set by the Commission for industry compliance with the additional capabilities included in the Report and Order (see p. 29 supra) will not be affected by any delays in the industry standard-setting process. This will provide a further incentive for the participants to complete that process in a timely manner.

Fourth, the Commission should designate members of its staff with appropriate technical expertise to participate as observers in the industry standard-setting process, as several industry commenters have previously suggested. The participation of Commission staff as observers will ensure that, when the revised J-Standard is submitted to the Commission, the staff is fully familiar with the course of intervening events and understands the dimensions of any remaining technical disputes.

Finally, the Report and Order should be as precise as possible in describing the capabilities that are to be added (and any other changes that are to be made) to the J-Standard. If the Report and Order are precise, the process of giving technical form to the Commission's decision should be relatively straightforward. But if the Report and Order are vague or ambiguous about the scope of the required changes, the result is likely to be disagreement among the parties and protracted delay. Insofar as the Commission ultimately agrees with the government regarding the current deficiencies in the J-Standard, we encourage the Commission to refer to Appendix 1 of the Government Petition for a precise description of the capabilities that should be added to correct those deficiencies.

F. Other General Issues

1. As the Commission has noted, the J-Standard applies to wireline, cellular, and broadband PCS carriers, the telecommunications carriers whose compliance with CALEA's assistance capability requirements is of most immediate concern to law enforcement. See Notice ¶ 134. The Commission

has asked for comments regarding "what role, if any, the Commission can or should play in assisting those telecommunications carriers not covered by J-STD-025 to set standards for, or to achieve compliance with, CALEA's requirements." Id. ¶ 141. The Commission seeks comments on how its determinations in this proceeding will affect the standards adopted by other industry segments and on whether the Commission "should consider the impact of the technical requirements we ultimately adopt in this proceeding on these other technologies and services." Ibid.

The Commission's determinations in this proceeding regarding CALEA's assistance capability requirements will have a direct and, in our view, beneficial effect on voluntary efforts by other industry segments to establish "safe harbor" standards under Section 107(a) of CALEA. Other industry groups have looked to the J-Standard in formulating their own CALEA safe harbor standards,[5] and they undoubtedly will pay equal attention to the Commission's modifications to the J-Standard. A determination by the Commission that Section 103 imposes a particular assistance capability should guide all telecommunications carriers. As a result, carriers who are not covered by the J-Standard can, and undoubtedly will, seek guidance from the Commission's Report and Order here in developing their own technical standards. We do not believe that the Commission needs to take any more direct action to foster the development of other industry standards; the standard-setting process will work best if the participants are allowed to go forward with the guidance provided by the Commission's decision in this proceeding.

2. The Notice incorporates an Initial Regulatory Flexibility Analysis (IFRA) required by the Regulatory Flexibility Act, 5 U.S.C. §§ 601 et seq. See Notice ¶¶ 148-164. Among other things, the

---

[5] For example, PCIA has published CALEA standards for one-way and two-way paging, and in the course of drafting those standards, PCIA looked to the J-Standard for guidance.

IFRA includes a description of projected reporting, record-keeping, and other compliance requirements. Id. ¶¶ 161-162; see 5 U.S.C. § 603(b)(4).

The Commission's discussion of reporting and record-keeping requirements notes that the Commission has previously proposed requiring telecommunications carriers to establish policies and procedures governing the conduct of officers and employees who are engaged in surveillance activity. Notice ¶ 161; see Notice of Proposed Rulemaking, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, ¶¶ 30-33 (released Oct. 10, 1997). The Commission tentatively concludes that "a substantial number of telecommunications carriers * * * already have in place practices for proper employee conduct and recordkeeping." Notice ¶ 161. The Commission further tentatively concludes that "the additional cost to most telecommunications carriers for conforming to the Commission regulations contained in this Further NPRM should be minimal." Ibid. The Commission has requested comments on these tentative conclusions.

The Commission is correct that a substantial number of telecommunications carriers already have in place practices and procedures for employee conduct and recordkeeping relating to authorized electronic surveillance. The extent to which existing practices and procedures are adequate to meet CALEA's systems security and integrity (SSI) requirements (see 47 U.S.C. §§ 229(b), 1004) is a separate issue that should be addressed in the context of the Commission's ongoing review of SSI issues. As for the additional reporting and recordkeeping costs that will be incurred by carriers as a result of the Commission's actions in this proceeding under Section 107(b), we agree with the Commission that those costs should be minimal.

II. Comments Regarding the Government "Punch List" Capabilities

The government's rulemaking petition identifies a number of specific respects in which the government believes the J-Standard to be deficient as a means of ensuring that carriers meet their assistance capability obligations under Section 103 of CALEA. See Government Petition at 24-58. The government has proposed additions and alterations to the J-Standard that are intended to eliminate these deficiencies. The government's proposed changes to the J-Standard have come to be referred to collectively as the "punch list."

The Commission has tentatively concluded that a number of the specific capabilities included in the punch list are required by Section 103 of CALEA. The Commission also has tentatively concluded that certain capabilities included in the punch list are not required by Section 103. The Commission has asked for comments on these tentative conclusions. The Commission also has asked for comments on a number of specific questions relating to the individual punch list items.

The following comments are submitted in response to these requests. The comments are presented in the order that the punch list capabilities are addressed in the Notice.

A. Conference Call Content

1. The J-Standard limits the ability of law enforcement to intercept the communications of parties to a conference call supported by the subscriber's equipment, facilities, or services. Under the J-Standard, law enforcement is provided with only those communications that are occurring over the legs of the call to which the subscriber's terminal equipment is actually connected (and hence audible to the intercept subject) at any point in time. See J-STD-025 § 4.5.1. As a result, if other parties to the conference call speak to each other when the subject places them on hold or drops off the call, the J-Standard does not provide access to those communications.

The Commission has tentatively concluded that Section 103(a)(1) of CALEA requires carriers to provide law enforcement with access to all content of subject-initiated conference calls supported by the subscriber's equipment, facilities, and services. Notice ¶¶ 77-78. We agree with that tentative conclusion. Section 103(a)(1) expressly provides that a carrier must provide access to "all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber." 47 U.S.C. § 1002(a)(1) (emphasis added). For reasons set forth in our earlier filings, this statutory obligation includes communications between parties on all legs of conference calls carried "to or from" the subscriber's "equipment, facilities, or services." See Government Petition at 32-33; Government June Reply Comments at 17-21. And as we have explained earlier, the failure to provide law enforcement with access to all legs of conference calls could result in the loss of important information that law enforcement agencies are entitled to obtain under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") and other applicable laws. See Government Petition at 31-32. We refer the Commission to the cited portions of our earlier filings for a more complete discussion of these points.

2. Section 103(a)(1) applies to communications carried by a carrier to or from the "equipment, facilities, or services of a subscriber." 47 U.S.C. § 1002(a)(1). The Notice requests comments on how the Commission should "define or interpret * * * the phrase 'equipment, facilities, or services' in the context of subscriber-initiated conference calls.'" Notice ¶ 77.

The government has addressed the scope of this language in its earlier filings in this proceeding. See Government June Reply Comments at 17-20. As we have explained, a subscriber's "services" encompasses all services provided to the subscriber by the carrier, including conference calling services and other multi-party calling services. A subscriber's "equipment" and "facilities"

encompass all of the elements of the carrier's network that support and are identifiable with the services that the carrier provides to the subscriber. Thus, if a carrier provides a subscriber with a conference calling service that has the capability to support communications between "held" legs of conference calls, the equipment and facilities used to provide that service are part of the subscriber's "equipment" and "facilities" for purposes of Section 103(a)(1), and communications between held legs of a conference call are carried "to or from the equipment, facilities, or services" of the subscriber. If the held legs remain "up" when the subject places them on hold or drops off the call, it is because the subscriber's services include that capability, and the network elements used to maintain the connection between the held legs remain part of the subscriber's equipment and facilities for the duration of the call.

3. The Commission has tentatively concluded that a carrier is not obligated to provide law enforcement with access to conversations between other parties to a conference call when "the call is either disconnected or rerouted" after the subject drops off "and the 'equipment, facilities, or services of a subscriber' are no longer used to maintain the conference call * * * ." Notice ¶ 78. If the call is actually "disconnected" when the subject drops off, the other legs of the call are broken down and no further communications between the other parties can take place, meaning that there is no further call content to deliver. If the call is not disconnected but is "rerouted" -- that is, if the carrier's network changes the path of the remaining call legs so that the communications no longer traverse the network element that originally handled the conference call -- the carrier's obligations depend on whether the call continues to use the "equipment, facilities, or services" of the subscriber. If "the 'equipment, facilities, or services of [the] subscriber' are no longer used to maintain the conference call" (Notice ¶ 78), then as the Commission has tentatively concluded, the carrier has no

obligation under Section 103(a)(1) to provide access to the subsequent communications. But if the subscriber's equipment, facilities, or services are still used to maintain the conference call when the subject drops off and the call is rerouted -- as will ordinarily be the case -- then the carrier's obligation under Section 103(a)(1) is unchanged. The use of the subscriber's equipment, facilities, or services remains the statutory touchstone.

4. Section 103(a)(1) provides that a carrier must give law enforcement access to "all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber." 47 U.S.C. § 1002(a)(1) (emphasis added); see also id. § 1002(d) (defining assistance obligations of mobile service provider that "no longer has access to the content of [a subscriber's] communications or call-identifying information within the service area in which interception has been occurring" because the call has been handed off to "to another service area or another service provider"). The Commission notes that, in some cases where a conference call is rerouted, the call may no longer be carried within the same "service area" that originally handled the call, but instead may be routed through a different service area. Notice ¶ 78. The Commission has tentatively concluded that Section 103(a)(1) does not obligate a carrier to provide access to the contents of the conference call in this circumstance. Ibid.

The government disagrees with this tentative conclusion. Section 103(a)(1)'s reference to communications "carried * * * within a service area" simply means that, at any one time, a carrier's assistance delivery obligations focus on a prescribed service area. It does not follow that a carrier's obligations under Section 103(a)(1) are limited to the same service area over the life of a call. When a carrier that has multiple service areas reroutes an ongoing communication from one service area to another one served by the same carrier (as often happens in the case of mobile wireless

communications), the carrier's assistance obligations under Section 103(a)(1) do not terminate; instead, they simply shift to the new service area. Thus, assuming that a carrier is otherwise obligated to provide access to held legs of a conference call under Section 103(a)(1), the rerouting of the conference call through another service area does not excuse the carrier from providing access to the call. The carrier either must continue to route the conference call through the original IAP or must ensure that law enforcement is able to access the conference call without loss of call content through another IAP.[6]

5. The Commission has tentatively concluded that a carrier's obligations under Section 103(a)(1) do not extend to "conversations between a participant of the conference call other than the subject and any person with whom the participant speaks on an alternative line * * * ." Notice ¶ 78. For example, "when A, the subject, is on a conference call with B and C, we tentatively conclude that [access to] C's conversation with D on call waiting is beyond CALEA's requirements." Ibid.

As a general matter, the government agrees with this tentative conclusion. When (to use the Commission's example) C uses his own call waiting service to speak to D rather than to A and B, the conversation between C and D ordinarily is not carried to or from A's "equipment, facilities, or services," and therefore is not within the scope of the carrier's obligations under Section 103(a)(1) (unless, of course, law enforcement has separate legal authority to intercept communications to and from C's facilities). But if C has the capability of joining D to the conference call, so that

---

[6] If the rerouting of the call involves not simply a different service area but another carrier, so that the original carrier is no longer involved in transmitting the call, then the original carrier has no further obligation under Section 103(a)(1) to provide access to the contents of the call. Cf. House Report at 22, reprinted in 1994 USCCAN at 3502 ("if an advanced intelligent network directs the communication to a different carrier, the subscriber's carrier only has the responsibility, under subsection (d) [of Section 103], to ensure that law enforcement can identify the new service provider handling the communication").

communications between C and D are transmitted to A during the course of the conference call, then those communications would be "carried to or from" A's equipment, facilities, or services and would be within the scope of the carrier's obligations under Section 103(a)(1) in that situation.

6. The Commission has asked for comments on the application of the statutory criteria of Section 107(b) to the development of an appropriate technical standard for delivery of conference call content. Notice ¶ 79. As an initial matter, we reiterate here a more general point made above: the criteria of Section 107(b) are directed at determining how identified deficiencies in industry standards are to be cured, not whether they are to be cured. Thus, if the Commission adheres to its tentative conclusion that carriers must provide law enforcement with the content of communications on all legs of conference calls in order to meet the assistance capability requirements of Section 103, then the J-Standard must be revised to include that capability. The criteria of Section 107(b) are relevant only to how that revision is carried out.

Section 107(b)(1) calls for technical standards that "meet the assistance capability requirements" of Section 103 "by cost-effective methods." 47 U.S.C. § 1006(b)(1). In calling on carriers to provide access to all legs of conference calls, the government is not seeking to dictate the technical details of implementation decisions. Cf. 47 U.S.C. § 1002(b)(1)(A) (CALEA does not authorize law enforcement agencies to "require any specific design of equipment, facilities, services, features, or system configurations to be adopted"). As a result, manufacturers and carriers are free to employ whatever software and/or hardware modifications will provide the required call content in the most cost-effective manner. We should add that if a carrier does not provide a conference calling service that permits other parties to speak with each other when the subject has placed them on hold or has dropped off the call, nothing in the government's proposal requires the carrier to incur

the cost of adding such a feature; the government seeks only to ensure that if a carrier chooses to provide its subscribers with this kind of conference calling service, law enforcement is provided with access (pursuant to legal authorization) to the communications taking place through that service.

Section 107(b)(2) calls on the Commission to "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). Requiring carriers to provide law enforcement with the content of "held" legs of conference calls is consistent with this goal because law enforcement, acting pursuant to an appropriate Title III order, is authorized to acquire this call content. As explained in our prior filings, Title III does not restrict law enforcement to intercepting communications in which the subscriber or intercept subject participates, but rather encompasses all communications taking place over the facilities under surveillance. See Government June Reply Comments at 22-30. To the extent that conversations on "held" legs of conference calls may happen to involve matters unrelated to criminal activity, law enforcement's statutory obligation under Title III to "minimize" the interception of such conversations (see 18 U.S.C. § 2518(5)) provides the requisite protection for privacy interests.

Section 107(b)(3) calls for the Commission to "minimize the cost of * * * compliance on residential ratepayers" when correcting deficiencies in industry technical standards. 47 U.S.C. § 1006(b)(3). In the absence of specific cost information from carriers or manufacturers, it is difficult to evaluate what effect the full implementation of Section 103(a)(1) with respect to conference call content will have on residential ratepayer costs, but the government does not anticipate that the impact will be significant. As noted above, the language of Section 107(b)(3) presupposes that the Commission must require "compliance" with Section 103; the only question is whether the cost of compliance on residential ratepayers can be minimized in some fashion. Leaving manufacturers and

carriers free to select the most cost-effective means of implementing this capability should tend to minimize any financial impact on residential ratepayers.

Section 107(b)(4) directs the Commission to establish technical standards that "serve the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C. § 1006(b)(4). There is no reason to expect that any technical standard regarding conference call content that may be adopted pursuant to this proceeding, whether framed by the Commission itself or by TR45.2 (see pp. 30-32 supra), will interfere with a carrier's ability to provide "new technologies and services to the public."

Finally, Section 107(b)(5) directs the Commission to "provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers * * * during any transition period." 47 U.S.C. § 1006(b)(5). As discussed above, the government believes that carriers that intend to meet their obligations under Section 103 by complying with the J-Standard should be required to implement the prescribed modifications to the J-Standard no later than 18 months after the modifications are required to have been adopted, meaning no later than 24 months after the Commission's Report and Order if the Commission remits the standard-setting task to TR45.2 under the proposed 180-day timetable (see pp. 29-30 supra). We do not contemplate that the Commission will subject carriers to any interim implementation obligations during the "transition period" preceding that deadline.

B. Party Join/Hold/Drop Information

1. The J-Standard does not require carriers to provide any message or signaling information indicating that a party has joined a multi-party call, been placed on hold, or dropped from the call. The Commission has tentatively concluded that the J-Standard is deficient in this regard and must be

modified to ensure that carriers provide law enforcement with "reasonably available" party join, party hold, and party drop information. Notice ¶¶ 85-86. The Commission has requested comments on this tentative conclusion.

The government agrees that Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with reasonably available party join/hold/drop information. For reasons presented in our previous filings and noted by the Commission (Notice ¶ 85), party join/hold/drop information fits squarely within CALEA's definition of "call-identifying information," which includes dialing and signaling information that identifies the "origin, direction, destination, or termination of each communication generated or received by a subscriber" (47 U.S.C. § 1001(2) (emphasis added)). See Government Petition at 44-45; Government June Reply Comments at 53. As a practical matter, party join, party hold, and party drop information enables law enforcement to follow the course of multi-party calls and to determine who is participating in such calls at any particular time. Without such information, law enforcement often would not know who joins or leaves a conference call, whether the subject alternated between legs of the call, or which parties may have heard or said particular communications during the course of the call. See Notice ¶ 85.

As the Commission notes (Notice ¶ 86), a carrier's obligation to provide party join/hold/drop information, like its obligation to provide other kinds of call-identifying information, applies to information that is "reasonably available" to the carrier. For reasons given above, the Commission need not and should not use this standard-setting proceeding to determine whether party join/hold/drop information is reasonably available to particular carriers or platforms. Instead, the Commission should frame an appropriate definition of "reasonably available" and leave the application of that definition to be worked out by individual carriers and law enforcement on a case-by-case basis.

See pp. 18-20 supra. This observation applies with equal force to the other items of call-identifying information discussed below.

The Commission has tentatively concluded that a carrier is obligated to provide party join/hold/drop information only when the carrier's own facilities, equipment, or services are involved in providing the service (and hence network signals associated with the change in party status are generated). Notice ¶ 86. The Commission has tentatively concluded that a carrier is not obligated to provide such information when changes in party status are handled by customer premises equipment because, "from the carrier's point of view, the call's status is unchanged" in such cases. Ibid. The government agrees with this tentative conclusion. If a carrier's network is not "aware" of a party join, hold, or drop because the change is handled by customer premises equipment, law enforcement does not expect the carrier to provide notice of the change. See Government June Reply Comments at 52 n.30.

2. TIA has suggested previously that party join/hold/drop information is already substantially available to law enforcement under the J-Standard. See Notice ¶ 86 (discussing TIA's submission). Specifically, TIA has suggested that the information covered by the government's proposed Party Join message is provided by the J-Standard's Change message (acting in conjunction with the Origination and TerminationAttempt messages), and that the information sought by the proposed Party Drop message is provided by the J-Standard's Release message. See CC Docket No. 97-213, TIA Comments at 52-53 (filed May 20, 1998). The Commission has invited comments on this suggestion. Notice ¶ 86.

The government has addressed TIA's suggestion in earlier filings. See Government June Reply Comments at 51-52. As we have explained before, an examination of the J-Standard does not

support the suggestion. The J-Standard's Change message is not a substitute for party join information because the Change message is triggered by changes in call identities, rather than by changes in party identities, and therefore will not identify party joins if a manufacturer uses a single call identity to cover multiple legs of a call. Id. at 48-49, 51-52. As for party drops, the J-Standard's Release message is not a proxy for a party drop message because the J-Standard does not require a carrier to send the Release message when a single call leg or call appearance is released; instead, it makes the delivery of the Release message for such events discretionary. Government June Reply Comments at 52. Finally, we note that TIA has not suggested that the J-Standard provides any message that notifies law enforcement of party holds. In short, the J-Standard's existing messages cannot reasonably be claimed to substitute for the party join, hold, and drop information that Section 103(a)(2) of CALEA requires carriers to provide.

3. Requiring carriers to provide party join/hold/drop information is consistent with the statutory criteria of Section 107(b). For the reasons given above and in our earlier filings, party join/hold/drop information must be provided in order for carriers to "meet the assistance capability requirements" of Section 103, and carriers and manufacturers will be free to implement this capability by whatever specific technical means prove to be most "cost-effective" for them. 47 U.S.C. § 1006(b)(1). If individual carriers believe that providing party join/hold/drop information will be prohibitively expensive for them, they may seek relief under Section 109(b) of CALEA, which provides the Commission with a suitably tailored mechanism for making carrier-specific assessments of cost and other relevant criteria regarding "reasonable achievability" (see pp. 9-10 supra).

Requiring carriers to provide party join/hold/drop information will not impair "the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). To the

contrary, this information may actually serve to enhance privacy. To the extent that receipt of party join/hold/drop information permits law enforcement to identify promptly the participants to a multi-party call, it may permit law enforcement to minimize surveillance of non-criminal conversations more quickly.

Requiring carriers to provide party join/hold/drop information should not have a material impact on residential ratepayers (47 U.S.C. § 1006(b)(3)) and should not affect "the provision of new technologies and services to the public" (id. § 1006(b)(4)). Finally, with respect to an implementation timetable (id. § 1006(b)(5)), we contemplate that this capability, like the other capabilities identified in the government's rulemaking petition, would be required to be implemented within 24 months of the Commission's Report and Order if the Commission provides for TR45.2 to adopt revised standards within 180 days (see pp. 29-30 supra).

C. Subject-Initiated Dialing and Signaling Information

1. During the course of a call that is subject to authorized electronic surveillance, an intercept subject may invoke services like three-way calling and call transfer by pressing feature keys or the flash hook. The J-Standard does not require carriers to provide a call data message when the subject inputs dialing or signaling information within a call in this fashion.

The Commission has tentatively concluded that subject-initiated dialing and signaling information constitutes "call-identifying information" for purposes of CALEA (Notice ¶ 91) and therefore must be provided to law enforcement when it is "reasonably available" to the carrier (Notice ¶ 94). The government agrees with this tentative conclusion. For reasons explained in our earlier filings, when a subject presses a feature key or the flash hook to invoke features like three-way calling, call waiting, and call forwarding, the resulting dialing and signaling information identifies

(depending on the particular feature involved) the "origin," "direction," "destination," and/or "termination" of each communication. See Government June Reply Comments at 46-48. Moreover, whenever the subject uses feature keys or the flash hook to control a call, he is engaged in the "direction" of his communications. Cf. 47 U.S.C. § 1002(a) (assistance capability requirements apply to all equipment, facilities, and services that allow subscriber to "originate, terminate, or direct communications") (emphasis added). The remote operation of these features (Notice ¶ 91) should not lead to a different result. However, we agree with the Commission that, insofar as these features are controlled by customer premises equipment and no network signal is generated, the dialing and signaling information will not be available to the carrier and therefore need not be provided by the carrier under Section 103(a)(2). See Government June Reply Comments at 49.

2. The Commission has noted that some commenters have asserted that the subscriber-initiated dialing and signaling information sought by the government is already provided in substantial part by the J-Standard. Notice ¶ 94. For example, TIA has asserted that, with respect to signaling activity that is transmitted from the subject to the network and detected by the switch, the J-Standard already provides law enforcement with "all potentially relevant call-identifying information." CC Docket No. 97-213, TIA Comments at 48-49.

These assertions are mistaken, for much the same reasons that TIA's similar assertions regarding party join and party drop information are mistaken (see pp. 46-47 supra). TIA's argument is based primarily on the operation of the J-Standard's Change message. But as discussed in our prior filings (see Government June Reply Comments at 48-49), and as reviewed above, the Change message is tied to changes in call identity rather than party identity, and therefore will not necessarily disclose the use of feature keys and hook flashes that change the parties to a particular conversation

within a multi-party call. For example, depending on how a particular manufacturer chooses to implement the J-Standard, a subject could press the flash hook to move back and forth repeatedly between two legs of a call without ever generating a Change message.

3. In the course of discussing subject-initiated dialing and signaling information, the Notice discusses the relationship between subject signaling and voice mail. Notice ¶ 93. The Notice states that "signaling data indicating that the subject is accessing his/her voice mail is properly classified as 'call-identifying information.'" Ibid. However, the Notice states that "[t]he contents of the voice mail * * * fall outside the scope of CALEA" because CALEA "does not apply to information services." Ibid. The first statement is correct, but the second statement requires qualification.

As the Commission is aware, Section 103(a)'s assistance capability requirements apply to "telecommunications carriers," and CALEA defines "telecommunications carrier" to exclude "persons or entities insofar as they are engaged in providing information services." 47 U.S.C. §§ 1001(8)(C)(i), 1002(a). CALEA's definition of "information services" includes voice mail services. See id. § 1001(6). Accordingly, "[t]he storage of a message in a voice mail or E-mail 'box' is not covered * * * ." House Report at 23, reprinted in 1994 USCCAN at 3503 (emphasis added). However, when a carrier redirects an incoming communication to a voice mail box, "[t]he redirection of the voice mail message to the 'box' * * * [is] covered," meaning that the carrier would have to provide the message to law enforcement in the course of the redirection (assuming, as always, that law enforcement has the necessary legal authorization to intercept the communication). Ibid.; see also id. at 20, reprinted in 1994 USCCAN at 3500 ("the call redirection portion of a voice mail service [is] covered"). Conversely, when the subscriber signals the carrier to deliver a voice mail message to the subscriber's terminal, and the carrier transmits the message to the subscriber using the

subscriber's equipment, facilities, and services, that transmission is likewise covered by Section 103(a). Thus, it is too broad to say that "the contents of the voice mail" fall outside the scope of CALEA: stored voice mail is not covered by CALEA, but the transmission of communications to and from voice mail boxes over a subscriber's "equipment, facilities, and services" is covered.

4. Requiring carriers to provide law enforcement with reasonably available subject-initiated dialing and signaling information is consistent with the criteria of Section 107(b) of CALEA. This capability must be added to the J-Standard in order to "meet the assistance capability requirements" of Section 103, and carriers and manufacturers are free to choose the most "cost-effective methods" for providing this information. 47 U.S.C. § 1006(b)(1). With respect to protecting the privacy and security of communications not authorized to be intercepted, minimizing the cost of compliance on residential ratepayers, and encouraging the provision of new technologies and services to the public (id. § 1006(b)(2)-(4)), this capability stands in much the same position as the capability to provide party join, hold, and drop information (see pp. 47-48 supra). Finally, the 24-month implementation period proposed above should be adequate to permit development, installation, and deployment of any network modifications required to provide this capability.

D. In-Band and Out-of-Band Network Signaling

1. When a call attempt is made to or from a subscriber's equipment, facilities, or services, the carrier's network generates in-band or out-of-band signals that identify call progress. These signals may be presented to the subject as audible tones, visual indicators, or alphanumeric display information. For outgoing call attempts, these signals indicate (for example) whether the call attempt ended with a busy signal, ringing, or before the network could complete the call. For incoming call attempts, these signals indicate (for example) whether the subject's telephone received a call waiting

tone or was alerted to the redirection of a call to voice mail by a "stutter" tone or a message-waiting indicator. Collectively, these signals show how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended.

The J-Standard does not require carriers to provide law enforcement with notification of network-generated in-band and out-of-band signaling relating to call progress. The Commission has tentatively concluded that certain types of in-band and out-of-band network signaling, such as notification that a voice mail message has been received by a subject, constitute "call-identifying information" under CALEA. Notice ¶ 99. The Commission suggests that there may be other types of in-band and out-of-band signaling information that would constitute call content rather than call identifying information. Ibid. However, the Commission correctly notes that CALEA requires carriers to provide law enforcement both with call content and with call-identifying information, and the Commission therefore does not propose to decide what network signaling information falls into which category "[u]nless necessary to establish technical standards under CALEA's safe harbor." Ibid. The Commission requests comments regarding "what types of in-band and out-of-band signaling" must be provided to meet the assistance capability requirements of Section 103. Ibid.

The government's rulemaking petition identifies the specific kinds of network-generated notification signals that the government believes to required by Section 103. See Government Petition, Appendix 1 (§ 64.1708(d)). The basic object is to receive network signals that report the progress of outgoing and incoming call attempts. Specifically, the government seeks delivery of a notification message when the accessing system sends an audible in-band signal to the subscriber (such as a busy signal) or sends an out-of-band signal to the subscriber's terminal to activate, deactivate, or control the following indications of incoming calls or messages:

- Any alerting of incoming calls or messages;
- Audible indications of incoming calls or messages;
- Visual indications of incoming calls or messages, such as lights indicating call waiting; and
- Alphanumeric display information, such as messages sent to the terminal, calling number identification, or calling name identification.

In our view, all of this information constitutes "call-identifying information," because it identifies the "termination" (and, in some instances, the "direction" or "destination") of a communication. See Government Petition at 45-46; Government June Reply Comments at 55-56. As a result, the J-Standard's failure to require carriers to deliver such information renders it deficient.[7] We do not believe that any of this information constitutes call content, but even if it did, that would not make the J-Standard any less deficient, since (as the Commission points out) Section 103 obligates carriers to provide law enforcement with all call content as well as call-identifying information. Indeed, a carrier's obligation to deliver call content under Section 103(a)(1) is even broader than its obligation to deliver call-identifying information under Section 103(a)(2), since Section 103(a)(1) is not restricted to call content that is "reasonably available" to the carrier.

2. Requiring carriers to deliver network-generated in-band and out-of-band signaling information to law enforcement is consistent with the statutory criteria of Section 107(b) of CALEA. For reasons given above and in our earlier filings, delivery of network-generated signaling information is necessary to "meet the assistance capability requirements" of Section 103 and may be carried out by "cost-effective methods." 47 U.S.C. § 1006(b)(1). If network signaling information is delivered

---

[7] TIA has asserted previously that the J-Standard provides much of the information that the government is seeking through this punch list capability. We have responded to that assertion in our earlier filings. See Government June Reply Comments at 57-59.

to law enforcement over a call data channel, as the government has proposed, the "the privacy and security of communications not authorized to be intercepted" (id. § 1006(b)(2)) will be enhanced by preventing the risk of inadvertent intrusions on call content in pen register cases. See Government Petition at 48. We are aware of no reason why delivery of this information would materially affect residential ratepayers or would impede the provision of new technologies and services to the public. 47 U.S.C. § 1006(b)(3)-(4). Finally, it should be possible for carriers to implement this capability within the 24-month period discussed above (see pp. 29-30 supra).

E. Timing Requirements

Section 103(a)(2) of CALEA obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication," and "in a manner that allows it to be associated with the communication to which it pertains." 47 U.S.C. § 1002(a)(2)(A)-(B). Despite these requirements, the J-Standard does not contain any provision obligating carriers to deliver call-identifying information in a timely fashion, nor does it contain any provision requiring carriers to provide information about the time that call events actually occurred. As a result, as matters now stand, a carrier that delivers call-identifying information to law enforcement is in compliance with the J-Standard even if it delivers the information long after a communication is over, and even if law enforcement is unable to associate particular call-identifying information with particular communications because it lacks accurate information about when the call events occurred.

The Commission has tentatively concluded that the J-Standard must be modified to require carriers to deliver call-identifying information within a "reasonable amount of time" and to "stamp" call-identifying information with the time of the underlying call event. Notice ¶ 104. The government

agrees with this tentative conclusion. By its terms, Section 103(a)(2) requires carriers to isolate call-identifying information "expeditiously" and to provide such information to law enforcement "before, during, or immediately after the transmission of a wire or electronic communication." 47 U.S.C. § 1002(a)(2)(A). An industry standard that places no time limit whatsoever on the delivery of call-identifying information is patently inconsistent with this requirement. And as the Commission has pointed out (Notice ¶ 104), time stamping is necessary to allow law enforcement agencies to "associate[] [call-identifying information] with the communication to which it pertains" (47 U.S.C. § 1002(a)(2)(B)), particularly when a subject makes or receives a series of calls within a short time. Ibid.

The Notice suggests that time stamp information -- for example, the information that a subject hung up at 1:23:00.00 AM -- is itself "call-identifying information." See Notice ¶ 104. Although it is possible to read the statutory definition of call-identifying information to encompass information about the timing of a communication's "origin, direction, destination, or termination" (47 U.S.C. § 1001(2)), the government's time stamp proposal does not require such a reading. Whether or not a time stamp is itself call-identifying information, information about the timing of call events must be provided to ensure that call-identifying information can "be associated with the communication to which it pertains," as required by Section 103(a)(2)(B) of CALEA (47 U.S.C. § 1002(a)(2)(B)). The government therefore invites the Commission to predicate any time stamp requirement in its Report and Order on Section 103(a)(2)(B)'s "association" requirement, as well as (or in lieu of) classifying time stamp information as "call-identifying information."

2. To give practical content to the general timing requirements of Section 103(a)(2), the J-Standard must be modified to incorporate specific timing provisions. In its rulemaking petition, the

government has proposed that time stamps be accurate to within 100 milliseconds and that call event messages be delivered within 3 seconds (99 percent of the time). See Government Petition, Appendix 1 (§ 64.1708(e)). The Commission has requested comments on the technical feasibility of these proposals.

The government does not believe that there are any technical reasons why carriers cannot meet these (or comparable) timing requirements. The specific delivery time proposed in the government's rulemaking petition (within 3 seconds of the associated call event) was selected to make compliance feasible for a wide range of carriers utilizing a variety of platforms. The vast majority of carriers routinely deliver signaling information for call setup and takedown purposes in well under three seconds -- commonly in a matter of milliseconds. And by requiring only 99 percent reliability, the proposed delivery requirement accommodates the possibility of network congestion. The government is not asking carriers to process call-identifying information for CALEA purposes any more rapidly than carriers handle such information for their own call processing purposes.

As the Commission has pointed out (Notice ¶ 104), Section 103(a)(2) does not specify particular timing requirements. The government therefore does not contend that the specific timing provisions discussed above are the only possible ones that would satisfy the requirements of Section 103(a)(2). But the J-Standard must be modified to incorporate <u>some</u> timing requirements in order to give effect to the general timing provisions of Section 103(a)(2), just as the J-Standard designates specific call-identifying information messages and message parameters (see J-STD-025 §§ 5.4.1-5.4.10, 6.3.1-6.3.10, 6.4.1-6.4.11) to give effect to CALEA's general definition of "call-identifying information." It therefore will not do for carriers to argue that it is "arbitrary" to incorporate specific timing requirements into the J-Standard. As we have noted before, the whole

point of the standard-setting process is to give specific content to the general provisions of Section 103 by identifying precisely what steps are required for a carrier to meet its underlying assistance capability obligations.

3. The timing requirements proposed above are consistent with the statutory criteria of Section 107(b) of CALEA. For the reasons given above and in our earlier filings, timing requirements are necessary to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). The Commission is not being called upon to prescribe how those requirements are to be implemented with respect to any particular platform, leaving manufacturers and carriers free to implement the requirements by the most "cost-effective methods" available to them. Ibid. Requiring accurate time stamps and timely delivery of call-identifying information will not harm "the privacy and security of communications not authorized to be intercepted" (id. § 1006(b)(2)); to the contrary, they have the potential to protect privacy interests by assisting law enforcement in minimizing the interception of non-criminal conversations. These timing requirements should not materially affect the costs borne by residential ratepayers and should not interfere with "the provision of new technologies and services to the public." Id. § 1006(b)(3)-(4). And the implementation period proposed above (see pp. 29-30 supra) should be more than sufficient to allow manufacturers and carriers to make any modifications needed to implement the specific timing requirements prescribed by the Commission (id. § 1006(b)(5)), particularly since carriers are not being asked to process call-identifying information more rapidly for CALEA purposes than for their own call processing purposes.

F. Surveillance Integrity

1. The government's rulemaking petition includes three specific capabilities that address the need for "surveillance integrity" -- the need for the carrier to take concrete measures to ensure that its equipment, facilities, and services are capable of delivering authorized communications and call-identifying information to law enforcement (see 47 U.S.C. § 1002(a)(1)-(2)) and the corresponding need for the carrier to protect "the privacy and security of communications and call-identifying information not authorized to be intercepted" (see id. § 1002(a)(4)(A)). See Government Petition at 52-57 and Appendix 1 (§ 64.1708(f)-(h)). The Commission has tentatively concluded that the J-Standard does not have to be modified to incorporate any of the capabilities covered by these punch list items. See Notice ¶¶ 109, 114, 121. The government respectfully disagrees with this tentative conclusion. The government does not contend that the specific surveillance integrity mechanisms proposed in the government's rulemaking petition are mandated by Section 103 of CALEA. But Section 103 obligates carriers to take some affirmative steps to ensure surveillance integrity, and the J-Standard excuses carriers from taking any such steps. The Commission must correct that deficiency.

As the Commission is aware, the government believes that the J-Standard falls short in three specific respects in terms of surveillance integrity. First, the J-Standard does not obligate carriers to take any steps to ensure that authorized surveillance is "up and running" within the carrier's network and that the carrier is accessing the call content and call-identifying information of the correct subscriber. Through human or mechanical error, a carrier may fail to initiate an interception or may inadvertently access the communications of the wrong subscriber. When this happens, law enforcement will not obtain the communications to which it is entitled, and if the interception is directed at the wrong subscriber, the privacy of communications to which law enforcement is not

entitled will be inadvertently compromised. Yet the J-Standard places a carrier under no obligation to monitor an interception (or to provide law enforcement with the means to monitor it) to safeguard against such errors.

Second, the J-Standard does not require carriers to employ any mechanism to ensure that the channels used to deliver intercepted call content from the carrier to law enforcement are in working order. If the connection between the carrier and law enforcement is physically broken or otherwise interrupted, potentially critical and irreplaceable evidence of criminal activity may be lost. Law enforcement agents monitoring the subscriber's calls will hear nothing, but in the case of an analog connection, they will have no way of knowing whether silence means that the connection is broken or instead that the subscriber is simply not using his phone. The J-Standard nevertheless does not require carriers to take any steps to ensure that the connection is operational or to enable law enforcement to detect interruptions in a timely manner.

Third, the J-Standard has no mechanism for ensuring that law enforcement is notified of changes in a subscriber's features and services that could affect the provisioning of the interception. When a subscriber adds or changes features and services like call forwarding, call waiting, and conference calling, law enforcement may have to make corresponding changes in the number of delivery channels in order for the intercepted communications actually to be delivered to law enforcement. If law enforcement is unaware of the subscriber's actions, the interception will not be adequately provisioned and critical evidence may be lost. Yet the J-Standard does not require a carrier to take any steps to alert law enforcement of feature and service changes that could lead to this kind of loss.

In our view, the language of Section 103 requires affirmative measures by carriers in each of these three respects, and the J-Standard is deficient as a legal matter in not requiring carriers to employ any such measures. By its terms, Section 103 requires carriers to "ensure" that their communications equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement, "to the exclusion of any other communications," "all communications" to or from the "equipment, facilities, or services of a subscriber * * * ." 47 U.S.C. § 1002(a)(1). Section 103 further requires carriers to "ensure" that their equipment, facilities, and services are capable of expeditiously isolating and delivering to law enforcement all "reasonably available" call-identifying information. Id. § 1002(a)(2). At the same time, Section 103 requires carriers to "ensure" that their equipment, facilities, and services are capable of implementing authorized electronic surveillance "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted." Id. § 1002(a)(4).

Simply stated, a carrier that does not take any affirmative steps to monitor the integrity of authorized electronic surveillance is not "ensuring," as Section 103 requires, that its equipment, facilities, and services are capable of delivering "all communications" and all reasonably available call-identifying information that law enforcement is authorized to intercept while protecting the privacy and security of other communications and call-identifying information. As law enforcement agencies have learned through decades of experience, electronic surveillance cannot be relied on to provide all of the communications covered by a given surveillance order, while excluding other communications, unless ongoing steps are taken to provide assurance of the surveillance's integrity. Thus, surveillance integrity features of the sort that we have proposed do not constitute mere "quality control" measures (Notice ¶ 121); to the contrary, they are essential components of compliance with

Section 103. Nor does the absence of these features, or similarly effective alternative measures, merely prevent a carrier's compliance with § 103 from being "proven or verified on a continual basis" (Notice ¶¶ 109, 114); rather, these deficiencies mean that carriers implementing the J-Standard will not be complying with the mandates of Section 103 in the first instance.

By way of analogy, we invite the Commission to imagine a statute that requires air carriers to "ensure" that their planes are capable of delivering "all" passengers safely to their destinations. Cf. 49 U.S.C. § 44705(1) (air carrier operating certificate "shall contain terms necessary to ensure safety in air transportation"). Suppose that a particular carrier has a fleet of planes that have the technical capability to transport the carrier's passengers among the various cities served by the carrier. However, the planes do not have automated systems to detect particular in-flight mechanical or electrical problems, and the carrier does not require its pilots to check for such problems in any other fashion. The planes do not have automated systems to report deviations from the plotted route, and the carrier does not require its pilots to monitor the route once the course has been set. Finally, when unexpected changes in passenger load cause the carrier to switch from a small plane to a larger plane, the carrier does not provide notice to the destination airport, which needs to make a corresponding change in runways to handle the larger plane.

It is possible that this air carrier could operate for some period without an accident. But it hardly would follow that the carrier was meeting its statutory obligation to "ensure" that its planes were capable of delivering all of its passengers safely. It would be no answer for the carrier to say that its planes have the range and size needed to deliver its passengers to their destinations; a law requiring the carrier to "ensure" safe delivery of all passengers obviously requires something more. And while the carrier might be able to ensure safe delivery without using a particular safety

mechanism, such as (for example) automated notification of course deviations, it would remain incumbent on the carrier to employ some affirmative mechanisms to ensure that all of its passengers will actually reach their destinations safely.

In the government's view, a telecommunications carrier that does not take any affirmative steps to "ensure" the integrity of authorized electronic surveillance is in the same position as the air carrier in the foregoing example. If a telecommunications carrier is to ensure (as Section 103 requires) that it is capable of delivering all communications and call-identifying information to law enforcement, while simultaneously protecting the privacy and security of communications and call-identifying information not authorized to be intercepted, it must take affirmative steps to make certain that the surveillance is up and running on the right subscriber; that the delivery channels from the carrier to law enforcement are working; and that the law enforcement agency is aware of changes in subscriber services that may require corresponding changes in the provisioning of the surveillance. Without such steps, it is inevitable that carriers will fail to provide law enforcement with all of the communications and call-identifying information to which law enforcement is entitled under Section 103 and underlying electronic surveillance statutes, and it is equally inevitable that carriers will occasionally deliver communications and call-identifying information to which law enforcement is not entitled. Yet the J-Standard does not require carriers to take any -- we repeat, any -- affirmative steps in any of these regards. The complete omission of any affirmative surveillance integrity requirements in the J-Standard simply cannot be squared with Section 103.

The Commission should also recognize that the absence of surveillance integrity features in the J-Standard not only will lead to the loss of evidence that law enforcement is authorized to acquire, but also may limit the evidentiary value of the evidence that law enforcement does acquire. Criminal

defendants challenging the use of electronic surveillance seek to exploit every discernible weakness in electronic surveillance techniques, and it cannot have been Congress's intention in enacting CALEA to expand their opportunities to do so. Yet to the extent that a defendant can argue that law enforcement may not have intercepted all of his communications over the surveilled facilities during the intercept period, he can claim that law enforcement missed a crucial communication (or a portion of a communication) that would have exculpated him. It was to ensure that our use of electronic surveillance could not be undermined in this fashion that we have traditionally included surveillance integrity features in our intercepts, and it was to preserve and protect -- rather than to undermine -- our continued ability to use electronic surveillance in successfully prosecuting criminals that Congress enacted CALEA. The J-Standard's lack of any surveillance integrity features directly compromises this goal.

2. Whether the absence of surveillance integrity mechanisms renders the J-Standard deficient is, of course, a distinct question from how the deficiency should be corrected. If the Commission revises its tentative conclusion regarding the first question, it then must turn to the second one.

As the Commission is aware, the government has proposed that carriers ensure surveillance integrity through the automated delivery of surveillance integrity messages. Specifically, we have proposed that carriers deliver: (1) a surveillance status message, which would periodically verify that the intercept is accessing the correct equipment, service, or facility; (ii) a continuity tone, which would verify that the call content channels between the carrier and law enforcement are in working order; and (iii) a feature status message, which would report specific changes in a subscriber's calling features and services. See Government Petition, Appendix 1 (64.1708(f)-(h)).

In proposing the automated delivery of this information to law enforcement, we should not be understood to be claiming that the information qualifies as "call-identifying information." To the contrary, we agree with the Commission's tentative conclusion that the information in question is not call-identifying information. See, e.g., Notice ¶ 121 (feature status messages "do not constitute call-identifying information"). The government seeks this information not because the information is itself call-identifying information, but rather because delivery of the information -- or some other, equally effective affirmative measure -- is necessary for a carrier to meet its statutory obligation of "ensuring" that law enforcement receives the communications it is entitled to receive while the privacy and security of other communications is protected.

In our view, each of the proposed punch list items relating to surveillance integrity satisfies the statutory criteria of Section 107(b) of CALEA. To begin, for the reasons given above and in our earlier filings, affirmative steps to ensure surveillance integrity are necessary to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). The automated delivery of surveillance status messages, feature status messages, and continuity checks will realize that goal. Moreover, automated delivery of this information, rather than reliance on manual alternatives that require human intervention and monitoring by carrier personnel, represents a "cost-effective method" (ibid.) of accomplishing that goal. Our discussions with industry have indicated that the cost of implementing a continuity check (such as a C-tone) would be trivial, and we anticipate that periodic automated delivery of surveillance status messages and feature status messages likewise would not involve significant expense.

The automated delivery of surveillance integrity information is also consistent with the goal of "protect[ing] the privacy and security of communications not authorized to be intercepted."

47 U.S.C. § 1006(b)(2). Indeed, as indicated above, the automated delivery of a surveillance status message will affirmatively enhance legitimate privacy interests, by promptly alerting law enforcement if a carrier has inadvertently directed the surveillance toward the wrong subscriber.[8]

Because the cost of delivering automated surveillance integrity messages should be relatively minor, implementing these features should not have a material impact on residential ratepayers. 47 U.S.C. § 1006(b)(3). And we see no way in which the implementation of these features could reasonably be claimed to impede "the provision of new technologies and services to the public." Id. § 1006(b)(4). Finally, with respect to the need for transition provisions (id. § 1006(b)(5)), there is no reason why these features cannot be implemented within the general 24-month implementation period proposed above (see pp. 29-30 supra).

As we have previously stated, we are not arguing that the automated messages proposed in the government's rulemaking petition are the only possible means of ensuring surveillance integrity under Section 103. See Government Petition at 53-54; Government June Reply Comments at 67, 72. We reiterate that point here. Although we continue to believe that automated messages are an appropriate and effective means of implementing Section 103, we acknowledge that there may be other means by which a carrier might meet its assistance capability obligations in these regards. But the Commission should not excuse carriers from having to implement any affirmative measures to ensure surveillance integrity if the Commission concludes that the particular measures proposed by the government are not mandated by Section 103 or are otherwise inappropriate. If the J-Standard

---

[8] The Commission has asked whether a continuity tone "could * * * be detected by the subscriber whose facilities are under surveillance." Notice ¶ 115. It could not. The tone would be applied solely to the channel delivering call content to law enforcement.

is deficient in this respect, the deficiency must be corrected -- if not by the means proposed by the government, then by some other, equally effective means.

G. Post-Cut-Through Dialing

1. In long distance calls, credit card calls, and (in some instances) local calls, the dialing and signaling information necessary to route the call to the intended party may occur after the call has been initially "cut through" by the originating carrier. See Government Petition at 38-39 & n.16. In these cases, the destination of the call is revealed only by the numbers dialed after the cut-through. Under the J-Standard, however, originating carriers are not obligated to provide law enforcement with access to post-cut-through dialing. Instead, law enforcement receives only the digits dialed before cut-through, such as the numbers dialed to access a "1-800" long distance service -- numbers that ordinarily have no value to law enforcement whatsoever.

The Commission has tentatively concluded that "post-cut-through digits representing all telephone numbers needed to route a call * * * are call-identifying information." Notice ¶ 128. The government agrees with that tentative conclusion. CALEA defines "call-identifying information" to include "dialing or signaling information that identifies the * * * destination * * * of each communication generated * * * by a subscriber." 47 U.S.C. § 1001(2). Post-cut-through digits that are used for call routing fit squarely within this statutory definition. CALEA's definition of "call-identifying information" conspicuously does <u>not</u> add a further requirement that such information be used by the originating carrier, as distinct from some other carrier, for call routing purposes. As a result, the fact that originating carriers transmit post-cut-through digits over a call content channel, rather than a call data channel, does not mean that post-cut-through dialing "should be treated as content for purposes of CALEA" (Notice ¶ 128).

2. The Commission has asked for comments on how post-cut-through dialing can be extracted from the call content channel by the originating carrier for delivery to law enforcement. Notice ¶ 128. In the absence of an "out-of-switch" solution, such as implementation of SS7's option for returning the number of the answering party to the originating carrier (see Government June Reply Comments at 43 n.25), we anticipate that the originating carrier's hardware will have to be modified in order to detect and extract post-cut-through digits. To capture post-cut-through digits for delivery to law enforcement, an originating carrier may apply a tone decoder to the call or may detect the dialed digits outside the switch by a "loop-around" or other means.

In a related vein, the Commission has asked for comments on whether post-cut-through digits used for call routing can be "distinguished" from other post-cut-through dialing. Notice ¶ 128. We assume that the Commission is interested in the ability of originating carriers to "distinguish" between these two types of post-cut-through dialing by automated, real-time means, permitting carriers to deliver to law enforcement only those post-cut-through digits that are used for call routing. As far as the government is aware, that technical capability does not currently exist. Post-cut-through dialing for call routing purposes currently can be distinguished from post-cut-through dialing for other purposes only by "manual" means (that is, human review). If originating carriers did have the technical ability to perform this function on an automated, real-time basis, law enforcement would have no objection to (and indeed would welcome) such an approach.

3. The Commission has asked for comments on whether post-cut-through dialed digits are "reasonably available" (47 U.S.C. § 1002(a)(2)) to originating carriers. Notice ¶ 128. The Commission notes in this regard that industry and privacy groups have expressed concern about the potential costs involved in "design[ing], build[ing], and incorporat[ing] [post-cut-through dialed digit

extraction] into telephone network infrastructures." Ibid. The Commission seeks comments on whether "originating, intermediate, or terminating carriers can deliver such call-identifying information by cost-effective means." Ibid. The government offers the following comments regarding reasonable availability and cost.

First, for reasons set forth above, the government does not believe that cost considerations are germane to determinations of "reasonable availability" under Section 103(a)(2) of CALEA. See pp. 13-15 supra. And for the Commission to attempt to include or exclude particular capabilities categorically from the J-Standard on the basis of cost considerations would be particularly ill-advised. The Commission's standard-setting role under Section 107(b) is, and should be, aimed at the formulation of generally applicable standards for the entire class of carriers (wireline, cellular, and broadband PCS) that are subject to the J-Standard. The costs associated with post-cut-through dialed digit extraction, in contrast, can be expected to vary from platform to platform and carrier to carrier. For reasons given above, the appropriate mechanism for dealing with such individualized cost concerns is the "reasonable achievability" mechanism of Section 109(b) of CALEA, not the safe-harbor standard-setting mechanism of Section 107(b). See pp. 9-15 supra.

Second, it would not be cost-effective to look to intermediate carriers or terminating carriers, rather than originating carriers, to provide law enforcement with post-cut-through dialing. In order for an intermediate carrier to capture post-cut-through dialing covered by a pen register order and deliver the dialed digits to law enforcement "before, during, or immediately after the transmission" of the call (47 U.S.C. § 1002(a)(2)(A)), the intermediate carrier would have to monitor every incoming call that it receives in order to determine whether the call originated from the facilities of a subscriber covered by the order, and it would have to do so with respect to every outstanding pen

register order in the country. Requiring a terminating carrier to capture and deliver post-cut-through digits would be equally burdensome: because an intercept subject could call any subscriber served by the terminating carrier, the terminating carrier would have to monitor every switch in its network. In contrast, the originating carrier only has to monitor the particular switches that are used to provide service to the particular subscriber whose facilities are under surveillance. There are still further practical problems, identified in our earlier filings, with requiring law enforcement to obtain post-cut-through dialed digits from carriers other than the originating carriers. See Government June Reply Comments at 41-42 & n.24.

Third, as we have noted above, the industry's proposed definition of "reasonably available" in the J-Standard would effectively excuse all originating carriers from providing access to post-cut-through dialing, even if doing so would not impose significant costs or technical obstacles, because post-cut-through digits are not present at the originating carrier's IAPs "for call processing purposes" (J-STD-025 § 4.2.1). We have already explained why the Commission should excise the "call processing purposes" restriction from the J-Standard's definition of "reasonably available." See pp. 23-24 supra. We simply remind the Commission here that failure to do so would effectively nullify the Commission's tentative conclusion that post-cut-through dialing is call-identifying information, and would make it far easier for criminals to evade authorized pen register surveillance.

4. Requiring originating carriers to provide post-cut-through dialed digits is consistent with the statutory criteria of Section 107(b). For the reasons outlined above and in our earlier filings, law enforcement must be provided with post-cut-through dialing used for call routing if the J-Standard is to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). Requiring originating carriers rather than other carriers to provide this information is a "cost-effective

method" of implementing this capability, as discussed above. Ibid. Requiring originating carriers to extract dialed digits from post-cut-through call content "protect[s] the privacy and security of communications not authorized to be intercepted." Id. § 1006(b)(2). We cannot provide a specific estimate of the extent to which the cost of this capability will be borne by residential ratepayers, but we note again that Section 107(b)(3) provides for the Commission to "minimize the cost of * * * compliance" on residential ratepayers, not to absolve carriers from compliance because of such costs. 47 U.S.C. § 1006(b)(3). Requiring originating carriers to extract post-cut-through digits should not adversely affect "the provision of new technologies and services to the public" (id. § 1006(b)(4)), and we see no reason why this capability cannot be implemented within 24 months after revised technical standards are adopted pursuant to the Commission's Report and Order, if not sooner.

H. Delivery Interface

1. In order for call content and call-identifying information to be delivered from a carrier to a law enforcement agency, the parties must use a common delivery interface. Although the J-Standard contains non-binding information regarding the delivery protocols preferred by law enforcement (see J-STD-025, Annex A, §§ A.5-A.6 & Figures 23-25), it does not contain any limitation on the number of protocols that may be used by carriers to deliver call content and call-identifying information.

Section 103 does not obligate carriers to use any particular delivery interface, and the government has not asked the Commission to impose such an obligation. However, the government has asked the Commission to place a limitation on the number of interfaces employed by carriers under the J-Standard. See Government Petition 57-58 & Appendix 1 (§ 64.1708(j)). As explained in the Government Petition, a limit on the number of protocols is necessary to "ensure," as a

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

The Government Petition therefore asks the Commission to limit the number of interfaces to no more than five for the delivery of call content (i.e., five CCC protocols) and five for the delivery of call-identifying information (i.e., five CDC protocols). See Government Petition, Appendix 1 (§ 64.1708(j)). Within this limit, industry should be free to determine for itself which protocols will be used. In proposing a limit of five protocols, we do not mean to suggest that five is the only reasonable limit. The adoption of some reasonable limit, however, is necessary to ensure that the assistance capability requirements of Section 103 are not rendered illusory in practice by a proliferation of differing protocols. The Commission therefore should determine that the J-Standard's failure to place a limit on the number of delivery interfaces renders it deficient and should require industry to select an appropriately limited number of protocols for use under the J-Standard.

2. Although the Government Petition asks the Commission to include a limit on the number of delivery interfaces as part of the Commission's Report and Order, the Notice does not express a tentative conclusion about the appropriateness of such a limit, nor does it seek comments on the issue. The omission of this issue from the Notice may reflect a perception on the part of the

Commission that the government is no longer seeking to modify the J-Standard in this regard. See Notice ¶ 13 & n.30. If so, that perception is incorrect.

The Commission may have misunderstood the import of a letter from Assistant Attorney General Stephen R. Colgate to Mr. Tom Barba regarding CALEA's assistance capability requirements, a copy of which is attached as an appendix to the Government Petition. In that letter, Assistant Attorney General Colgate stated that "a single delivery interface is not mandated by CALEA." Government Petition, Appendix 5, p. 3 (emphasis added). The Colgate letter went on to explain that the government supported a compromise under which industry would employ "a limited number of no more than five delivery interfaces." Ibid.

The Notice implies that the Commission understands the Colgate letter to have dropped the subject of delivery interface protocols from the government's "punch list." See Notice ¶ 13 & n.30. That is not the case. The Colgate letter simply states that Section 103 of CALEA does not obligate industry to select "a single delivery interface." The letter does not suggest that carriers should therefore be free under the J-Standard to employ an unlimited number of delivery interface protocols. To the contrary, it urges the adoption of a specific limit on the number of protocols. The Government Petition, filed after the Colgate letter, reiterates that request. In short, the government continues to believe that a limitation on the number of delivery interface protocols is necessary in order to ensure the effective delivery of call content and call-identifying information under Section 103 of CALEA, and we renew our request for the Commission to include such a limitation in its Report and Order.

3. Imposing a limitation on the number of delivery interface protocols is consistent with the criteria of Section 107(b) of CALEA. For the reasons given above, limiting the number of

delivery interfaces will ensure that industry "meet[s] the assistance capability requirements" of Section 103 and will do so "by cost-effective methods." 47 U.S.C. § 1006(b)(1). Placing a limit on the number of delivery interface protocols will not affect "the privacy and security of communications not authorized to be intercepted" and should not increase "the cost of * * * compliance on residential ratepayers." Id. § 1006(b)(2)-(3). Because the government's proposal would leave to industry itself the choice of which protocols to use, and because the proposal would impose no restriction on the choice of protocols for other (non-CALEA-related) network delivery functions, the proposal would not impair "the provision of new technologies and services to the public. Id. § 1006(b)(4). And because industry is free to select from existing delivery interface protocols, rather than having to develop new protocols, there is no need to provide for a special transition period or transitional obligations once industry has designated its preferred protocols pursuant to the Commission's Report and Order. Id. § 1006(b)(5).

III. Comments Regarding Other Capabilities

The Commission also has requested comments regarding two aspects of the J-Standard that have been called into question by CDT and other privacy groups. First, the J-Standard requires carriers to provide law enforcement with access to certain information regarding the location of mobile terminals when law enforcement is legally authorized to obtain such information. CDT contends that the J-Standard's location information provisions are invalid because location information is not "call-identifying information." Second, when communications are transmitted using packet switching protocols, the J-Standard requires carriers to deliver the entire packet data stream associated with a given communication, including call content, except where information is not authorized to be acquired. CDT argues that when law enforcement lacks legal authority to intercept

call content, Section 103(a)(4)(A) of CALEA (47 U.S.C. § 1002(a)(4)(A)) requires carriers to strip out call content from the packet data stream before delivering it to law enforcement. The Commission has tentatively rejected the first of these two objections and has asked for additional comments regarding the issues raised by the second objection. For reasons that we present below, we agree with the Commission's tentative conclusion regarding location information, and we do not believe that CALEA requires the Commission to modify the J-Standard's packet mode provisions in the manner urged by CDT.

A. Location Information

1. In certain circumstances, the J-Standard requires carriers to provide law enforcement agencies with location information at the beginning and end of communications to and from mobile terminals. See J-STD-025 § 5.4.1 (Answer Message parameters), § 5.4.5 (Origination Message parameters), § 5.4.6 (PacketEnvelope Message parameters), § 5.4.8 (Release Message parameters). The "Location" parameter is defined as a text string that "provides location information about the subject's mobile terminal." Id. § 6.4.6.

The Commission has tentatively concluded that location information is "call-identifying information" under CALEA. Notice ¶ 52. For reasons that we have previously presented to the Commission, we agree with that conclusion. As we have explained previously, location information comes within the general statutory definition of "call-identifying information" (47 U.S.C. § 1001(2)), and Section 103(a)(2) of CALEA (47 U.S.C. § 1002(a)(2)) excludes location information from that general definition only in cases where a law enforcement agency is acquiring information "solely pursuant to the [statutory] authority for pen registers and trap and trace devices * * * ." See

Government May Comments at 17-21; Government June Reply Comments at 78-79. We incorporate our earlier comments on this issue by reference here.

2. The Notice states that the J-Standard is "unclear" regarding the degree of specificity required for location information. Notice ¶ 54. The Commission has tentatively concluded that "location information should be construed [in the J-Standard] to mean cell site location at the beginning and end of the communication." Id. ¶ 55. The Notice requests comment on this tentative conclusion.

We agree that the J-Standard requires a carrier only to have the capability to supply cell site information (or comparably specific location information), and only at the beginning and termination of the call. This means that a carrier that has the capability of supplying cell site information is in compliance with this part of the J-Standard and, hence, in compliance (in this respect) with Section 103 of CALEA. See Government May Comments at 19. A carrier need not have the capability to deliver more detailed location information in order to satisfy its obligations under the J-Standard and CALEA.[9]

---

[9] While CALEA does not require carriers to deliver more extensive location information than that specified by the J-Standard, neither does CALEA prohibit them from delivering more extensive location information when: (1) they have designed their networks to generate such information; and (2) law enforcement has been legally authorized by a court to obtain such information. In relatively rare cases, where law enforcement has shown that precise location information is vital to a criminal investigation, courts have ordered wireless carriers who possess such information to provide it to law enforcement. The delivery of such information is entirely consistent with Section 103(a)(4)(A) of CALEA, which obligates carriers to protect "the privacy and security of communications and call-identifying information not authorized to be intercepted" (47 U.S.C. § 1002(a)(4)(A)), because the information will be provided only when it is "authorized to be intercepted." We repeat, however, that CALEA does not obligate carriers to design their networks to provide more extensive location information than the J-Standard itself specifies.

3. The Commission has tentatively concluded that the location information required by the J-Standard is "reasonably available." Notice ¶ 56. While determinations of "reasonable availability" may vary among carriers and platforms (see pp. 18-19 supra), this tentative conclusion is likely to be correct as a general matter. As the Notice points out, location information is already available to wireless carriers in connection with billing, hand-off, and system use features. Ibid. And as the Notice points out, carriers will also be required to have location information capabilities by the E911 initiative. Ibid. As a result, the location information covered by the J-Standard should be "reasonably available" to wireless carriers even under the existing definition of "reasonably available" in the J-Standard, and a fortiori, such information should be "reasonably available" if that definition is modified in the respects that we have proposed (see pp. 20-25 supra). In response to the Commission's request for comments on "how the Commission should decide or interpret the term 'reasonably available' in the context of the proposed location information requirement" (Notice ¶ 56), we do not believe that there is any need for the Commission to interpret or construe "reasonable availability" differently in connection with location information than in connection with the other kinds of call-identifying information at issue in this proceeding.

4. Because the J-Standard's location information provisions do not render the J-Standard deficient, the Commission need not address the statutory criteria in Section 107(b), which are directed at determining how deficiencies in industry standards are to be redressed. We note, however, that providing location information is consistent with those statutory criteria. For reasons that the Commission itself has recognized, location information is "call-identifying information," and therefore must be provided to law enforcement in order to "meet the assistance capability requirements" of Section 103. 47 U.S.C. § 1006(b)(1). Such information can be provided "by cost-effective methods"

(ibid.), particularly in light of the fact that the same kind of information is already generated and used by wireless carriers for other purposes. As explained above, the J-Standard makes location information available only when law enforcement is judicially authorized to obtain it, and hence the J-Standard does not jeopardize "the privacy and security of communications not authorized to be intercepted." Id. § 1006(b)(2). The J-Standard's location information provisions should not materially affect residential ratepayers, nor should they interfere with "the provision of new technologies and services to the public." Id. § 1006(b)(3)-(4). Finally, we agree with the Commission (see Notice ¶¶ 46, 55) that the compliance deadline of June 30, 2000, previously established by the Commission should be sufficient for development and implementation of this feature.

B. Separation of Call Content and Call-Identifying Information in Packet Mode Communications

CDT's petition presents a discrete objection to the J-Standard's treatment of packet mode communications. The J-Standard requires carriers transmitting communications using packet switching protocols to deliver the entire packet data stream associated with a given communication, including call content, except where information is not authorized to be acquired. See J-STD-025 § 4.5.2, ¶ 2 (Packet Data IAP). CDT has asserted that this aspect of the J-Standard violates Section 103(a)(4)(A) of CALEA, which requires carriers to "protect[] * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ." 47 U.S.C. § 1002(a)(4)(A). CDT has asked the Commission to modify the J-Standard to require carriers to strip out call content from the packet data stream when law enforcement is operating on the basis of pen register authority, so that call content that law enforcement is not authorized to intercept is not

transmitted. See Notice ¶ 59; CC Docket No. 97-213, CDT Comments at 34-38 (filed May 20, 1998).

The Commission has not reached a tentative conclusion regarding CDT's proposal. Instead, it has requested additional comments and information. The Commission is seeking comments not only on the specific packet mode issue raised by CDT, but also on more general issues regarding how CALEA should be applied to packet mode communications. See Notice ¶¶ 63-66. In response to the Commission's request, we first address the specific issue raised by CDT: whether Section 103(a)(4)(A) requires carriers to remove call content from packets that are sent to law enforcement on the basis of pen register authority. We then address the broader packet mode issues identified in the Notice.

1. At the outset, we wish to make one point very clear: the government has no desire to receive call content from carriers when its legal authority does not entitle it to intercept call content. As a result, if the J-Standard had provided for carriers to strip out call content from the packet stream in pen register cases, as CDT proposes, rather than relying on law enforcement to perform that function, the government would have been -- and still would be -- satisfied with such an arrangement. The initiative for delivering "full" packets to law enforcement, even in pen register cases, has come from industry, not from law enforcement.

Having said that, however, we must be equally clear in saying that the J-Standard's treatment of packet mode communications in pen register cases does not conflict with anything in CALEA, and hence the J-Standard is not legally deficient in this regard. See Government May Comments at 21-22. As we have explained previously, CALEA amended the pen register statute (18 U.S.C. §§ 3121 et seq.) to require law enforcement to "use technology reasonably available to it that restricts the

recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." 18 U.S.C. 3121(c) (added by Section 207(b)(2) of CALEA). As a technical matter, it is perfectly feasible for law enforcement to employ equipment that distinguishes between a packet's header and its communications payload and makes only the relevant header information available for "recording or decoding."[10] In pen register cases involving packet mode communications, the J-Standard simply -- and quite permissibly -- relies on law enforcement to comply with its legal obligations under 18 U.S.C. § 3121(c) in this fashion.

The Notice suggests that if a carrier were to deliver both call-identifying information and call content to law enforcement in a pen register case, it would "seem" (Notice ¶ 63) to violate the carrier's obligation under Section 103(a)(4)(A) to "protect[] * * * the privacy and security of communications and call-identifying information not authorized to be intercepted * * * ." But that is what has always happened in pen register cases in the analog environment. As we have explained before, and as CDT itself has acknowledged, when garden-variety pen register surveillance is carried out over the "local loop" between the subscriber and the central office, law enforcement receives access to all signals transmitted over the subscriber's line on the local loop, including call content as well as dialing and signaling information. In such cases, the signals are sent to a device that is configured to record and decode the dialing and signaling information utilized in call processing (see p. 26 supra) without recording or disclosing the call content. Nothing in the language or legislative history of CALEA indicates that Congress meant to prohibit this longstanding arrangement. It is worth noting that Section 103(a)(4) does not state that carriers "shall not deliver" communications

---

[10] The ability to distinguish between headers and payload is inherent in packet mode protocols. The position of the payload within the packet either is identified in the header or is defined (i.e., fixed) by the protocol itself. With that information in hand, it is technically trivial to strip out the payload.

and call-identifying information that law enforcement is not authorized to intercept, but only that carriers shall "protect the privacy and security" of such information. A carrier is entitled to rely on law enforcement's discharge of its legal obligation under 18 U.S.C. § 3121(c) as a means of "protecting the privacy and security" of information that law enforcement is not authorized to intercept. Accordingly, the J-Standard is not deficient in this regard.

2. In connection with CDT's specific challenge to the J-Standard's packet mode provisions, the Commission has posed a number of broader questions about the application of CALEA to packet mode communications. See Notice ¶ 65. The Commission has asked for comments on "whether and, if so, how the statutory requirements of Section 103(a) of CALEA apply to packet-mode communications." Ibid. The Commission asks for comments on what constitutes "the equivalent of 'call-identifying information' for packet-mode telecommunications services within the context of CALEA." Ibid. And the Commission asks whether packet-mode call-identifying information "[w]ill * * * be 'reasonably available' to carriers and, thus, subject to the provisions of Section 103(a)(2) of CALEA." Ibid.

We understand the Commission's interest in developing a fuller understanding of how CALEA applies to packet mode communications. However, we urge the Commission to proceed cautiously and not to take on unnecessary burdens in this regard. CDT's specific challenge to the J-Standard can be resolved without the need to resolve broader questions that may arise concerning the relationship between CALEA and packet mode communications. And if the Commission agrees that the J-Standard is not deficient in the specific respect identified by CDT, there is no need -- and no basis -- for the Commission to go further. As the Commission itself has stated, "the uncontested technical requirements [of the J-Standard] are beyond the scope of this proceeding." Notice ¶ 45

(emphasis added). CDT's rulemaking petition contests only one provision of the J-Standard involving packet mode communications (J-STD-025 § 4.5.2). As a result, other provisions of the J-Standard that may relate to packet mode communications are simply not within the scope of this proceeding, and absent any claim (much less any determination) that they are deficient, they are not subject to the Commission's standard-setting authority under Section 107(b).

Having said that, we offer the following comments on the general questions that the Commission has raised concerning packet mode communications. First, CALEA's assistance capability requirements do not draw any distinction between packet mode communications and circuit mode communications.[11] The obligations imposed by Section 103 apply equally to all "telecommunications carriers," meaning all "person[s] or entit[ies] engaged in the transmission or switching of wire or electronic communications as a common carrier for hire * * * ." 47 U.S.C. § 1001(8). The assistance capability requirements of Section 103 encompass all "wire and electronic communications," and all associated call-identifying information, carried by such carriers. Id. § 103(a)(1)-(2). If a telecommunications carrier is transmitting a "wire communication" or an "electronic communication," as those terms are defined (18 U.S.C. § 2510(1), (12)), the carrier must comply with Section 103 with respect to those communications, regardless of whether the carrier is using packet-mode technology or some other technology to transit the communications. Thus, to answer the Commission's threshold question, the statutory requirements of Section 103 do apply to packet mode communications, just as they apply to communications that are not transmitted using packet mode protocols.

---

[11] For a general discussion of the difference between packet mode communications and circuit mode communications, see J-STD-025, Annex B, § B.1.

As noted above in connection with our discussion of subject-initiated dialing and signaling information, CALEA does draw a statutory distinction between "telecommunications carriers" and providers of "information services." See 47 U.S.C. §§ 1001(6), 1001(8)(C)(i), 1002(b)(2)(A). This statutory distinction, however, does not correspond to any distinction between packet mode communications and circuit mode communications. A telecommunications carrier can use either packet mode or circuit mode technology to transmit wire and electronic communications. The use of packet mode protocols does not turn the transmission of a wire or electronic communication by a telecommunications carrier into the provision of information services.

As for what constitutes "the equivalent of 'call-identifying information' for packet-mode telecommunications services within the context of CALEA" (Notice ¶ 65), the starting point for analysis is the statutory definition of "call-identifying information" itself. "Call-identifying information" encompasses all "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). When information is transmitted using packet mode protocols, "call-identifying information" therefore would encompass all information that identifies (or is required to identify) the "origin, direction, destination, or termination" of the communication packet -- in short, all information used in routing the packet.

This information will be included in the parameters found in the packet header. In the case of connectionless packet mode services (Notice ¶ 65), the header of each packet will identify the packet's origin and destination addresses. In the case of connection-oriented packet mode services (ibid.), the packet header contains a connection identifier that is associated with the origin and

destination addresses. The specific parameters that identify the "origin, direction, destination, or termination" of the packet will vary depending on the data service and protocols involved.

Finally, whether packet-mode call-identifying information "[w]ill * * * be 'reasonably available' to carriers" (Notice ¶ 65) cannot be answered categorically, any more than one can state categorically whether circuit-mode call-identifying information will be reasonably available to carriers. The general definition of "reasonably available" that we have proposed above (see p. 25 supra) should be equally applicable to packet mode communication and circuit mode communications. Whether particular call-identifying information is reasonably available under this definition may vary among carriers, hardware platforms, and packet protocols. As long as a packet stream can be accessed, it is technically straightforward to isolate the parameters in the packet header that constitute call-identifying information, as indicated above.

DATE: December 14, 1998

Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

Donald Remy
Deputy Assistant Attorney General

_____

_____

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

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

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

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

Certificate of Service

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), Washington, D.C., hereby certify that, on December 14, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Comments Regarding Further Notice of Proposed Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Washington, D.C. this 14th day of December, 1998.

_____
David Yarbrough