September 29, 2000

The Honorable William E. Kennard
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

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

Dear Chairman Kennard:

The Telecommunications Industry Association ("TIA") respectfully submits the attached *Report on Surveillance of Packet-Mode Technologies* for the Commission's consideration.

In its *Third Report and Order*,[1] the Commission considered the issue of CALEA compliance for packet-mode communications. Although the Commission expressed some concerns with the technical solutions provided by the industry safe harbor standard (J-STD-025),[2] it decided that CALEA solutions consistent with J-STD-025 should be provided by September 30, 2001.

At the same time, however, the Commission noted "that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solutions." The Commission also recognized that "we must avoid implementing CALEA requirements that could impede the development of new technologies" and concluded that "[w]e do not believe that the record sufficiently addresses packet technologies and the problems that they may present for CALEA purposes." As a result, the Commission requested that TIA further study the technical issues concerning the surveillance of packet mode technologies and submit a report to the Commission by September 30, 2000.

---

[1] In the Matter of Communications Assistance for Law Enforcement Act, *Third Report and Order*, CC Docket No. 97-213, FCC 99-230, ¶ 55 (rel. August 31, 1999) ("Third Report & Order").

[2] Telecommunications Industry Association & Alliance for Telecommunications Industry Solutions, Interim Standard, *Lawfully Authorized Electronic Surveillance*, J-STD-025 (December 1997).

As mentioned in TIA's previous status reports to the Commission,[3] TIA immediately formed a working group, drawing on the technical expertise of its various standards committees, to provide technical input to this study. In order to expand the technical expertise contributing to the packet data study, TIA also invited a broad variety of packet-oriented technical groups to participate in a series of Joint Experts Meetings ("JEM"). The first session of the JEM was held on May 3-5, 2000 in Las Vegas, Nevada. The second session was held in Washington, D.C. from June 27-29.

TIA appreciates the hard work and contributions made by all of the companies and organizations that participated in the JEM process. Both sessions of the JEM were well attended and sparked lively discussion. Participants included not only a broad spectrum of the industry, but also representatives from the Federal Bureau of Investigation and the Center for Democracy and Technology. TIA was especially pleased that representatives of the Commission's staff were able to participate in both meetings. A list of attendees from the two sessions is attached.

Without attempting to summarize the entire *Report*, TIA would like to draw the Commission's attention to a few, critical issues raised during the Joint Experts Meetings.

- **Packet-Mode Services Are Extremely Varied and Diverse.** As the Commission properly noted in its *Third Report and Order*, "packet technologies are rapidly changing and different technologies may require differing CALEA solutions for separating call-identifying information from call content." The JEM's experience fully validates the Commission's statement. Although a large group of experts in a wide variety of different packet data technologies participated in the discussions, the JEM was able to evaluate only a fraction of the technologies currently being used or developed. The JEM also noted that packet data protocols vary significantly and that any one packet data standard is unlikely to work for all protocols – unless some "one-size-fits-all" approach (such as that identified in J-STD-025) is adopted. As a result, it may be appropriate for the Commission to encourage separate standards for each, individual packet technology (for example, PacketCable's standard for packetized cable telephony).

- **The Uncertain Legal Framework Complicates Development Efforts.** TIA viewed its mandate from the Commission to be fairly narrow – to discuss the technical issues raised by the Commission and not to address legal questions such as what constitutes "call-identifying information" for a packet-mode service or whether a particular packet-mode technology is a "communications service" or "information service" for purposes of CALEA. TIA considered those questions to be outside of the scope of the Commission's

[3] Telecommunications Industry Association, *Status Report*, CC Docket No. 97-213 (filed on December 23, 1999); Telecommunications Industry Association, *Second Status Report*, CC Docket No. 97-213 (filed on May 17, 1999).

request. Nevertheless, the JEM discussion repeatedly demonstrated that technical analysis of what was feasible or infeasible depended on such legal issues. The JEM participants were frequently frustrated by the fact that there was no clear, legal framework (either in the statute or from the Commission's decisions) in which to base their evaluations. For example, it is ambiguous how the term "call-identifying information" applies (if at all) to packet data. Without clearer guidance of what constitutes "call-identifying information" for packet data, industry cannot accurately report on the technical impact and feasibility of making such information available to law enforcement. Similarly, just because a specific packet mode technology is discussed in the *Report* does not mean that the JEM viewed the technology as being a communications services for purposes of CALEA.

- **Technical Difficulty of Analyzing Packet Data Traffic.** Because of the inherent flexibility of packet-mode technologies, these technologies are used to transport a theoretically unlimited number of different services, applications and protocols. New protocols are being introduced almost daily. It is not technically feasible to determine, on a packet by packet basis, the application or service that is being provided in a particular packet stream. Encapsulation (i.e., wrapping packets within packets) and encryption of packets renders identification of the type of service being conveyed (e.g., communication vs. information) even more difficult, if not possible. As a result, it would be a significant burden to try to analyze packets in a real-time basis to extract the kind of information that law enforcement might wish to obtain. (For example, the information could be buried within several layers of encapsulated packets, within a protocol with which the carrier transporting the packet has no familiarity).

- **Call-Management Servers vs. Sessions Without Call-Management Servers.** This identification and analysis problem may be less severe with technologies that have call set-up and tear-down capabilities – i.e., technologies that include a Call Management Server ("CMS"). As the JEM noted, the point where a CMS sets up a communication may be the only time that a packet-mode communication service can be distinguished from an information service and that call-identification-like information might be identified. Again, however, what might be feasible will vary widely from CMS-technology to CMS-technology. For transport services without a CMS, it is extremely burdensome to segregate individual packets out of the stream of packets being conveyed by the transport carrier and extract the kind of information law enforcement is requesting. In those transport technologies, where the whole packet stream must be examined in order to gather relevant call-identification-like information, the process of filtering may overload the network's processing capacity or severely degrade network performance.

- **FBI's Carnivore Presentation.** During the JEM's second session, the FBI gave a presentation on its existing packet-data surveillance device (nicknamed "Carnivore"). The "Carnivore" presentation from the FBI was extremely enlightening. First, it verified the "gut feel" of the JEM's technical experts that development of a filter protocol like

Carnivore is extremely resource intensive and fluid because of the ever changing nature of packet protocols and the constant introduction of new protocols. As the FBI acknowledged, requiring carriers and equipment vendors to develop similar filtering technology would be extremely expensive and burdensome. Second, at least as explained by the FBI, the Carnivore device would allow law enforcement to conduct the kind of filtering envisioned by J-STD-025, thus raising the question whether it would be cost-effective (or even privacy-protective) to require carriers to develop their own, separate capabilities.

- **Most Cost-Efficient and Technically-Feasible Solution.** The consensus among the JEM participants was that (for the reasons discussed above and in more detail in the *Report*) providing the entire packet stream for a particular subscriber is by far the most cost-effective and technically feasible method for providing access to law enforcement. Of course, in order to address privacy concerns, law enforcement must obtain the appropriate legal authorization to receive this packet stream (such as a Title III order) and strict legal procedures should be adopted to assure compliance with the limits on that authorization. To require carriers to develop a filtering program would be extremely burdensome and expensive (requiring continuous updates and modifications) – especially for non-CMS packet services. For some CMS services, it might be possible to separate call-identification-like information from content – but what would be feasible will vary from technology to technology and would require individual standards.

In conclusion, TIA would encourage the Commission to establish a procedure by which CALEA solutions for packet data technologies could be implemented in a more efficient and rational method. As TIA noted in its recent comments in this docket,[4] the Commission should immediately suspend the September 30, 2001 compliance deadline pending the completion of any proceedings the Commission may initiate after evaluating this *Report*. Manufacturers and carriers are unsure whether to continue expending considerable resources developing complicated and expensive solutions consistent with the J-STD-025, if it is possible that those solutions may prove to be only an "interim" or "temporary remedy." By suspending the deadline, the Commission will enable itself to solicit comments on the *Report* and make a final, informed decision.

TIA appreciates the confidence expressed by the Commission in entrusting to TIA the responsibility for preparing this *Report*. If you have any questions about the *Report*, please do not hesitate to contact me.

---

[4] Telecommunications Industry Association, *Comments*, CC Docket No. 97-213 (filed September 15, 2000).

Pursuant to 47 C.F.R. § 1.1206, copies of the *Report* will be filed with the Commission's Secretary. TIA is also providing copies of this *Report* to several of the Commission staff involved in this proceeding.

Sincerely,

/s/

Matthew J. Flanigan
President
Grant Seiffert
Vice President, Government Relations

cc (w/encl.): The Honorable Harold Furchtgott-Roth
The Honorable Susan Ness
The Honorable Michael Powell
The Honorable Gloria Tristani