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

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

DECLARATION OF SUPERVISORY SPECIAL AGENT DAVE YARBROUGH

I, Dave Yarbrough, hereby declare as follows:

1. I am a Supervisory Special Agent in the Federal Bureau of Investigation currently assigned to the CALEA Implementation Section. I began serving in this position in October 1994, just after the enactment of the Communications Assistance for Law Enforcement Act (CALEA). I was sworn in as a Special Agent on May 15, 1983. Prior to joining the FBI, I received a Bachelor's degree in Criminal Justice and a Masters in Public Administration, and worked as a police officer in a large city for eight years. Since my appointment, I was assigned to the Charlotte and St. Louis Field Offices, where I investigated property-related crimes. In 1985, I was assigned to the Washington Field Office where I worked on cases involving foreign counterintelligence. In 1990, I received additional training at Quantico, Virginia in technical investigative methods including telephonic surveillance. For four years, I provided assistance in employing electronic surveillance

techniques, particularly telephonic surveillance, in a variety of investigations. My duties included reviewing court orders authorizing surveillance, installing the intercept hardware, and ensuring that the surveillance was terminated in a timely fashion. During my last year in this position, I supervised the deployment of over two hundred telephonic intercepts.

2. The purpose of this declaration is to provide the Commission with information about how electronic surveillance traditionally has been conducted, how changes in telecommunications technology have affected law enforcement's ability to conduct legally authorized electronic surveillance, and how the capabilities included in the government's CALEA "punch list" relate to law enforcement's traditional electronic surveillance capabilities.

3. For many decades, law enforcement agencies have been able to use legally authorized electronic surveillance to collect evidence in criminal investigations. The principal statutory provision authorizing this surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq*. Title III authorizes law enforcement to intercept communications occurring over specified facilities, subject to a court's authorization based on probable cause and other rigorous statutory requirements.

4. Congress's 1986 modifications of Title III, which were designed to update the Act and to clarify federal privacy protections and electronic surveillance standards in light of changes in computer and telecommunications technologies, added a court order requirement for "pen registers" and “trap and trace” devices. Pen registers do not intercept

the contents of calls, but instead record outgoing dialed digits, tones, and any other signals from a subscriber's telecommunications equipment, facilities or services; trap and trace devices provide information concerning the origination of incoming calls.

5. Prior to 1984, the great majority of local and long distance telecommunications were carried by AT&T, which held a virtual monopoly on these services. This dominance resulted in a largely homogeneous telephone network in which the technology of the equipment was generally uniform throughout the network. The telephone system was largely based on "analog" technology, which converted voices into electronic patterns that mimic natural sound waves. The electronic impulses would then travel over copper wires, and were directed to the receiver by electronic contact switches.

6. In this environment, known to engineers as the "POTS" (Plain Old Telephone Service) environment, law enforcement agents could conduct court-authorized electronic surveillance by gaining access to telephone lines between the service provider's central office and a subscriber's home or office (the "local loop"). To carry out pen register and trap-and-trace surveillance in the POTS environment, law enforcement used a device called a Dialed Number Recorder (DNR). When attached to a subscriber's telephone facilities or services, a DNR collects all of the dialing and signaling information that traverses the facilities or service during the course of a call. These devices also print reports that indicate ringing, a busy signal, the beginning time of call placement ("off-hook"), the duration of a call, the concluding time of a call ("on-hook"), and the time a called party answers. In the POTS

environment, Title III surveillance involved the attachment of surveillance equipment to the local loop, which delivered information traversing the loop to law enforcement.

7. Until fairly recently, law enforcement officers using these techniques to conduct court-authorized surveillance have been able, as a technical matter, to intercept the content of all communications traversing a subscriber's local loop. In addition, law enforcement in the POTS environment has been able to collect dialing input and other signaling information relevant to the status of a call by monitoring the local loop. Thus, law enforcement officers in the POTS environment could perform effective surveillance through technologically-straightforward intercepts attached to a subscriber's local loop. Law enforcement officers were able to determine when and to which numbers calls were made from telephone facilities under surveillance, when and from which numbers calls were received by those facilities, and the complete contents of those calls. Moreover, the techniques employed created no technological limitations on the number of court-authorized interceptions that could be conducted, and law enforcement agents could themselves verify the accuracy, integrity, and operability of their intercepts throughout the surveillance period.

8. This situation has changed radically over the past two decades, particularly following the 1984 breakup of AT&T. The number of long distance and local service providers has increased dramatically, and this number has expanded even further with the advent of wireless technologies. Law enforcement agencies now must deal with well over 1,000 different telecommunications service providers employing a host of new technological developments. These developments have become possible in part because analog technology

is being replaced by digital technology, which converts communications into streams of binary data representing the digits "0" and "1." Rather than being routed at the carrier's switching facility by an electrical contact switch, a call handled by the new systems is typically routed by one or more computers. Whereas, historically, the telecommunications facilities for which interception authority was granted were associated with fixed, physical equipment (usually the local loop), the availability of new network capabilities and advanced communications services and features mean that telecommunications need not always be transmitted to the same specific location, or through the same wireline loop. Indeed, sophisticated digital technology generally dissociates a subscriber's communications facilities from particular pieces of physical equipment, because functions that were formerly performed by dedicated hardware are now performed by software that employs whatever network hardware may be available at least cost.

9. The development of these new technologies has made available a range of new services that enable subscribers to manage their telecommunications in ways they could not before. For example, in the past decade or so, the following services have become widely available: call forwarding, call transfer, direct implementation by the subscriber of new services, voice-activated dialing and speed dialing from the service provider's centralized facility, the ability to access voice "mail box" message systems, and the ability to initiate a multi-party call and then depart, leaving the other parties still connected.

10. These new telecommunications technologies allow for the efficient transmission of multiple, simultaneous communications of various subscribers over fiber

optic lines and wire facilities. Features such as call forwarding permit subscribers to redirect calls, meaning that communications will not necessarily be transmitted to the same specific physical location or through the same wire line loop. Likewise, "follow me" features enable subscribers to forward their calls anywhere in the Nation. And personal communications services enable subscribers to define their own portfolio of services, use any fixed or mobile terminal or telephone instrument, and make and receive calls across multiple networks without regard to their location.

11. All of these services have removed a subscriber's communications from a fixed local wire loop that can be intercepted through equipment controlled by law enforcement officers conducting court-authorized surveillance. Thus, whereas in the POTS environment law enforcement officers typically used their own equipment to physically tap into an existing wire leading to a subscriber's house or business, with the advanced services offered by a telecommunications carrier's computers, electronic surveillance often must now be accomplished through the modification of software employed by the carrier to route surveillance information to a designated law enforcement monitoring location. In order for law enforcement to acquire all information identifying the origin, direction, destination, or termination of a call ("call-identifying information") and all call content pursuant to court-authorized surveillance, intercepts in the modern environment must be conducted in the carrier's network by the carrier. Therefore, law enforcement will no longer have direct access to the intercept point.

12. In many respects, the punch list capabilities that law enforcement believes must be added to the industry-developed CALEA standard, J-STD-025 (the "J-Standard"), concern communications and call-identifying information that law enforcement was able to collect in the POTS environment. In other respects, the punch list items would result in the delivery of communications, and/or call-identifying information that law enforcement generally could not collect in the POTS environment, either because law enforcement was technically impeded from accessing the relevant services, or because the services were not available to subscribers. In the following discussion, I will briefly identify the particular information relevant to the punch list item that was or was not available to law enforcement in the POTS environment, explain how law enforcement's ability to access this information has changed in the modern environment, note how this information is treated under the J-Standard, note the punch list's treatment of the information, and briefly explain why the capability set forth in the punch list is important to law enforcement.

A. Conference Call Content

13. In the POTS environment, conference calls were set up by an operator at the request of an individual, and had a simple "hub-and-spoke" structure — *i.e.*, the operator would designate a number which all of the participating individuals would dial to become connected to the call, and each participant would at all times be able to hear all of the input from the other participants. No communications could take place independent of other participants in the conference. If law enforcement was monitoring a particular subscriber's local loop, law enforcement could obtain access to all communications in the conference call,

but only for as long as that subscriber's local loop remained connected to the call. Even in the POTS environment, however, law enforcement could obtain access to all communications in the conference call for the entire duration of the call if it were able to dial into the number used to set up the conference call.

14. Modern telecommunications networks enable the subscriber to initiate a conference call by joining multiple parties in a single call. The subscriber can place one or more parties on hold while simultaneously joining other parties. Additionally, the subscriber can, in many networks, drop off the call while the conference call continues.

15. The J-Standard does not require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with the content of all "legs" of a conference call. For example, it would not require a telecommunications carrier to provide law enforcement with the content of conversations occurring on conference call legs that have been placed on hold.

16. This punch list item would require telecommunications carriers to provide law enforcement conducting court-ordered surveillance with the communications of all parties in a conference call that is initiated and supported by the facility under surveillance. This would include the communications of parties to the conference call who are speaking to each other when the subject places them on hold or a party drops off the call.

17. If law enforcement were to lose the ability to intercept all legs of a conference call, criminals could easily evade court-authorized surveillance by arranging to conduct incriminating conversations on these held call legs. It is not uncommon, for example, for

prisoners to manipulate conference calling services in such a way as to avoid surveillance while conducting criminal enterprises from prison. This is a familiar situation encountered by law enforcement and conference calling is a common feature offered by carriers.

B. Party Join/Hold/Drop Information

18. Acting pursuant to pen register orders, law enforcement in the POTS environment was able to acquire all dialing input and other signaling information relevant to determining the status of a call. This information included tones and signaling information (*e.g.*, the pressing of the flash hook) indicating (1) call waiting, (2) the placing of a party on hold, (3) the initiation of a conference call, or (4) the transfer of a call. By acquiring such dialing and signaling information, law enforcement could identify the final destination of a call, and could in many instances determine who was a party to a call at any given time — information which is often critical in a criminal investigation.

19. In the POTS environment, for example, law enforcement obtained signaling information indicating that an individual had joined other participants in a multi-party call. However, law enforcement could not, as a practical matter, determine which particular participant was placed on hold during, or was dropped from, a multi-party call. Law enforcement could, therefore, identify the range of participants who might be involved in a multi-party call, but could only infer which participants heard particular portions of the call.

20. In the modern telecommunications environment, a subscriber may have services or features that support multi-party calls, such that various associates can be added to, placed on hold during, or dropped from the subscriber's calls. Telecommunications

carriers implementing the J-Standard would not be required to deliver messages identifying these activities to law enforcement during the course of a multi-party call.

21. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with information indicating that an individual has joined, has been placed on hold during, or has been dropped from, a multi-party call.

22. Without this punch list item, law enforcement will find it difficult to determine who is participating in various parts of a call. Law enforcement must collect this information in order to be able to interpret surveillance information for use in investigations and prosecutions. The prison example mentioned earlier is just one situation in which conference calls may be used by criminal co-conspirators to discuss criminal activity. In these cases, if law enforcement is not able to determine, for example, whether the individual who set up the call or any other participant has dropped off during the course of the call, it would not be able to determine with certainty that individual's level of involvement in the criminal activity. This information may be quite significant in a fast moving kidnaping or murder-for-hire scheme.

C. Subject-Initiated Dialing and Signaling Information

23. When executing a court-authorized surveillance, law enforcement in the POTS environment was able to detect the input of dialing or signaling information during the course of a call. For example, law enforcement was able to detect flash hook signaling by detecting recorded changes to the electrical signaling on the analog local loop.

24. Today, a subscriber's service may include features such as call forwarding, three-way calling, or call transfer, and the subscriber may input dialing or signaling information within a call to manage such services. A subscriber may generate this information by pressing a feature key, such as a hold or transfer key, or by pressing the flash hook. For example, an individual who is speaking to one associate may press a transfer key (thereby placing the first associate on hold), call another associate, speak to the second associate, then press the transfer key again and drop off the call, leaving the two associates to continue conversing with each other.

25. The J-Standard does not require telecommunications carriers to alert law enforcement during court-authorized surveillance to the input of dialing and signaling information within a call.

26. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with information indicating that an individual has pressed or dialed certain feature keys to manipulate a call.

27. The inability to know whether an individual has been transferred or has been placed on hold or dropped from a call will impair law enforcement's ability to know who is participating in the call at any particular time, which will interfere with its ability to interpret and use information it collects through court-authorized surveillance.

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

28. When a call attempt is made, the carrier's network generates signaling, including stutter dial tones and other audible tones and signals, that identifies the progress

of the call. In the POTS environment, law enforcement was able to collect this information by monitoring the local loop.

29. Network generated signals in today's telecommunications networks may be either "in-band" (transmitted over the same circuit as the communication) or "out-of-band" (transmitted over a separate circuit), and may be presented to the caller 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 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 light. Collectively, these signals show how the network treated a call attempt: whether it was completed, how it was redirected or modified, and how it ended.

30. The J-Standard does not require telecommunications carriers to provide law enforcement with notification of network-generated in-band and out-of-band signaling related to call progress. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with certain types of network signals that report the progress of outgoing and incoming call attempts.

31. The inability to obtain information relating to this network-generated signaling would significantly interfere with law enforcement's ability to interpret information it collects through court-authorized surveillance. Without this information, law enforcement may misinterpret, or miss altogether, messages sent to a subscriber.

E. Timing Requirements

32. By monitoring the local loop in the POTS environment, law enforcement could collect call-identifying information simultaneously with call content. Law enforcement itself was thus able to correlate this information with the content of an intercepted call.

33. Because law enforcement no longer has direct access to the intercept point, law enforcement must rely upon the carrier to deliver call-identifying information quickly and in a manner that allows it to be correlated with the content of a call. The J-Standard does not require telecommunications carriers to deliver this information to law enforcement within any set period of time after the corresponding communication, nor does it require the affixing of a time-stamp to enable the information to be correlated with the content of an intercepted communication.

34. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with call-identifying information within a specified time after the communication has occurred, and to affix a time-stamp with a set degree of accuracy.

35. The timely delivery of this information together with a time-stamp is crucial to law enforcement's ability to react in time to prevent crimes that it overhears while conducting Title III surveillance. Without the ability to correlate call-identifying information related to a call with the content of the call, law enforcement may be unable to make effective use of electronic surveillance information at trial. In other words, law enforcement may record a conversation at its monitoring location on one channel, during or shortly after

the actual conversation. The J-Standard provides that the data associated with the call will be provided to the law enforcement monitoring location on a separate channel from the call content. If the call-identifying information does not reach law enforcement close to the time of the conversation, law enforcement may not be able to correctly correlate this information with the recorded conversation to which it pertains. This problem will be particularly acute when the subscriber under surveillance makes or receives several calls in rapid succession.

F. Surveillance Integrity—Continuity Tone

36. When law enforcement conducted interceptions in the POTS environment, it could, through the application of a continuous tone to the circuit, promptly discern whether there was any interruption in the delivery of information obtained pursuant to a court-authorized surveillance.

37. Because law enforcement no longer has direct access to the intercept point, it can no longer determine for itself on a continuous basis whether the delivery channel or circuit is operating properly. Consequently, it must rely on the carrier to enable it to detect interruptions in a surveillance effort. Under the J-Standard, telecommunications carriers would not be required to deliver such a tone or take any steps to enable law enforcement to detect interruptions in a timely manner.

38. This punch list item would require telecommunications carriers to provide law enforcement with an automated continuity check, in the form of a continuous tone that will verify that the channels set up to deliver call content subject to a court-authorized interception are in working order.

39. Without this capability, law enforcement cannot know whether a lack of calling activity on an interception reflects the fact that no calls are being made on the facilities under surveillance, or instead results from an interruption in the interception. Consequently, law enforcement would risk missing pertinent communications and related information if a surveillance were to be interrupted.

G. Surveillance Integrity—Surveillance Status Message

40. In the POTS environment, law enforcement was able to acquire sufficient signaling information to know that it was monitoring the correct subscriber. This is because it had physical access to the local loop and could manually confirm whether an interception device was operating and accessing the correct subscriber's equipment, service, or facility.

41. Because law enforcement no longer has direct access to the intercept point, it must rely on the carrier to ensure that the surveillance is continuously functioning properly. Nonetheless, the J-Standard does not require telecommunications carriers to take any affirmative steps to enable law enforcement to confirm that an intercept is working correctly and is accessing the correct subscriber's service.

42. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with an automated message on a regular basis indicating that the interception is working correctly and is accessing the correct subscriber's service.

43. Absent some means of monitoring whether an interception device is accessing the correct equipment, service, or facility, the interception could be overridden inadvertently

or removed by carrier personnel for hours or days without law enforcement's knowledge. This could happen even if a continuity tone were being used, because this tone applies to the status of a call content channel or circuit, while the surveillance status message applies to the operation of the surveillance software in the network. Thus, without surveillance status messages, law enforcement could receive an active circuit without being able to confirm that the surveillance software itself was activated and functioning properly. Law enforcement needs this capability in order to be able to collect all of the information it is authorized by a court order to collect, and to avoid inadvertently collecting information not covered by the court order. Providing this message in an automated fashion would enable law enforcement to quickly correct any deficiency in the implementation of the surveillance.

H. Surveillance Integrity—Feature status message

44. In the POTS environment, law enforcement could collect information regarding a subscriber's portfolio of features, but only by contacting the carrier who would typically provide the information by facsimiles and telephone calls. However, because there were relatively few services or features a subscriber could choose which would affect the number of delivery channels needed for an interception effort, the fact that law enforcement received information on service changes by these relatively inefficient means did not significantly impair law enforcement's surveillance capabilities.

45. In today's digital environment, subscribers may make instantaneous changes in their services and features, many of which require law enforcement to change the provisioning of delivery channels in a court-authorized interception. However, the J-

Standard does not require telecommunications carriers to notify law enforcement of changes in a subscriber's portfolio of features and services.

46. This punch list item would require telecommunications carriers to provide law enforcement conducting court-authorized surveillance with messages alerting law enforcement to changes in a subscriber's features and services.

47. Whenever a subscriber adds or changes features and services, such as call forwarding or features permitting the subscriber to make multi-party calls, law enforcement may have to make corresponding changes in order to ensure that it will receive all communications and call-identifying information that are subject to a surveillance order. For example, without knowing what features are activated at any given time on a subscriber's service, law enforcement cannot know how many interception delivery channels and circuits it needs. Furthermore, if an individual were to cease his service or change his telephone numbers, law enforcement may be unable to obtain continuous surveillance coverage, or could inadvertently begin monitoring communications not authorized to be intercepted.

I. Post Cut-Through Dialing

48. When conducting an interception on the local loop, law enforcement used DNRs to obtain digits dialed by a subscriber by monitoring pulses and tones transmitted over the subscriber's local loop. Consequently, law enforcement was able to collect all of the subscriber's dialing information in the POTS environment.

49. When an individual makes a call, for example, through a long distance carrier or with a credit card, he typically will dial through one carrier's service to another carrier's

service (e.g., an 800 number service). Once he is connected to the second carrier, he will be prompted to continue dialing to reach the party he is calling. The numbers that the caller dials after being connected to the second carrier are referred to as "post cut-through" dialed digits. All of the numbers that the caller dials — including post cut-through — are transmitted over the first carrier's equipment, facilities, or services to reach the called party.

50. Because law enforcement no longer has direct access to the interception point, it will no longer be able to collect this dialing and signaling information without the assistance of the carrier. Whereas the J-Standard does not require telecommunications carriers to provide information about post cut-through dialed digits to law enforcement, this punch list item would require carriers to deliver this information to law enforcement conducting court-authorized surveillance.

51. Law enforcement uses information about the destination or termination of a call to ascertain the identity of the party called and that party's location. Consequently, without access to post cut-though dialed digits, it would be highly unlikely that law enforcement would be able to identify persons whom a target is calling or their location. Once criminals become aware that they can defeat electronic surveillance by first dialing a long-distance service provider or using a prepaid calling card, they will most certainly avail themselves of this technique. As a result, law enforcement's ability to develop evidence of criminal activity through the use of telecommunications surveillance will be rapidly and severely degraded.

J. Delivery Interface

52. Since law enforcement set up and managed its own intercepts in the POTS environment, it depended solely on its own equipment to collect surveillance information. Consequently, the compatibility of the delivery interface was simply not an issue. Because law enforcement must now rely on carriers to conduct electronic surveillance from within their networks, it must be able to interface with the carrier's network to receive surveillance information. A common delivery interface protocol between the carrier and law enforcement is therefore necessary to deliver call content and call-identifying information collected pursuant to court authorization.

53. The J-Standard places no limits upon the number of different interface protocols used by telecommunications carriers. This punch list item limits the total number of interface protocols used by carriers in delivering surveillance information to law enforcement.

54. If carriers are free to employ a large number of different interface protocols, law enforcement agencies, particularly small and medium-sized police departments, could face practical, in some instances insurmountable, financial burdens in conducting network-based electronic surveillance.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on January 27, 1999.

_____

Dave Yarbrough
Supervisory Special Agent
Federal Bureau of Investigation
CALEA Implementation Section