

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington D.C.

**RECEIVED**

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

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

---

**COMMENTS  
OF THE  
UNITED STATES TELEPHONE ASSOCIATION**

Its Attorneys:

Lawrence E. Sarjeant  
Linda L. Kent  
Keith Townsend  
John W. Hunter

1401 H Street, NW, Suite 600  
Washington, D.C. 20005  
(202) 326-7248

December 14, 1998

No. of Copies rec'd 049  
List ABCDE

---

## **TABLE OF CONTENTS**

<b>SUMMARY</b> .....	<b>i</b>
<b>I. INTRODUCTION</b> .....	<b>1</b>
<b>II. THE INTERIM STANDARD SHOULD NOT BE MODIFIED</b> .....	<b>2</b>
<b>A. CALEA Limits Assistance Capability Requirements and Defers to the Industry to Promulgate Standards</b> .....	<b>3</b>
<b>B. The Cost of Implementing the Interim Standard and the Punch List Far Exceeds the Amount Appropriated</b> .....	<b>5</b>
<b>C. The Commission Must Allow a Reasonable Time to Comply With Any Modifications Adopted in this Proceeding</b> .....	<b>9</b>
<b>D. The Interim Standard Provides Sufficient Flexibility Regarding Packet-Mode Telecommunications</b> .....	<b>11</b>
<b>III. ALL OF THE FBI'S PUNCH LIST ITEMS ARE BEYOND THE SCOPE OF CALEA</b> .....	<b>13</b>
<b>IV. CONCLUSION</b> .....	<b>18</b>

## SUMMARY

USTA supports the J-STD-025 adopted by the industry standards-setting body. This standard is not deficient. It provides law enforcement with all of the capabilities required under Section 103. The standard already reflects compromises on the part of carriers. The Commission must recognize, as law enforcement fails to do, that Section 103 limits the scope of the assistance capability requirements and defers to the industry to promulgate standards. There is no requirement that the carrier alter its network to provide call identifying information. In fact, law enforcement is prohibited from requiring the design of systems or features.

USTA is concerned that the cost of implementing the standard and the punch list items far exceeds the amount appropriated. The Attorney General has obtained information regarding some of the manufacturer's costs; that information is subject to confidentiality agreements and has not been shared with industry. The Commission must obtain this information if it is to have a complete record upon which to conduct its review of the punch list items. Of course, the costs of the punch list items will be in addition to the software, hardware, training and installation costs which carriers must incur just to implement the standard. Deployment will significantly impact the implementation costs and the FBI has not provided the necessary guidance regarding the switch capacity requirements. USTA estimates that for its member companies, the installation costs could reach from \$2.2 to \$3.1 billion. When actual software costs and software release schedules become known and the per switch capacity requirements are specified by the FBI, the implementation costs could increase. The FBI has used its authority to promulgate cost recovery and capacity requirements which shift the costs to the carriers. USTA is challenging these regulations in court.

The Commission must also allow a reasonable time to comply with any new requirements adopted in this proceeding. Wireline carriers are already addressing issues such as local number portability, opening of toll free codes and Year 2000. As explained in USTA's August 18, 1998 ex parte, wireline carriers need at least two years to implement switch changes.

USTA believes that the interim standard provides sufficient flexibility regarding packet-mode telecommunications since it is not feasible to separate call identifying information from call content in packet-mode telecommunications. USTA also explains that the standard is not deficient regarding the FBI's wish list which goes far beyond the scope of the statutory language. None of the punch list items should be adopted.

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

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )  
 )  
Communications Assistance for Law )  
Enforcement Act )

CC Docket No. 97-213

---

**COMMENTS  
OF THE  
UNITED STATES TELEPHONE ASSOCIATION**

The United States Telephone Association (USTA) respectfully submits its comments in the above-referenced proceeding. USTA is the principal trade association of the local exchange carrier (LEC) industry. Its members provide over 95 percent of the incumbent LEC-provided access lines in the U.S. USTA's member companies are telecommunications carriers as defined in the Communications Assistance for Law Enforcement Act (CALEA).

**I. INTRODUCTION.**

In a Further Notice of Proposed Rulemaking (FNPRM) released November 5, 1998, the Commission has requested comment on alleged deficiencies in the technical standards for telecommunications carriers to meet the assistance capability requirements contained in CALEA.<sup>1</sup> USTA, in association with the Cellular Telecommunications Industry Association (CTIA) and the Personal Communications Industry Association (PCIA), filed a response to both the CDT and DOJ/FBI deficiency petitions on April 9, 1998. In that response, USTA, CTIA and

---

<sup>1</sup>See, Center for Democracy and Technology (CDT) Petition for Rulemaking Under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed March 26, 1998 and Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) Joint Petition for Expedited Rulemaking, filed March 27, 1998.

PCIA requested that the Commission resolve the issues regarding the interim industry standard, J-STD-025, remand to the Telecommunications Industry Association (TIA) TR45.2 Subcommittee any determination regarding the standard ultimately adopted by the Commission so that Subcommittee could develop additional technical requirements as needed, toll the compliance date during the Commission's deliberations, grant an industry-wide extension of the compliance date to allow adequate time to implement the revised standard, ensure that any rule promulgated by the Commission is voluntary so that carriers retain the opportunity to determine the best means to meet the assistance capability requirements of CALEA given their particular equipment and resources and make a determination as to whether compliance with CALEA is reasonably achievable at this time. USTA continues to support this request. As will be discussed herein, USTA maintains its support for the J-STD-025. The packet-mode provisions contained in the standard are sufficient to meet the assistance capability requirements of Section 103 of CALEA. The nine punch list items are beyond the scope of the plain wording of the statute and should not be included in the standard.

## **II. THE INTERIM STANDARD SHOULD NOT BE MODIFIED.**

Under Section 107(b) of CALEA, the Commission must determine whether, based upon an analysis of the statute, J-STD-025 is deficient for failure to satisfy the assistance capability requirements of Section 103. The standard is not deficient. It provides law enforcement with all of the capabilities required by CALEA. The standard was the product of the compromise and consensus-building which is typical of the process by which interested participants develop and implement industry standards. Both law enforcement and telecommunications carriers participated in the development of J-STD-025. Consequently, the resulting standard already

reflects compromises on the part of carriers. It includes features, such as location tracking and the delivery of packet information containing both call-identifying information and call content even when law enforcement was not authorized under the statute to receive call content. Despite the fact that carriers believed that these features were beyond the scope of CALEA, they were accepted in an effort to accommodate law enforcement requests.

**A. CALEA Limits Assistance Capability Requirements and Defers to the Industry to Promulgate Standards.**

Law enforcement consistently ignores the fact that Section 103 limits the scope of the assistance capability requirements. Under Subsection 103(a), carriers are only required to provide law enforcement access to call identifying information about the origin and destination of communications that is reasonably available to the carrier. There is no requirement that the carrier must alter its network to provide call identifying information. As the legislative history explains, “[h]owever, if such information is not reasonably available, the carrier does not have to modify its system to make it available.”<sup>2</sup>

Under Subsection 103(b) law enforcement is not permitted to require the specific design of systems or features, nor prohibit adoption of any such design, by wire or electronic communications service providers or equipment manufacturers. “The legislation leaves it to each carrier to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communication can be

---

<sup>2</sup>H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 22.

intercepted at some point that meets the legislated requirements.”<sup>3</sup> As the legislative history reveals, Congress intended the assistance capability requirements to be both a floor and a ceiling. “The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information it had in the past. The Committee urges against overbroad interpretation of the requirements.”<sup>4</sup> Failure to provide the capabilities listed in Section 103 is the sole statutory basis upon which the Commission may make its determination regarding the deficiency of the standard. This is important because the challenge to the standard advanced by law enforcement is based on its request for features that go far beyond the scope of Section 103.

USTA strongly supports the Commission’s tentative conclusion that the technical requirements of the standards, consistent with the Commission’s determination reached in this proceeding, should be developed by the established standards-setting bodies and/or individual carriers. This is entirely consistent with CALEA. Section 103(a) specifies that *a carrier* shall ensure that its equipment, facilities, or services comply with the assistance capability requirements. Section 107(a) discusses compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization. The legislative history confirms this.

The legislation provides that the telecommunications industry itself shall decide how to implement law enforcement’s requirements. The bill allows industry associations and standard-setting bodies, in consultation with law enforcement, to establish publicly available specifications creating ‘safe harbors’ for carriers.

---

<sup>3</sup>*Id.* at 23.

<sup>4</sup>*Id.* at 22.

This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and finding ways to meet them without impeding the deployment of new services...The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements...Section 2606 established a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations.<sup>5</sup>

Clearly, the Commission should analyze the proposals to alter the interim standard consistent with the intent of Congress which requires that the industry standard be given deference and the assistance capability requirements be narrowly interpreted so as not to require any specific design or system configurations or to expand law enforcement's current capabilities.

**B. The Cost of Implementing the Interim Standard and the Punch List Far Exceeds the Amount Appropriated.**

According to the legislative history, CALEA requires the Federal government to pay all reasonable costs incurred by industry to retrofit existing facilities to bring them into compliance with the interception requirements. Congress authorized \$500 million for that purpose and specified that if that amount was not sufficient, "any equipment, features or services deployed on the date of enactment which government does not pay to retrofit, shall be considered to be in compliance until the equipment, feature or service is replaced or significantly upgraded or otherwise undergoes major modification...However, to the extent that industry must install additional capacity to meet law enforcement needs, the bill requires the government to pay all capacity costs from date of enactment...The Federal government, in its role of providing technical support to state and local law enforcement, will pay costs incurred in meeting the initial

---

<sup>5</sup>*Id.* at 19, 22, 26.

capacity needs and the future maximum capacity needs for electronic surveillance at all levels of government.”<sup>6</sup> In accordance with Subsection 104 (e), until the Attorney General agrees to reimburse a carrier for such modifications, the carrier shall be considered to be in compliance with the capacity notices.

While the Commission has requested information on the costs associated with law enforcement’s punch list items, the Commission must be aware that the initial expenditures for CALEA will involve implementation of J-STD-025. The costs to develop and implement the punch list items will be in addition to those amounts. DOJ has obtained cost estimates from some manufacturers regarding the development and implementation of J-STD-025 and each of the punch list items. That information is subject to confidentiality agreements, although it is unclear whether such agreements would cover aggregated information. Even so, the DOJ has shared some of this information with Congress and the Attorney General, and, in an October 6, 1998 letter to Senator Ted Stevens, indicated that moving CALEA’s grandfather date would cost the government in excess of \$2 billion. USTA has joined with CTIA, PCIA and TIA in requesting that the Attorney General provide the Commission with the basis for the \$2 billion estimate, any aggregate information which may be disclosed and any assumptions or formula used to analyze the costs. The Associations also requested that the Attorney General provide detailed information on the cost assumptions included in any proposal for a national buy out of specific platforms or equipment. If the Commission is to receive the cost information it has requested as part of its Section 107 analysis, it must obtain this information from DOJ.

---

<sup>6</sup>*Id.* at 16.

USTA has attempted to gather implementation cost information from some of its member companies. In order to implement the Section 103 requirements, carriers must provide CALEA capability and capacity in every switch. Capability costs consist of software costs, hardware costs to support the software functions and delivery of surveillance, training costs and installation costs. Capacity costs consist of the hardware cost to meet the capacity requirements adopted by the FBI and installation costs.

As explained above, given the lack of information, it is difficult to estimate the capability costs. In order to implement CALEA capability into every switch, the software must be developed by and obtained from the manufacturers subject to a right to use fee. It is not known whether DOJ will undertake a national buyout from each switch manufacturer for the software. In addition, as noted above, not all manufacturers have provided DOJ with software cost estimates for the standard and the punch list items.

Deployment will significantly impact the implementation costs. If J-STD-025 is required to be installed in every switch by June 30, 2000, implementation costs would be much higher than if DOJ would prioritize switches which it believes must be compliant by that date and permit the remaining switches to be CALEA-compliant as part of a regularly scheduled upgrade. Some manufacturers are planning to provide the J-STD-025 capability over several software loads which may require out-of-cycle software purchases which will increase the cost of implementation. Some switches may require additional software loads anyway due to the vintage of the switch. Hardware costs may vary due to the architecture of the switch.

Based on preliminary schedules of the major wireline switch manufacturers, the availability of the software for the punch list items will be later than the availability of the

standard itself and may not be grouped into a generic software release. This will increase the number of software upgrades and the costs, particularly if the purchases must be made out-of-cycle from regularly scheduled upgrades.

The capacity requirements included in the FBI's Final Notice of Capacity adopted March 12, 1998, which itself was three years late, will significantly increase the costs of implementation. While USTA requested guidance from the FBI to assist in developing traffic models to determine the number of call data and call content channels per office, the FBI refused to cooperate. Consequently, the assumptions used to estimate the per switch capacity impacts the cost of deployment. For example, cost estimates based on historical capacity as compared to the FBI's maximum number per county can vary by a factor of four or more. In addition, the FBI's Final Capacity Notice provides little guidance for allocating the county capacity number to individual switches within the county. Without this information, carriers and the government may have to incur the exorbitant costs of providing the county capacity in every switch. Significant costs also will be incurred to design and provide receivers to collect post dialing digits and network tones if the Commission were to require this capability despite the fact that it is not available to the carrier.. Of course these costs could be avoided if the FBI would utilize call content channels where signals could be delivered to existing pen register devices for recording -- in effect preserving the capability available today.

USTA estimates that implementation costs for its member companies could reach from \$2.2 to \$3.1 billion. When actual software cost and software release schedules become known and the per switch capacity requirements are defined by the FBI, the implementation costs could increase.

Adding insult to injury and contrary to the statute which requires that all the costs of modifying existing equipment, much of the cost of designing and deploying future equipment and all of the cost of providing capacity be borne by the government, the FBI has used its authority to promulgate cost recovery and capacity regulations which shift the costs to the carriers by minimizing the costs eligible for reimbursement. USTA has challenged these regulations in court. USTA urges the Commission to seek the actual cost information from the Attorney General so that it will have a complete record upon which to conduct its review of the punch list items pursuant to Section 107.

**C. The Commission Must Allow a Reasonable Time to Comply With Any Modifications Adopted in this Proceeding.**

As the Commission states, Subsection 107(b)(5) requires that carriers be afforded a reasonable amount of time to comply with and/or transition to any new standards. Pursuant to Subsection 107(c), the Commission extended the compliance date for the "core" features of J-STD-025 or the development of an individual solution until June 30, 2000. The Commission must also provide a reasonable amount of time to implement any new technical requirements which it may adopt in this proceeding.

This is particularly important given the costs which the wireline industry will be forced to bear and the system changes which the wireline industry must implement to address other important issues such as local number portability, the opening of toll free codes 866 and 855 by April 1, 2000 and July 1, 2000 respectively and Year 2000 computer changes. For example, these carriers must provide local number portability for the top 100 MSAs by December 31, 1998. After that date, incumbent LECs have at most 180 days, and in the majority of cases it is

less time, after receipt of a bona fide request to provide local number portability. In order to address the Year 2000 issues, carriers have announced that they will impose a moratorium on any switch activity during the period from December 1999 to February 2000. These activities will make it difficult to meet the June 30, 2000 CALEA compliance date already adopted by the Commission for J-STD-025. In most companies and particularly in small telephone companies, the same personnel are responsible for implementing the necessary changes in the network. USTA would recommend that these items take priority as both the Commission and the carriers have already planned for implementation of the changes necessary to accommodate those issues.

The initial timeframe should, in any event, be no sooner than two years after an order is adopted by the Commission. As USTA explained in an August 18, 1998 *ex parte*, a large wireline carrier would require approximately twelve months from the time a software product is generally available to make a generic switch upgrade in every switch.<sup>7</sup> An additional year will be required to install a hardware product and/or additional generic loads which may be necessary depending upon the switch. Any installation plan contemplated by a wireline carrier must consider the vintage of each switch, the status of the existing platform, the carrier's budget planning and the availability of reimbursement from the government as required by CALEA. The Commission must ensure that any new technical requirements are implemented in the most efficient and cost effective manner.

---

<sup>7</sup>The term "generally available" is significant. Usually, after a manufacturer has completed the coding of new software, there is a period of from three to six months during which the software is tested in a live switch in the network (variously called "first office application" or "verification office" testing) before the software is generally available.

**D. The Interim Standard Provides Sufficient Flexibility Regarding Packet-Mode Telecommunications.**

Unlike traditional telecommunications services, including ISDN and SS7, which generally separate call identifying information from call content, packet mode data services combine the call identifying information and the content in a single protocol data unit. It is not feasible to separate call identifying information from call content in packet-mode telecommunications.

Data traffic is growing exponentially. Router and switch manufacturers can barely keep up with user demand. All manner of innovative techniques are being employed to streamline and speed up the processing and routing of packets. For example, wherever possible, routing is being embedded in hardware or firmware to achieve maximum speed. Self routing techniques are being employed to route packets immediately rather than examining the packets via software algorithms. The elimination of the software processing in order to achieve needed speeds also eliminates the flexibility that would be needed to separate call identifying data from call content. If each protocol unit had to be analyzed by software to determine if it is subject to law enforcement interception, then processed in software to separate call identifying data from call content, analyzed again for routing to the proper law enforcement agency, and processed to ensure appropriate formatting, not only would the cost of data switches and routers increase drastically, but performance and delivery of user data would suffer drastically. It is important to note that the processing procedure described above would have to be applied to all data packets, not just the small number of packets subject to interception by law enforcement.

Traditional telecommunications services networks require a small number of interfaces and interconnections and have a predictable hierarchy of interconnecting relationships to complete a call. In contrast, data networks have a large number of interfaces, protocols and interconnecting arrangements which are still evolving; i.e., frame relay, SMDS, cell relay and the Internet's various higher level protocols. Different standards and procedures would have to be developed for each if call identifying information and call content were required to be separated.

The configuration of a packet network also inhibits the ability to separate call identifying information from call content. In traditional telecommunications networks, services and applications are implemented in and delivered by the network. For example, the central office switch that serves the target of a law enforcement surveillance provides services such as caller ID and call forwarding and "knows" the target's use of those services; i.e., the calling and called number, time of call and time of disconnection. In packet networks, the "services" are provided outside the network through the user's PC and the various servers with which the PC interacts. Even the idea of a "call" is different. While the traditional telephone network establishes a path between the surveillance target and the called party, in a data network each packet stands on its own and the "call" exists only for the period of time it takes the packet to transit the network, or several interconnected networks, and arrive at its destination. In some cases, due to data network congestion, the packet never arrives.<sup>8</sup>

---

<sup>8</sup>In the case of hybrid services such as Internet telephony, separation of call data from content becomes even more difficult. For example, if the target uses an Internet telephony service to complete a voice telephone call, the carrier's frame relay switch has no information regarding the nature of the packets being carried between the target's LAN and the Internet Service Provider. The switch cannot detect whether the information being transmitted contains

(continued...)

It is clear that requiring packet-mode telecommunications to be compliant with CALEA would inhibit the development of new, faster services and features. As the Commission notes, it is premature to impose any particular technical requirements for packet-mode telecommunications at this time. The J-STD-025 addresses this issue by providing for an option for carriers to deliver content for law enforcement to separate call identifying information from call content. This compromise reflects both the reasonable availability of technical requirements and the reasonable achievability of such requirements. The standard should not be altered.

**III. ALL OF THE FBI'S PUNCH LIST ITEMS ARE BEYOND THE SCOPE OF CALEA.**

The nine additional punch list items which constitute law enforcement's wish list of electronic surveillance capabilities go far beyond simply preserving the intercept capabilities that previously existed and represent an expansion of law enforcement's surveillance capabilities. As discussed above, Congress stated that the statute should be interpreted narrowly and it expressly limited the scope of the assistance capability requirements. Congress also required that deference be given the industry-developed standards. Close examination of J-STD-025 compared to the wish list of law enforcement reveal that the standard is not deficient, but facilitates full compliance with CALEA. While the Commission properly recognizes that three of the features, surveillance status, feature status and continuity check tone, should not be included in the standard, all of the remaining punch list items are beyond the scope of CALEA and must be rejected as well.

---

<sup>8</sup>(...continued)

e-mail data, digitally encoded voice content or call set-up information. If the Internet service provider offers some form of secure service, the communication could be encrypted.

### 1. Content of Subject-Initiated Conference Calls.

This function expands law enforcement's capabilities to enable monitoring of a multiparty or conference call after the subject leaves the call. Therefore, it involves interception of conference call communications that do not involve any person directly using the telephone equipment or facilities covered by the intercept order. Law enforcement has claimed that this capability was historically available. With call waiting and three way calling services widely available in 1984, the delivery of conversations of parties on hold could not be achieved by monitoring the target's line. If the target could not hear the parties on hold, neither could anyone else. Thus, this capability was not historically available and is not reasonably available now. In addition, modification of a separate conference bridge service, rented for the call, to accommodate content surveillance of all participants on a conference call is not reasonably achievable.

This item is contrary to the wording of Subsection 103(a)(1) which requires interception only of communications *to or from* equipment, facilities or services of a subscriber. This functionality would include communications that do not even touch the subscriber's facilities as well as communications that merely transit a subscriber's facilities. J-STD-025 provides for delivery of all communications that may be heard by any person using the intercept subject's facilities, including the communications of all participants in a conference call that may be heard over the facilities. The Commission must reject this item as beyond the scope of CALEA.

### 2. Party Hold, Join, Drop on Conference Calls.

This item would require a carrier to generate a data message for law enforcement when a party to a conference call is placed on hold by the intercept target, a party joins a conference call

or a party is dropped from a conference call. This capability was not historically available and represents a significant expansion of previous wiretapping capability.

J-STD-025 already requires provision of information that satisfies the “party join” and “party drop” capabilities. The standard requires provision of a data message to law enforcement when a party joins a conference call supported by the subscriber’s facilities — either through initiation by the subscriber of a call to a new party who is added to the call, or through receipt of a call from a new party who is added to the conference call. The standard also requires provision of a data message when a party is released from a conference call. The J-STD-025 contains the capability that is reasonably available and reasonably achievable.

J-STD-025 does not require any message when a party is placed on hold or released from hold by the intercept target. Party hold information does not meet the definition of call-identifying information contained in the statute. A party on hold does not identify “the origin, direction, destination or termination of communication”. To the extent that a party is placed on hold by a hold key on the subscriber’s equipment, it will not be detected by the network. Thus, party hold is not reasonably available.

### 3. Subject-Initiated Dialing and Signaling Information.

This item refers to information which is generated by actions taken by the intercept target, such as dialing, the use of flash hooks, feature keys and all key usage by the target. Subject-initiated dialing is not call identifying information because it does not identify the origin, direction, destination or termination of a communication. Further, local signaling activity, such as signaling that is internal to a PBX, is not reasonably available to the carrier. Such information is not used by the carrier and thus there would be no reason for the carrier to incur the costs to

detect it. New signaling systems would have to be designed and installed to make local signaling information available to law enforcement which would be extremely expensive.

J-STD-025 requires the provision of all reasonably available call-identifying information that law enforcement could obtain from subject-initiated signaling activity: signaling activity that is transmitted from the subscriber to the network and detected by the switch and signaling activity that controls local functions of the subscriber's equipment. This is sufficient to provide law enforcement with relevant call-identifying information resulting from subject-initiated, network detected signaling activity.

#### 4. In-Band and Out-of-Band Signaling.

This item would require a carrier to capture all network/switch-generated tones, as well as out-of-band signaling messages and to deliver them via a call data channel. In-band detection and extraction in the switch is not reasonably available within the scope of current switch architecture and would not be reasonably achievable as design and hardware and software additions would be required. J-STD-025 requires that most audible signaling information be provided over the call content channel. Historically, this is exactly how this information has been provided to law enforcement. The standard is not deficient.

#### 5. Timing Information.

This item would require delivery of call-identifying information within three seconds of the event producing the call-identifying information and a time stamp indicating the timing of the event to an accuracy of 100 milliseconds. Such requirements are not reasonably available given the capabilities of existing networks. Such performance standards are not included in any of the requirements of Section 103.

J-STD-025 stipulates that call-identifying information will be provided to law enforcement as soon as it is generated, except when the call data channel becomes congested. It is law enforcement's responsibility to ensure it has ordered a sufficient number of such channels to facilitate interceptions without congestion.

#### 6. Dialed Digit Extraction.

This item would require carriers to extract digits dialed by the target after the circuit is set-up by the switch and deliver those digits to law enforcement through the call data channel, despite the fact that monitoring and interpreting these digits historically has been achieved through a call content channel and J-STD-025 provides for a call content channel to be connected where law enforcement can obtain these digits.

Dialed digit extraction does not fall within the definition of call identifying information for the initial carrier because the initial carrier does not need to use the digits for call routing, or for any other purpose, and thus does not detect the digits in its switch. Further, post-cut-through digits are not reasonably available to the initial carrier as call-identifying information. Switches detect dialed digits through a "tone receiver" which is only connected to a call circuit until the call is completed. At that point the tone receiver is available for use on another call. Because tone receivers can be repeatedly used, switches contain far fewer tone receivers than the number of simultaneous calls the switch can support. Thus, dialed digit extraction through a call data channel is not reasonably available. In fact, major switch modifications would be required to dedicate a tone receiver for the duration of each call in order to detect post-cut-through digits and deliver them to law enforcement. In addition, newer technologies, such as voice-recognition dialing, would require even more complicated solutions to detect post-cut-through digits.

Requiring compliance with CALEA could interfere with the evolution of these new technologies.

In addition, the delivery of post-cut-through dialing information pursuant to a pen register order would not protect the privacy and security of call identifying information not authorized to be intercepted as required under Section 103. Post-cut-through digits include credit card numbers and responses to automatic queuing systems. This information may not be disclosed pursuant to a pen register order. A carrier would not be able to segregate protected information from digits used for call routing.

J-STD-025 permits access to all post-cut-through digits in two ways. The information is available through the call content channel provided by the carrier conducting the initial intercept because post-cut-through digits are transmitted on the call content channel just like any other content. In addition, post-cut-through dialing information is available pursuant to a pen register order or subpoena directed to the carrier that completes the call. Thus, the standard is not deficient and this item must be rejected.

#### **IV. CONCLUSION.**

The J-STD-025 represents the reasonably available and reasonably achievable technical requirements that fully meet the statutory requirements of Section 103. The Commission should give deference to the industry standard, as required by CALEA, and eliminate all of the punch list items. These items will add significant costs which are unjustified and may be unrecoverable

from the government, despite the intent of Congress, based on the cost recovery regulations adopted by the FBI. USTA urges the Commission to preserve the flexibility provided in the standard for packet-mode telecommunications. If the Commission adopts any new requirements, it must allow a reasonable time for the industry to implement those requirements.

Respectfully submitted,

**UNITED STATES TELEPHONE ASSOCIATION**

By: \_\_\_\_\_

*Linda L. Kent*

Its Attorneys:

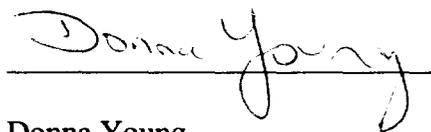
Lawrence E. Sarjeant  
Linda L. Kent  
Keith Townsend  
John W. Hunter

1401 H Street, NW, Suite 600  
Washington, D.C. 20005  
(202) 326-7248

December 14, 1998

**CERTIFICATE OF SERVICE**

I, Donna Young, do certify that on December 14, 1998, copies of the accompanying Comments of the United States Telephone Association were either hand-delivered, or deposited in the U.S. Mail, first-class, postage prepaid to the persons on the attached service list.

A handwritten signature in cursive script that reads "Donna Young". The signature is written over a horizontal line.

Donna Young

Rozanne R. Worrell  
U.S. Department of Justice  
Federal Bureau of Investigation  
Telecommunications Industry Liaison Unit  
P.O. Box 220450  
Chantilly, VA 20153

Michael Altschul  
Randall S. Coleman  
Cellular Telecommunications Industry Assn.  
1250 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20036

Roseanna DeMaria  
AT&T Wireless Services  
32 Avenue of the Americas - Room 1731  
New York, NY 10013

Stanton McCandlis  
Electronic Frontier Foundation  
1550 Bryant Street - Suite 725  
San Francisco, CA 94103

Stewart A. Baker  
Thomas M. Barba  
Brent H. Weingardt  
L. Benjamin Ederington  
Steptoe & Johnson LLP  
1330 Connecticut Avenue, NW  
Washington, DC 20036

Richard McKenna, **HQE03J36**  
GTE  
P.O. Box 152092  
Irving, TX 75015

Andre J. Lachance  
GTE  
1850 M Street, NW  
Suite 1200  
Washington, DC 20036

John T. Scott, III  
Crowell & Moring LLP  
1001 Pennsylvania Avenue, NW  
Washington, DC 20004

Mark C. Rosenblum  
Ava B. Kleinman  
Seth S. Gross  
AT&T  
295 North Maple Avenue - Room 3252J1  
Basking Ridge, NJ 07920

Jerry Berman  
Daniel J. Weitzner  
James X. Dempsey  
Center for Democracy and Technology  
1634 Eye Street, NW  
Washington, DC 20006

Andy Oram  
Computer Professionals for Social Responsibility  
P.O. Box 717  
Palo Alto, CA 94302

Matthew J. Flanigan  
Grant Seiffert  
Telecommunications Industry Assn.  
1201 Pennsylvania Avenue, NW  
Suite 315  
Washington, DC 20004

Gail L. Polivy  
GTE  
1850 M Street, NW  
Suite 1200  
Washington, DC 20036

James D. Ellis  
Robert M. Lynch  
Durward D. Dupre  
SBC  
175 E. Houston - Room 1258  
San Antonio, TX 78205

Lucille M. Mates  
Frank C. Magill  
SBC  
175 E. Houston  
Room 1258  
San Antonio, TX 78205

Kathryn Marie Krause  
Edward M. Chavez  
U S WEST, Inc.  
1020-19th Street, NW  
Suite 700  
Washington, DC 20036

Dan L. Poole  
U S WEST  
1020-19th Street, NW  
Suite 700  
Washington, DC 20036

John H. Harwood II  
Samir Jain  
Wilmer, Cutler & Pickering  
2445 M Street, NW  
Washington, DC 20037

Kevin C. Gallagher  
360° Communications Co.  
8725 W. Higgins Road  
Chicago, IL 60631

Joseph R. Assenzo  
Sprint Spectrum LP  
4900 Main Street  
12th Floor  
Kansas City, MO 64112

Emilio W. Cividanes  
Piper & Marbury, LLP  
1200-19th Street, NW  
Washington, DC 20036

David Cosson  
L. Marie Guillory  
NTCA  
2626 Pennsylvania Avenue, NW  
Washington, DC 20037

James T. Roche  
GlobeCast  
400 North Capitol Street, NW  
Suite 177  
Washington, DC 20001

Barbara J. Kern  
Ameritech Corp.  
2000 West Ameritech Center Drive  
Room 4H74  
Hoffman Estates, IL 60196

Kathleen Q. Abernathy  
David A. Gross  
Donna L. Bethea  
AirTouch Communications, Inc.  
1818 N Street, NW  
Washington, DC 20036

Judith St. Ledger-Roty  
Paul G. Madison  
Kelley Drye & Warren, LLP  
1200-19th Street, NW  
Fifth Floor  
Washington, DC 20036

Barry Steinhardt  
A. Cassidy Sehgal  
American Civil Liberties Union  
125 Broad Street  
18th Floor  
New York, NY 10004

Electronic Privacy Information Center  
666 Pennsylvania Avenue, SE  
Suite 301  
Washington, DC 20003

Electronic Frontier Foundation  
1550 Bryant Street  
Suite 725  
San Francisco, CA 94103

Elizabeth R. Sachs  
Lukas, McGowan, Nace & Gutierrez  
1111-19th Street, NW  
Suite 1200  
Washington, DC 20036

Carole C. Harris  
Christine M. Gill  
Anne L. Fruehauf  
McDermott, Will & Emery  
600-13th Street, NW  
Washington, DC 20005

Peter M. Connolly  
Koteen & Naftalin  
1150 Connecticut Avenue, NW  
Washington, DC 20036

Stuart Polikoff  
Lisa M. Zaina  
OPASTCO  
21 Dupont Circle, NW  
Suite 700  
Washington, DC 20036

J. Lloyd Nault, II  
BellSouth  
4300 BellSouth Center  
675 West Peachtree Street, NE  
Atlanta, GA 30375

Eric W. DeSilva  
Stephen J. Rosen  
Wiley, Rein & Fielding  
1776 K Street, NW  
Washington, DC 20006

Alan R. Shark  
American Mobile Telecommunications Assn., Inc.  
1150-18th Street, NW  
Suite 250  
Washington, DC 20036

William L. Roughton, Jr.  
PrimeCo Personal Communications, LP  
601-13th Street, NW  
Suite 320 South  
Washington, DC 20005

Michael K. Kurtis  
Jeanne W. Stockman  
Kurtis & Associates, PC  
2000 M Street, NW  
Suite 600  
Washington, DC 20036

Robert S. Foosner  
Lawrence R. Krevor  
Laura L. Holloway  
Nextel Communications, Inc.  
1450 G Street, NW  
Suite 425  
Washington, DC 20005

M. Robert Sutherland  
Theodore R. Kingsley  
BellSouth  
1155 Peachtree Street, NW  
Atlanta, GA 30309

Michael P. Goggin  
BellSouth  
1100 Peachtree Street, NE  
Suite 910  
Atlanta, GA 30309

Mark J. Golden  
Mary E. Madigan  
Personal Communications Industry Assn.  
500 Montgomery Street  
Suite 700  
Alexandria, VA 22314

Henry M. Rivera  
Larry S. Solomon  
J. Thomas Nolan  
M. Tamber Christian  
Ginsburg, Feldman & Bress, Chtd.  
1250 Connecticut Avenue, NW  
Washington, DC 20036

Caressa D. Bennet  
Dorothy E. Cukier  
Bennet & Bennet, PLLC  
1019-19th Street, NW  
Suite 500  
Washington, DC 20036

David L. Nace  
B. Lynn F. Ratnavale  
Lukas, Nace, Gutierrez & Sachs Chtd.  
1111-19th Street, NW  
Suite 1200  
Washington, DC 20036

Kevin C. Gallagher  
360° Communications Co.  
8725 W. Higgins Road  
Chicago, IL 60631

Glenn S. Rabin  
ALLTEL  
655-15th Street, NW  
Suite 220  
Washington, DC 20005

Pamela J. Riley  
David A. Gross  
AirTouch Communications, Inc.  
1818 N Street, NW  
Suite 320 South  
Washington, DC 20036

James F. Ireland  
Cole, Raywid & Braverman, LLP  
1919 Pennsylvania Avenue, NW  
Suite 200  
Washington, DC 20006

Rich Barth  
Mary Brooner  
Motorola, Inc.  
1350 Eye Street, NW  
Suite 400  
Washington, DC 20005

Teresa Marrero  
Teleport Communications Group, Inc.  
Two Teleport Drive  
Staten Island, NY 10311

John T. Scott, III  
Crowell & Moring, LLP  
1001 Pennsylvania Avenue, NW  
Washington, DC 20004

Elaine Carpenter  
Aliant Communicaitons  
1440 M Street  
Lincoln, NE 68508

William L. Roughton, Jr.  
PrimeCo Personal Communications, LP  
601-13th Street, NW  
Suite 320 South  
Washington, DC 20005

Michael W. Mowery  
AirTouch Communications, Inc.  
2999 Oak Road, MS1025  
Walnut Creek, CA 95596

Lisa M. Zaina  
Stuart Polikoff  
OPASTCO  
21 Dupont Circle, NW  
Suite 700  
Washington, DC 20036

Peter M. Connolly  
Koteen & Naftalin  
1150 Connecticut Avenue, NW  
Washington, DC 20036

Susan W. Smith  
CenturyTel Wireless, Inc.  
3505 Summerhill Road  
No. 4 Summer Place  
Texarkana, TX 75501

James X. Dempsey  
Daniel H. Weitzner  
Center for Democracy and Technology  
1634 Eye Street, NW - Suite 1100  
Washington, DC 20006

Martin L. Stern  
Lisa A. Leventhal  
Preston Gates Ellis & Rouvelas Meeds LLP  
1735 New York Avenue, NW  
Suite 500  
Washington, DC 20006

David L. Sobel  
Electronic Privacy Information Center  
666 Pennsylvania Avenue, SE  
Suite 300  
Washington, DC 20003

Steven Shapiro  
American Civil Liberties Union  
125 Broad Street  
New York, NY 10004

Barry Steinhardt  
Electronic Frontier Foundation  
1550 Bryant Street  
Suite 725  
San Francisco, CA 94103

Kurt A. Wimmer  
Gerard J. Waldron  
Alane C. Weixel  
Covington & Burling  
1201 Pennsylvania Avenue, NW  
P.O. Box 7566  
Washington, DC 20044

Judith St. Ledger-Roty  
Paul G. Madison  
Kelley Drye & Warren, LLP  
1200-19th Street, NW  
Suite 500  
Washington, DC 20036

Joseph R. Assenzo  
Sprint Spectrum LP d/b/a/ Sprint PCS  
4900 Main Street  
12th Floor  
Kansas City, MO 64112

Jill F. Dorsey  
Powertel, Inc.  
1233 O.G. Skinner Drive  
West Point, GA 31833

Frank S. Froncek  
Northern Telecom Inc.  
4001 East Chapel Hill-Nelson Highway  
Research Triangle Park, NC 27709

Stephen L. Goodman  
William F. Maher, Jr.  
Halprin, Temple, Goodman & Sugrue  
1100 New York Avenue, NW  
Suite 650 - East Tower  
Washington, DC 20005

L. Marie Guillory  
Jill Canfield  
National Telephone Cooperative Assn.  
2626 Pennsylvania Avenue, NW  
Washington, DC 20037

Richard J. Metzger  
Emily M. Williams  
Association for Local Telecommunications Services  
888-17th Street, NW  
Suite 900  
Washington, DC 20006

ITS  
1231-20th Street, NW  
Washington, DC 20036