U.S. Department of Justice

Federal Bureau of Investigation

EX PARTE OR LATE FILED

CALEA Implementation Section
Suite 300
14800 Conference Center Drive
Chantilly, VA 20151

EX PARTE SUBMISSION

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, N.W.- Room 222
Washington, D.C. 20554

Re: **Written Ex Parte Submission**
In the Matter Of: Jurisdictional Separations Reform and Referral to the Federal-State Joint Board, CC Docket No. 80-286: In the Matter Of: Communications Assistance for Law Enforcement Act, CC Docket No. 97-213

Dear Ms. Salas:

During the week of July 27, 1998, Supervisory Special Agent David Yarbrough and Program Analyst Michael Gallagher of the Federal Bureau of Investigations (FBI), attended the National Association of Regulatory Commissions (NARUC) summer conference. While attending the NARUC summer conference, the FBI met with the following individuals regarding CALEA related matters: Honorable David W. Rolka (Pennsylvania Public Utility Commission), Honorable Joan H. Smith (Oregon Public Utility Commission), Honorable Thomas L. Welch (Maine Public Utilities Commission)Cynthia Van Landuyt (Oregon Public Utility Commission), Joel B. Shifman (Maine Public Utilities Commission), Samuel Loudenslager (Arkansas Public Service Commission), Scott Potter (Public Utilities Commission of Ohio), and James Bradford Ramsey (NARUC). The FBI also met with the following FCC staff members: Kathryn Brown, Kenneth Moran, Kaylene Shannon, and James Schlichting.

The purpose of the meetings was to provide members and staff of the Joint Board with an oral and written status briefing on issues related to the implementation of the Communications Assistance for Law Enforcement Act. The FBI upon its earliest possible convenience is providing this Ex Parte letter and written presentation, pursuant to § 1.1206 of the Commission's Rules, 47 C.F.R. § 1.1206. Enclosed please find an original and two copies of the Federal Bureau of Investigation's written presentation. Copies of the written presentation have already been provided to all individuals met by the FBI.

Sincerely,

David Yarbrough
Supervisory Special Agent
Federal Bureau of Investigations

U.S. DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

For Policy Information:
Digital Telephony & Encryption Policy Unit
Office of Public & Congressional Affairs
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535
(202) 324-5355

For Technical Information:
CALEA Implementation Section
Suite #300
14800 Conference Center Drive
Chantilly, Virginia 20151
(703) 814-4700

June 1998

CALEA

TALKING POINTS

The Nation's telecommunications systems and networks are often used in the furtherance of serious, and sometimes violent criminal activities that include terrorism, kidnappings, extortion, organized crime, drug trafficking and corruption.

One of law enforcement's most important and effective tools in the investigation of these crimes by federal, state and local law enforcement agencies is court-authorized electronic surveillance or "wiretaps", pen registers and trap and traces.

In 1968, Congress carefully considered and passed the Omnibus Crime Control and Safe Streets Act which laid out a meticulous procedure by which law enforcement can obtain judicial authorization to conduct electronic surveillance in the fight against crime. This law was enacted after Congress exhaustively debated law enforcement's need to effectively address serious criminal activity and an individual's right to privacy.

Forty-four states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted similar legislation authorizing their state and local law enforcement agencies to conduct court-authorized electronic surveillance in the investigation of serious criminal activity. Approximately fifty-two percent of the court-authorized criminal wiretaps conducted in 1997, were conducted by state and local law enforcement.

The use of court-authorized electronic surveillance has proven invaluable in the prevention of criminal acts and successful resolution in numerous criminal investigations. During the past 16 years, evidence obtained from court-authorized electronic surveillances has been responsible for the conviction of more than 26,000 dangerous felons.

The evidence and information obtained through court-authorized electronic surveillance generally can not be obtained through any other methods or investigative techniques. Further, the law only allows the use of court-authorized wiretaps when other investigative techniques have either proven unsuccessful, or are too dangerous to employ.

In 1970, Congress amended the federal wiretap statute to require providers of communications services (telephone companies) to provide law enforcement with the ". . . technical assistance necessary to accomplish the intercept . . ." In the old telecommunications environment, only minor assistance from telephone companies was needed by law enforcement to accomplish the interception (e.g., identity of "access points," etc.). Much greater assistance is now necessary because of their use of new and advanced telecommunications technologies, services and features.

Recent and continuing advances in telecommunications technology along with the introduction of new technologies, transmission modes, and new services and features, have impaired, and in some instances, prevented the telephone companies from assisting law enforcement in the full implementation of electronic surveillance court orders.

These new technological developments are not intentionally being introduced to prevent court-authorized electronic surveillance or thwart law enforcement's ability to effectively enforce criminal laws and protect the public safety. However, these new telecommunications systems are preventing the telephone companies from providing law enforcement with access to all conversations and call-identifying information emanating from or directed to the telephone instrument that is the subject of the court-authorized electronic surveillance, to the exclusion of all others.

In October 1994, Congress took action to protect public safety and national security by enacting the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414. The law is intended to clarify and further define the existing statutory obligation of telephone companies to assist law enforcement in executing electronic surveillance court orders.

CALEA does not change or expand law enforcement's fundamental statutory authority to conduct various types of electronic surveillance. It simply seeks to ensure that after law enforcement obtains the appropriate legal authority, telecommunications carriers will have the necessary technical capability and sufficient capacity to fulfill their statutory obligations to assist law enforcement. In many instances, telecommunications carriers do not have either the capability and capacity to handle all electronic surveillance court orders.

CALEA sets forth, in law, the assistance capability requirements that telecommunications carriers need to meet and maintain within their networks to assist law enforcement in conducting court-authorized electronic surveillance. Specifically, CALEA directs the telecommunications industry to design, develop and deploy solutions that meet the Section 103 assistance capability requirements.

Telecommunications carriers with equipment, facilities, or services installed or deployed after January 1, 1995, must be capable of meeting the assistance capability requirements by October 25, 1998, four years after the law's enactment, at the expense of the carriers. Telecommunications carriers with equipment, facilities or services installed or deployed on or before January 1, 1995, must also meet the assistance capability requirements by October 25, 1998, if they have received government reimbursement for those direct costs associated with compliance.

Under Section 107 of CALEA, the telecommunications industry is encouraged to use existing telecommunications standards setting bodies to develop technical requirements or standards to meet the assistance capability requirements of Section 103. However, the absence of standards or technical requirements (or a standard that is deemed to be deficient) does not relieve them of their responsibility to meet section 103.

Section 104 of CALEA requires the Attorney General to identify the number of simultaneous interceptions, or capacity requirements, that telecommunications carriers will be obligated to support in specific geographic areas. To meet this directive, the FBI conducted an unprecedented survey of past electronic surveillance activity nationwide to establish a historical baseline from which future interception needs could be projected.

The FBI has identified law enforcement's future interception needs in a Final Notice of Capacity which was published on March 12, 1998. Telecommunications carriers are required to inform the FBI by September 8, 1998, if they cannot meet the capacity requirements as they are stated in the Final Notice. Thereafter, carriers are required to comply with the capacity requirements within three years of the Notice's publication, that is by March 12, 2001.

The Federal Communications Commission (FCC) serves a very important role with regard to CALEA implementation. FCC responsibilities include establishing, by rule, technical requirements for CALEA Section 103 assistance capability requirements if a party petitions an industry standard as deficient. In addition, the FCC is also responsible for establishing regulations concerning telecommunications system security and integrity. Pursuant to Section 105 of CALEA, the FCC is developing rules that will direct telecommunications carriers to adopt procedures regarding the administration of electronic surveillance.

Section 109 of CALEA authorizes the Attorney General to establish rules and procedures for providing reimbursement to telecommunications carriers for the direct costs associated with CALEA compliance. These reimbursements will be subject to the Final Cost Recovery Rules that became effective on April 21, 1997.

Under Section 110 of CALEA, Congress authorized up to $500 million to be appropriated for this reimbursement effort. The Omnibus Consolidated Appropriations Act of 1997 established the Telecommunications Carrier Compliance Fund (TCCF) for the purpose of making these reimbursements. Thus far, the Congress has appropriated approximately $102.5 million of the authorized $500 million.

Recent Developments

Standards Issue:

On December 5, 1997, the telecommunications industry adopted, over the objections of the law enforcement community, an interim standard to meet the Section 103 assistance capability requirements. Law enforcement believes that the industry's interim standard does not go far enough to protect the public and national security.

The Department of Justice (DOJ) issued an opinion on January 23, 1998, finding that the industry interim standard lacks nine capabilities required by CALEA and the underlying electronic surveillance statutes which are necessary to meet certain evidentiary and minimization

requirements dictated by law. Without these capabilities, law enforcement will not be able to ensure the integrity of future intercept efforts.

The Center for Democracy and Technology (CDT), an organization representing privacy interests, filed a Petition of Deficiency with the Federal Communications Commission (FCC) on March 26, 1998. CDT's petition claims that the industry's interim standard is deficient in that it exceeds the intercept capabilities permitted by CALEA and fails to protect personal privacy.

On March 27, 1998, the DOJ and the FBI also filed a Petition of Deficiency with the FCC. The DOJ/FBI petition argues that the industry's interim standard is deficient in that it fails to include nine capabilities determined by DOJ as necessary to meet certain evidentiary and minimization requirements dictated by law.

On March 30, 1998, AT&T Wireless, Lucent Technologies, and Ericsson petitioned the FCC for an extension of CALEA's October 25, 1998 compliance date. According to the companies, the absence of a "stable standard ensures delay in the delivery of CALEA-compliant technology and underscores the need for the extension of the compliant date." The companies have asked that the date be extended to October 1, 2000.

On April 2, 1998, the Telecommunications Industry Association (TIA) filed a Petition for Rulemaking, asking the FCC to resolve the standards issue. TIA requested the FCC to determine whether the industry standard is over inclusive or under inclusive and to provide guidance to telecommunications equipment manufacturers.

On April 9, 1998, the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), and the United States Telephone Association (USTA) asked the FCC to resolve the disagreement existing between law enforcement and the telecommunications industry regarding the industry's interim standard. Specifically, the associations asked the FCC to: (1) recommend that the standard go through the industry's standard-setting process; (2) set a new CALEA compliance date once the standard is complete; (3) clarify that adopting the standard is voluntary on the part of carriers; and (4) rule that compliance is not reasonably achievable for equipment installed after January 1, 1995.

As part of the FCC petition process, the FBI and DOJ have jointly filed comments and reply comments regarding an extension to the October 1998 compliance deadline and the standard. The most recent filing occurred on June 13, 1998. In this reply comment, the FBI/DOJ asserted that each of the capabilities included in its petition of deficiency fall under the requirements of Section 103 of CALEA. The FBI and DOJ specifically addressed why each of the "punch list" items should be included in any future standard developed by the FCC. These reply comments also addressed concerns voiced by the industry and privacy groups over location information and packet switching.

The DOJ and the FBI have asked the FCC to rule on the standard in an expedited manner, requesting that the matter be resolved by September, 28, 1998.

Legal Issues:

CTIA and PCIA filed a joint lawsuit on April 28, 1998 in the U.S. District Court challenging the FBI's definition of "installed or deployed" as it applies to the January 1, 1995 cut-off date for reimbursements to the industry for CALEA compliance.

Legislative Issues:

There has been significant activity in this session of Congress that may possibly result in changes to CALEA. In response to continuing disagreement over implementation issues, the telecommunications industry, led by the CTIA and PCIA, has stepped up efforts to lobby Congress to change the law.

On March 4, 1998, Representative Barr (R-GA) introduced H.R. 3321. The Barr measure, in its current form, would drastically alter CALEA. Representative Barr's pending legislation would expand the reimbursement pool of eligible equipment, facilities and services by changing the January 1, 1995 cut-off date to October 1, 2000, and by defining "deployed" as "available anywhere in the telecommunications industry." The legislation would also extend reimbursement eligibility indefinitely for some equipment, facilities and services by defining the term "significantly upgraded or otherwise undergoes major modification" so narrowly that many carriers might not perform a modification that qualifies for years to come. With regard to CALEA's assistance capability requirements, the measure establishes that compliance will not be "reasonably achievable" until 24 months following the adoption of a publicly available standard. In addition, the October 25, 1998 capability compliance date would be extended to October 1, 2000.

On April 29, 1998, Representative Zoe Lofgren (R-CA) offered an amendment to change CALEA to the House Judiciary Committee. The amendment, very similar in language to Representative Barr's legislation, was withdrawn following dialogue with Representative Bill McCollum (R-FL), Chair of the House Judiciary Committee's Subcommittee on Crime. According to reports, the dialogue led to the committee agreeing that they needed to do more than change CALEA dates. The committee agreed to a "comprehensive reform of CALEA." Representative McCollum is to direct the committee effort in this regard.

On June 22, 1998, the House of Representatives suspended the rules and passed the DOJ Authorization Act for FY 1999 through 2001 (H.R. 3303). Included in the bill was a provision amending CALEA's capability compliance date (from October 25, 1998 to October 1, 2000) and the date governing a carriers' eligibility for government reimbursement (from January 1, 1995 to October 1, 2000). The changing of these dates, should they be enacted into law, would have significant negative public safety and national security ramifications. An extension to the October 25, 1998 compliance deadline will prolong the existence of technological impediments to law enforcement's electronic surveillance abilities. Moreover, an extension to the January 1, 1995 date will increase the reimbursement eligibility pool and thus, grand fathered status of non-compliant telecommunications services and features.

CALEA

QUESTIONS & ANSWERS

What is the Communications Assistance for Law Enforcement Act (CALEA)?

The Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, was signed into law by President Clinton on October 25, 1994. It's purpose is to clarify the extent to which telecommunications carriers must provide technical assistance to law enforcement in the conduct of lawfully authorized electronic surveillance.

Why was CALEA necessary?

Rapid changes and advances in telecommunications technologies (such as call forwarding and voice activated speed dialing) began to compromise law enforcement's ability to conduct electronic surveillance. In response, Congress enacted CALEA to preserve electronic surveillance as an important investigative tool so that law enforcement could continue to protect the public from some of our nation's most serious and violent offenders.

Does CALEA expand law enforcement's electronic surveillance powers?

No. CALEA does not change or expand law enforcement's fundamental statutory authority to conduct various types of electronic surveillance. CALEA simply seeks to ensure that after law enforcement obtains the appropriate legal authority to conduct electronic surveillance, telecommunications carriers will have the necessary technical capability and sufficient capacity to fulfill their legal obligation to accommodate law enforcement's requests for assistance.

What is the FBI's role in CALEA implementation?

Under the law, the Attorney General has been designated with certain CALEA implementation responsibilities. The Attorney General delegated these responsibilities to the Federal Bureau of Investigation (FBI). The FBI established the CALEA Implementation Section (CIS) to further implementation on behalf of federal, state, and local law enforcement.

Does CALEA apply to every type of telecommunications carrier?

CALEA applies to all telecommunications carriers as defined in Section 102 (8) of the statue. Such telecommunications carriers include a "person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."

When are telecommunications carriers required to comply with CALEA?

Telecommunications carriers must meet CALEA's Section 103 assistance capability requirements by October 25, 1998. Pursuant to Section 104 of CALEA, telecommunications carriers are also required to meet law enforcement's capacity requirements three years after the publication of the Final Notice of Capacity, that is by March 12, 2001.

Why did the Department of Justice and the FBI petition the industry's interim standard at the Federal Communications Commission?

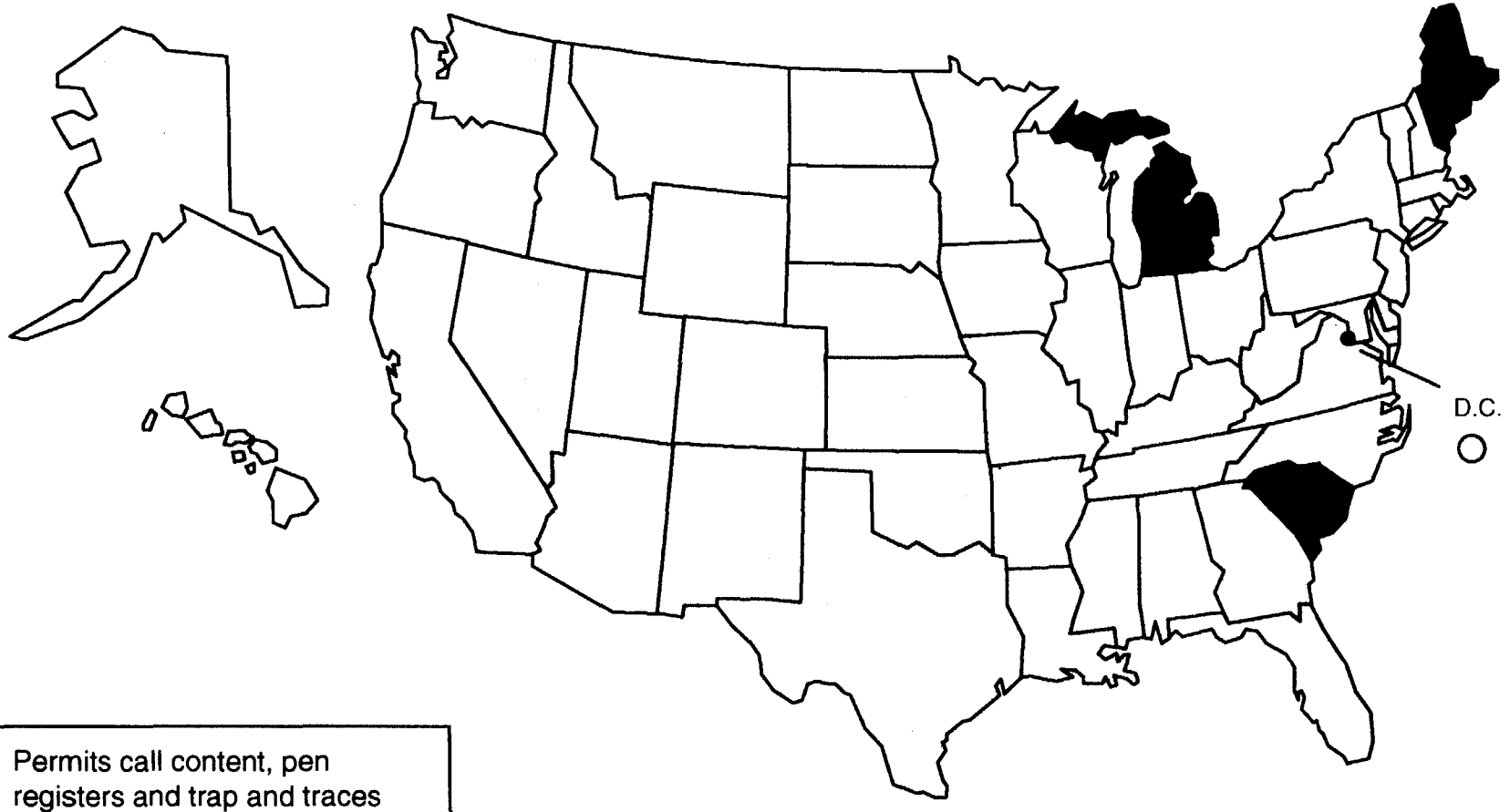
Having reached a consensus among the law enforcement community, on March 27, 1998, the Department of Justice (DOJ) and the FBI filed a Petition of Deficiency before the Federal Communications Commission (FCC) regarding the telecommunications industry's interim standard. The decision to petition followed a detailed legal review of the industry's interim standard by DOJ. The interim standard was found to be deficient because it lacked nine capabilities required by CALEA and underlying electronic surveillance statutes that are necessary to meet certain evidentiary and minimization requirements dictated by law. Without these capabilities, law enforcement will not be able to ensure the integrity of future intercept efforts.

Is statutory change to CALEA necessary?

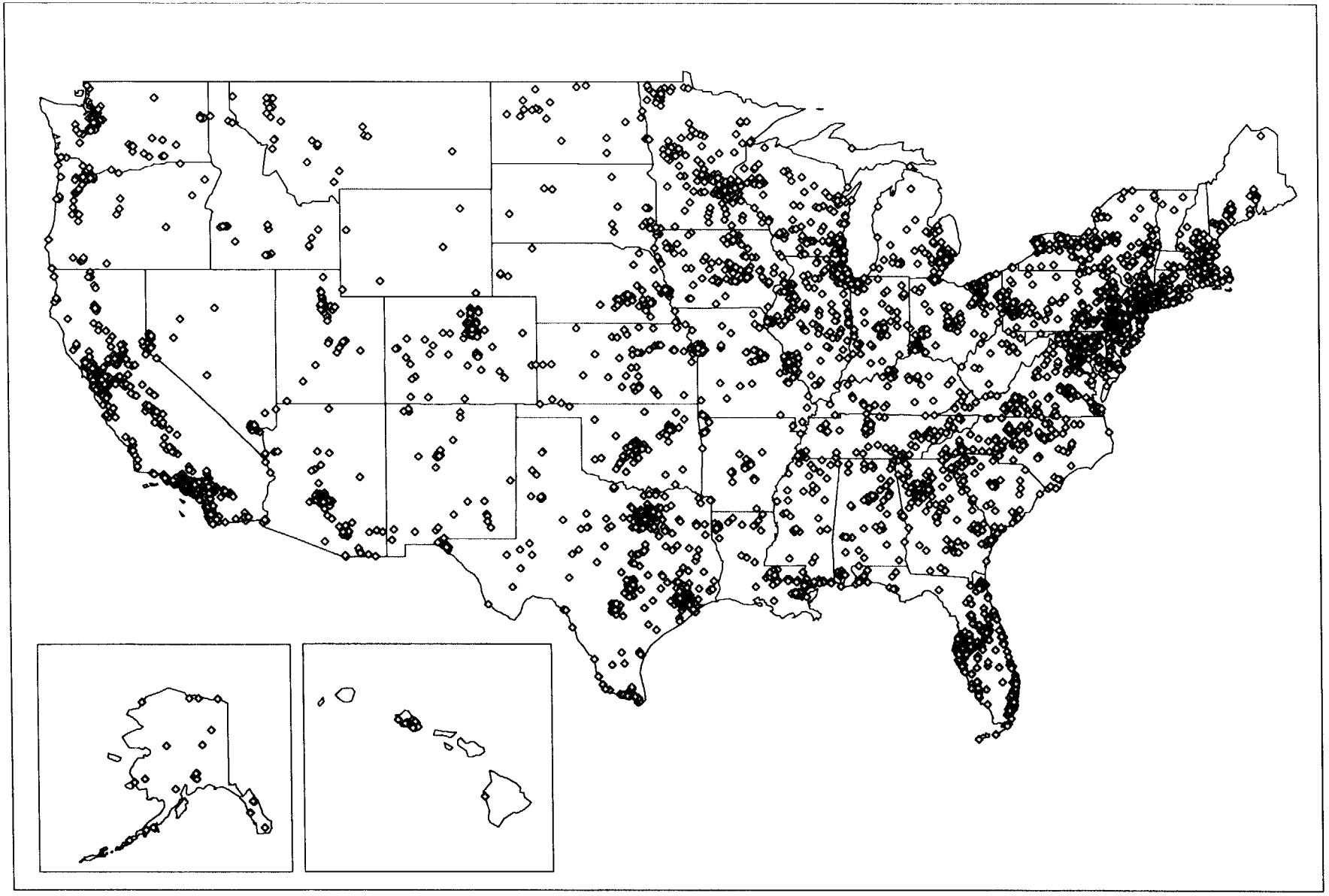
Law enforcement does not believe that it is necessary for Congress to revisit CALEA and change the law. The existing statute provides ample recourse for industry to resolve its concerns over compliance dates, the standard, and cost. CALEA allows a carrier to petition the FCC for an extension of the October 25, 1998 compliance date if that carrier believes compliance by this date is not reasonably achievable through the application of technology available within the compliance period. The law also permits any party believing a telecommunications industry's standard to be deficient to petition the FCC to establish technical requirements. Several parties to date have petitioned the FCC to resolve the standards issue and the FCC is expected to rule on the standard by September 28, 1998. In addition, CALEA allows carriers believing that compliance will provide an undue financial burden to petition the FCC that compliance is not reasonably

achievable. As illustrated, statutory change is unnecessary. Statutory change will only raise the costs of CALEA to taxpayers and prolong the threat to public safety by delaying compliance with this very important law.

LOCAL LAW ENFORCEMENT JURISDICTIONS THAT AUTHORIZE ELECTRONIC SURVEILLANCE AS OF JULY 1, 1998



Legend:

- Permits call content, pen registers and trap and traces
- Only permits pen registers and trap and traces
- Prohibits electronic surveillance

SWITCHES WITH INTERCEPT ACTIVITY
JANUARY 1, 1993 - MARCH 1, 1995