THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT*

EXECUTIVE SUMMARY

Criminal organizations and individuals frequently use the telecommunications systems of the United States to further serious violent crimes, including terrorism, kidnapping, extortion, organized crime, drug trafficking, and public corruption. One of the most effective tools law enforcement uses to investigate these crimes is court-authorized electronic surveillance. However, continuing advances in telecommunications technology have impaired and in some instances prevented telecommunications carriers from assisting law enforcement in conducting court-authorized electronic surveillance.

In the early 1990s, the Federal Bureau of Investigation (FBI) asked Congress for legislation to assist law enforcement agencies to conduct electronic surveillance. The FBI argued that advances in the telecommunications industry such as cellular telephones, call forwarding, and speed dialing challenged the ability of law enforcement agencies to fully perform electronic surveillance. In response, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994 to enable law enforcement to conduct electronic surveillance despite the deployment of new technologies and wireless services that have altered the character of electronic surveillance. In short, CALEA requires telecommunications carriers (carriers) to modify the design of their equipment, facilities, and services to ensure that law enforcement can perform electronic surveillance (for purposes of this report, the term electronic surveillance is used only in the sense of the real-time interception of information). To facilitate CALEA implementation, Congress appropriated $500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995.

*** THE FULL VERSION OF THIS REPORT INCLUDED INFORMATION THAT THE FBI CONSIDERED TO BE LAW ENFORCEMENT SENSITIVE. TO CREATE THIS PUBLIC VERSION OF THE REPORT, THE OIG REDACTED (DELETED) THE SENSITIVE PORTIONS AND NOTED THAT THE INFORMATION DELETED IS LAW ENFORCEMENT SENSITIVE.**

Effective implementation of CALEA relies heavily on the shared responsibilities of the FBI, the Federal Communications Commission (FCC), telecommunications carriers, and telecommunications equipment manufacturers. CALEA also required the Department of Justice (DOJ) Office of the Inspector General (OIG) to conduct biennial audits of the progress of CALEA implementation.[1]

Audit Approach

The OIG initiated this audit to: (1) review CALEA implementation costs and progress; (2) review the impediments to CALEA implementation, including the effects of emerging technologies; and (3) determine how the implementation of CALEA, or lack thereof, impacts federal, state, and local law enforcement in its ability to conduct electronic surveillance.

As part of our audit, we interviewed officials within the FBI and the DOJ who have CALEA implementation responsibilities, as well as representatives from telecommunications service providers, the FCC, advocacy groups, and federal, state, and local law enforcement. We reviewed the FBI's 2004 Threat Assessment Report, the *FBI Investigative Technology Division CALEA Law Enforcement Case Examples,* and other documents to gain an understanding of issues encountered by law enforcement while conducting electronic surveillance. We also mailed a survey to a statistical sample of 1,396 federal, state, and local law enforcement officials to identify issues that affect law enforcement's ability to conduct electronic surveillance. Appendix I contains more information about the objectives, scope, and methodology of this audit.

CALEA Implementation Costs and Progress

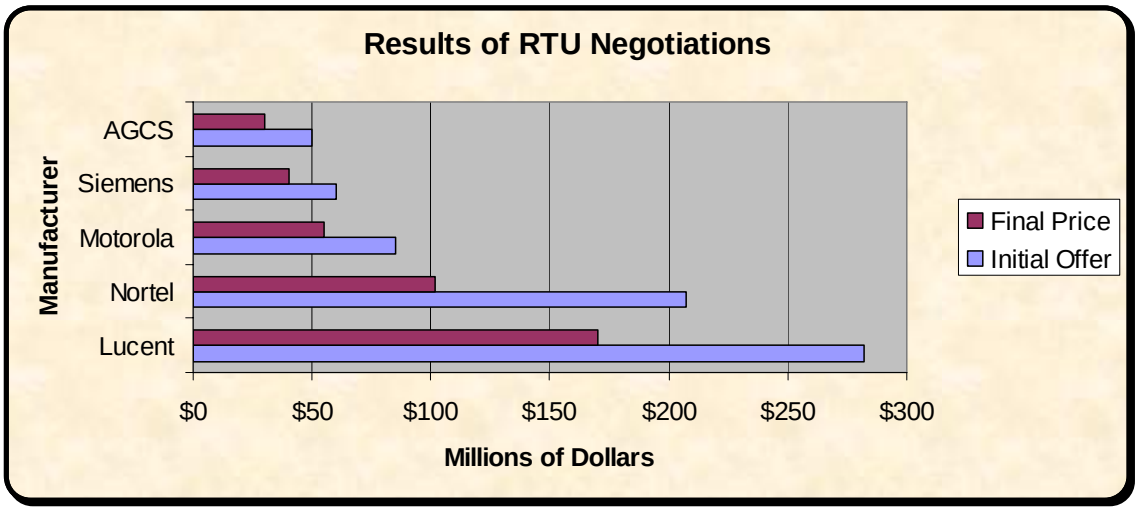
After 10 years and over $450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant.[2] Although we acknowledge that the FBI bases its estimates on the best available data, we could not provide assurance on the accuracy of these estimates. Neither the FBI nor the FCC know the actual rate of CALEA compliance because there is no

[1] See Appendix V for a summary of the prior OIG audits.

[2] A switch is a telephone company device which "makes the connection" when a call is placed. Modern switches are specialized computers.

requirement for carriers to report the number of switches that are compliant. During the past 10 years, the FBI has spent about $400 million to reimburse manufacturers for their purchase of CALEA-compliant software licenses (Right-to-Use or RTU licenses). These software licensing agreements allowed the carriers to meet CALEA intercept requirements by collecting and delivering to law enforcement pertinent call-identifying information, call content, or both.

Through extensive negotiations, the FBI negotiated substantially reduced costs for the RTU licenses compared to the initial cost proposals as shown in the following chart.



Source: *Determination and Findings Regarding the Implementation of the Communications Assistance for Law Enforcement Act (1999)*

The FBI also entered into additional RTU license agreements totaling $50 million to reimburse carriers for the purchase of RTU Enhanced Dial-Out software licenses. The "dial-out" software takes advantage of the Public Switched Telephone Network (PSTN) already in place between carrier equipment performing an intercept and a law enforcement collection site.[3]

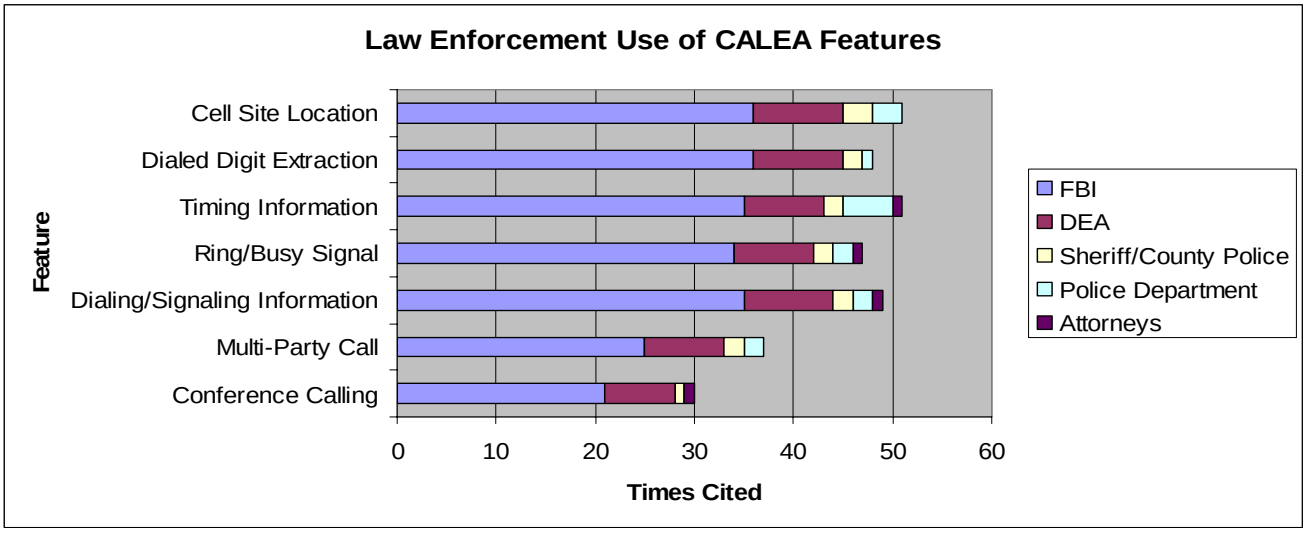
Although the FBI was able to negotiate substantially reduced costs for the RTU license agreements compared to the carriers' initial cost proposals, as reported in previous OIG audits, the cost information given to us by the FBI did not provide a basis to determine the reasonableness of the RTU licenses' costs. Accordingly, our prior

[3] The PSTN refers to the publicly available dial-up telephone network. It is an interconnection of switching centers and connections to customers that offers voice dial-up between customers connected to the PSTN.

reports offered no opinion.

Benefits of CALEA

For the switches with activated CALEA software, we found that CALEA has provided federal, state, and local law enforcement with beneficial features to conduct electronic surveillance.[4] The law enforcement officials we interviewed said that electronic surveillance is a vital investigative tool and that the CALEA features are extremely beneficial. In addition, of the 82 agencies that responded to our survey stating that they performed electronic surveillance, the following chart shows a breakdown of law enforcement's use of the CALEA features:



Source: Law enforcement responses to the OIG survey

Law enforcement officials also stated that CALEA has greatly reduced the amount of time it takes carriers to initiate a wiretap. Prior to CALEA, both the carrier and law enforcement had to be physically present at the switch location during the electronic surveillance. With CALEA, provisioning, or the providing of electronic surveillance service by the carrier, is completed remotely from a central location for all electronic surveillance in a carrier's network. According to carrier and law enforcement officials, this process has significantly reduced carrier and law enforcement travel costs and time.

[4] A list of these features, known as "punchlist" items, is described in Appendix IX.

Impediments to Implementing CALEA

Despite these successes, the FBI has encountered significant impediments in implementing CALEA. These impediments included the contentious standard-development process, carrier requests for extensions and enforcement orders for non-compliance, and the extended negotiations with carriers over software activation agreements.

Developing Technical Standards

Electronic surveillance standards provide the basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance. In accordance with CALEA, the FBI consults with telecommunication carriers and manufacturers to determine what capabilities will be included in the CALEA standards. Developing electronic surveillance standards is a lengthy process. For example, the initial CALEA standards took 10 years to develop and implement because of protracted litigation over law enforcement wiretapping requirements. These delays are the primary reason CALEA implementation continues on wireline systems.

CALEA gives the lead role in setting electronic surveillance standards to the telecommunications industry and this delegation has created considerable tension between the FBI and the telecommunications industry throughout the standards development process. According to the FBI, CALEA allows the telecommunications industry to decide what law enforcement needs to accomplish effective electronic surveillance. If the FBI believes a standard is deficient, it must challenge the standard by filing a deficiency petition with the FCC. Instead of having to explain why law enforcement needs a particular feature or service, the FBI's preference would be to place the onus on the telecommunications industry to explain why a feature or service law enforcement wants is not technically feasible.

Carrier Extensions and Enforcement Orders for Non-Compliance

Under CALEA, the FCC has the power to grant carriers time extensions for complying with the statute. The FCC granted hundreds of extensions in conjunction with the FBI's flexible deployment

initiatives.[5] These extensions are now a source of contention between the FBI and the telecommunications industry because carriers have delayed the implementation process by continuing to seek extensions from the FCC. For example, the FCC issued extensions to many wireline and wireless carriers for complying with CALEA until June 30, 2002, and then to June 30, 2004. Furthermore, in 2004 carriers filed for time extensions for complying with CALEA until June 30, 2006.

Carrier officials we interviewed have argued that the extensions are warranted. A telecommunications industry representative noted that while the FBI blames the FCC for granting carriers repeated extensions, the extensions were approved in conjunction with the FBI's flexible deployment initiatives.

Until this point, the FBI's pursuit of legal remedies for carrier non-compliance with CALEA has not included filing enforcement actions.[6] The FBI explained that it has not sought enforcement orders for two reasons: (1) pre-1995 equipment is deemed CALEA-compliant until the FBI agrees to reimburse carriers for their deployment costs, and (2) post-1995 equipment has been covered under FCC time extensions. FBI officials summarized the current status of this issue by saying that it cannot file suit to enforce CALEA because the carriers currently do not have to comply with the statute.

Telecommunications industry representatives cited law enforcement's failure to file enforcement actions as evidence that carrier non-compliance is not a real concern. A representative indicated that carriers were not protected from enforcement actions because the FCC has not ruled on the latest extension requests. However, several state and local law enforcement agencies we

[5] Since 2000, the FBI has offered carriers the opportunity to participate in four flexible deployment initiatives. Under these initiatives, the FBI supported a carrier's petition to the FCC for a time extension for complying with a CALEA deadline if the carrier provided the FBI with: (1) its projected CALEA deployment schedules for all switches in its network, and (2) information pertaining to recent electronic surveillance activity. In addition, the FBI supported a carrier's petition if its projected compliance schedules did not delay the implementation of CALEA solutions in areas with high electronic surveillance activity.

[6] Under Section 108 of CALEA, an order enforcing CALEA may be issued by the court that approved the electronic surveillance order with which the carrier failed to comply or upon the application of the Attorney General through a civil action. A court issuing an enforcement order must allow reasonable time for compliance and may impose a civil penalty not to exceed $10,000 per day for each day of violation of the enforcement order.

interviewed said their failure to file CALEA enforcement actions was a matter of practicality. If they already know a carrier does not have the ability to conduct the electronic surveillance, they will not bother going through the trouble and expense of obtaining an enforcement order. In addition, one local law enforcement official noted that although a local judge might be willing to issue an Order to Show Cause against a carrier, the agency would have to wait three months for a hearing. Given that the wiretap is needed immediately, the official said the law enforcement agency instead will pursue a traditional wiretap, which does not provide the CALEA features.[7]

Activation Negotiations on Pre-1995 Equipment

Although the FBI has spent over $450 million on RTU licenses since 1994, entering into these agreements did not guarantee that CALEA-compliant software solutions were operable. The agreements provided the carriers with the CALEA-compliant software solutions. However, the agreements did not include the activation costs. Software must be activated; engineering and provisioning practices developed; security policies implemented; and in a handful of cases, external hardware deployed, prior to a carrier facilitating surveillance that utilizes the software.

At the time of this audit, the FBI was negotiating reimbursement agreements with four wireline carriers regarding deploying CALEA solutions on pre-1995 wireline equipment.[8] According to the FBI, it concluded negotiations with two carriers in September 2005 for a total cost of $4.5 million. FBI officials said substantial personnel turnover at the third carrier made negotiations difficult, and the FBI said it is postponing further discussions with this carrier until the agreements with the first two carriers are finalized. The FBI also temporarily discontinued negotiations with the fourth carrier because the carrier's initial proposal of $170 million far exceeded the amount of remaining funds.

[7] CALEA offers additional features not available through a traditional wiretap. These additional features are the "punchlist" features described in Appendix IX.

[8] The FBI estimates that entering into software activation agreements with these four carriers would make about 90 percent of the wireline switches CALEA-compliant.

Effects of Delayed Implementation on Wireline Systems

We found that the beneficial features CALEA provided generally have not been realized on wireline systems. However, we believe the following factors mitigate the effects of the delayed implementation: (1) the growing popularity of Internet telephony, (2) the limited number of wireline wiretaps, (3) the apparent limited effect on criminal investigations, and (4) emerging technologies.

Growing Popularity of Internet Telephony

Internet telephony and Internet telephony service providers represent a growing portion of the telecommunications industry.[9] An April 2005 report from research firm International Data Corporation (IDC) predicts that U.S. residential Internet telephony customers will grow from 3 million in 2005 to 27 million by the end of 2009. In addition, a carrier representative we interviewed reiterated a widely held belief that the Internet will swallow up the conventional telephone network, essentially replacing traditional telephone services in the near future.

Limited Number of Wireline Intercepts

According to the April 2005 *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*, the most common location specified in wiretap applications authorized in 2004 was "portable device, carried by/on individual."[10] According to the report, 88 percent of all wiretaps authorized involved portable devices such as portable digital pagers and cellular telephones. The report noted that since 2000 – the first year that the "portable device, carried by/on individual" category was

[9] Unlike a traditional telephone service, Internet telephone service allows the routing of voice conversations over the Internet by converting the sound into packets of data, sending it across the Internet, and reassembling it into sound on the other end.

[10] The Omnibus Crime Control and Safe Street Act of 1968 required the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The statute requires that specific information be provided to the AO, including the offense(s) under investigation; the location of the intercept; the cost of the surveillance; and the number of arrests, trials, and convictions that directly result from the surveillance.

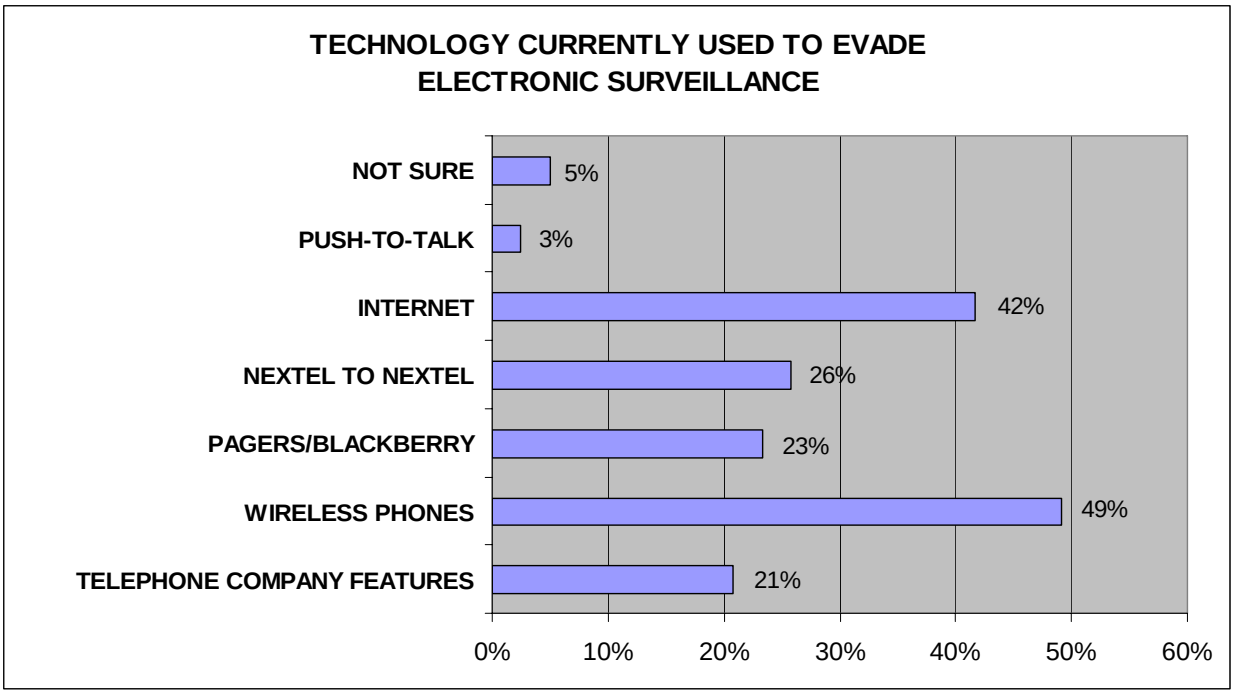
used – "the proportion of wiretaps involving fixed locations has declined as the use of mobile communications devices has become more prevalent." According to the report, only 5 percent of all intercept devices were authorized for personal residences, and 2 percent were authorized for business establishments such as offices, restaurants, and hotels.

Furthermore, our discussions with four wireline carriers in areas of the country with high electronic surveillance activity revealed a limited number of court orders for intercepts requiring CALEA features. For example, a wireline carrier reported that from 2002 to 2004, less than one percent of the court orders it received for intercepts required CALEA features. According to the federal, state, and local law enforcement officials we interviewed and surveyed, their agencies do not request intercepts requiring CALEA features for several reasons (e.g., the high cost charged by carriers, carrier noncompliance, or the investigation only required a traditional wiretap).

The Apparent Limited Effect on Criminal Investigations

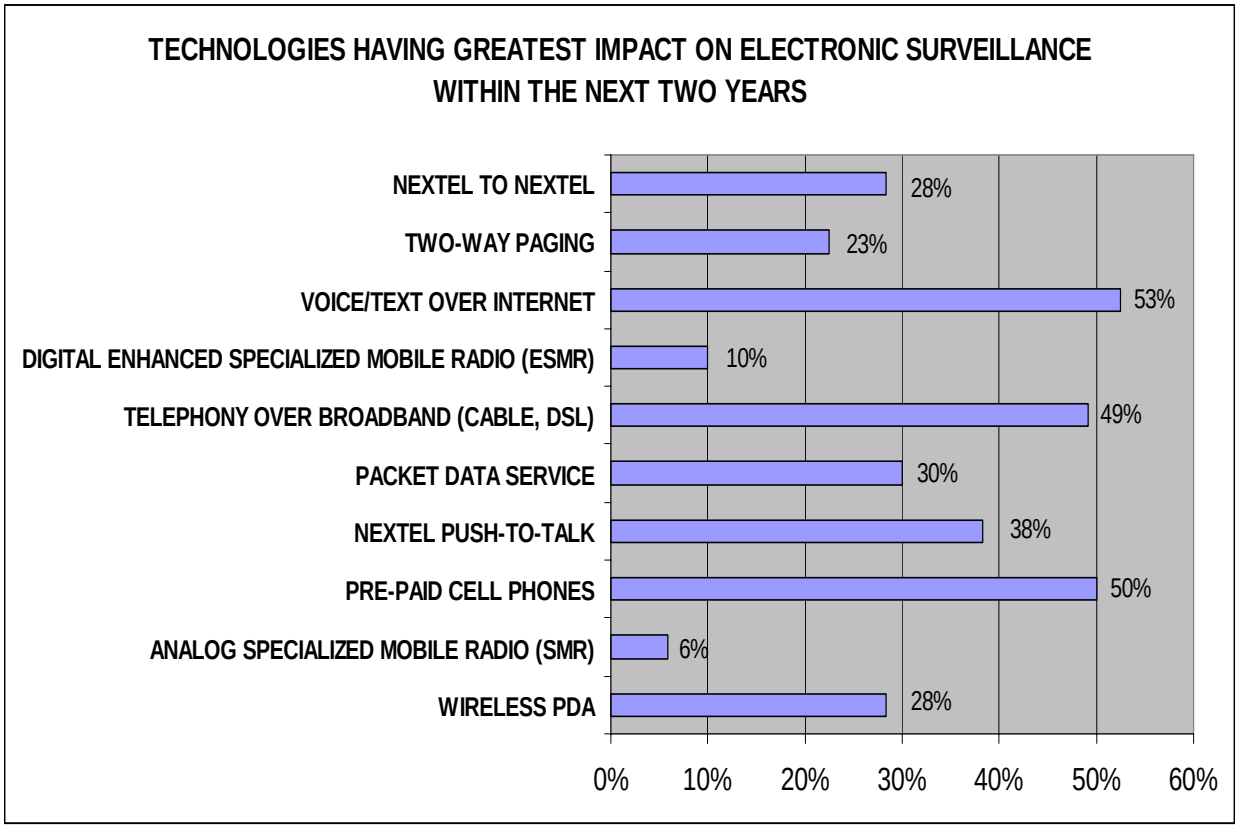
The FBI measures the impact of CALEA and identifies federal, state, and local law enforcement concerns through distribution of Threat Assessment Surveys and by maintaining a help desk that law enforcement officials can contact when they have difficulty conducting electronic surveillance or if they have questions.[11] Our review of the FBI's Threat Assessment Surveys revealed that the law enforcement community is less concerned over the ability to perform electronic surveillance on wireline equipment, and more concerned over new and emerging technologies. As shown in the following chart, 49 percent of those surveyed believed that criminals evaded surveillance using wireless phones, and 42 percent believed the use of the Internet allowed criminal evasion of electronic surveillance.

[11] The FBI developed the Threat Assessment Survey to better understand and anticipate future electronic surveillance threats to law enforcement. The surveys were conducted from November 2003 through September 2004 at the national and regional meetings of the National Technical Investigator Association, and at various DEA and FBI training sessions.



Source: OIG analysis of 120 FBI Threat Assessment Surveys

As shown in the following chart, law enforcement officers who completed the survey expected that pre-paid cell phones, telephony over broadband, and voice or text over the Internet would have the greatest impact on their agency's electronic surveillance activities within the next two years.



Source: OIG analysis of 120 FBI Threat Assessment Surveys

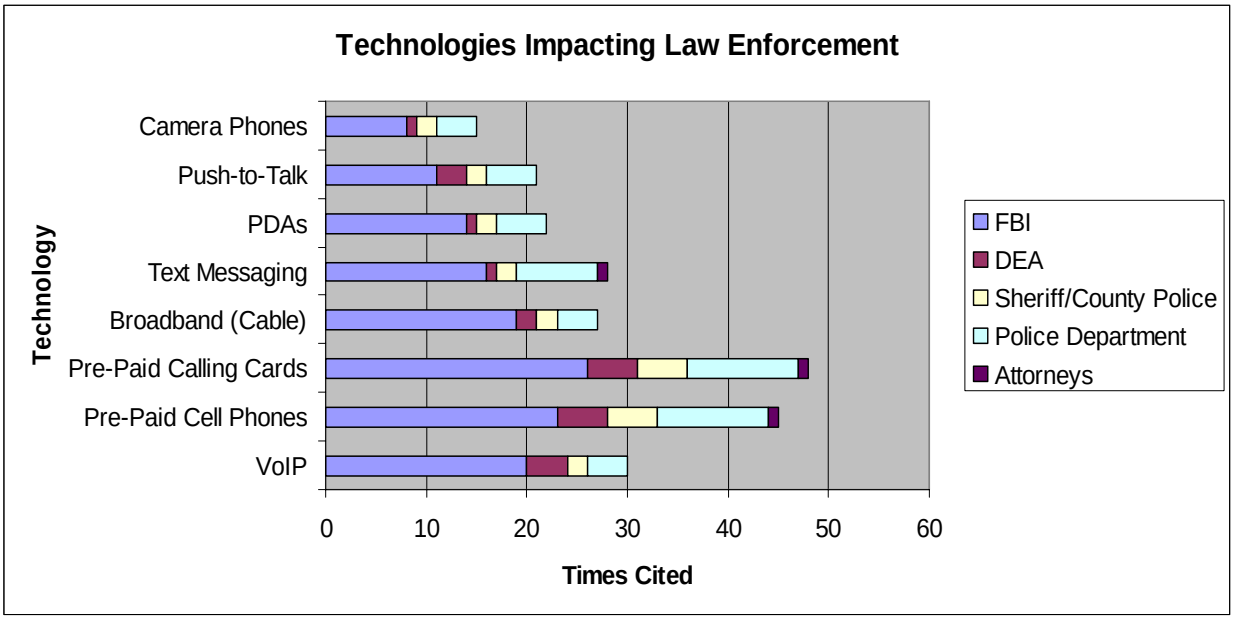
In our interviews with FBI officials, we requested specific examples that illustrate existing intercept problems. The FBI provided a document entitled *FBI Investigative Technology Division CALEA Law Enforcement Case Examples* dated October 29, 2004. The document contained 23 examples of unsuccessful intercepts, none of which involved electronic surveillance problems for wireline intercepts. The 23 examples involved either wireless or Voice over Internet Protocol (VoIP), which seems to be law enforcement's primary concern since a low percentage of wireline intercepts are conducted.[12] In addition, we believe these examples are not necessarily indicative of technology that is negatively impacting law enforcement's ability to conduct electronic surveillance because the carriers identified in these examples have either implemented CALEA solutions or contracted with a trusted third party to administer its CALEA responsibilities.

[12] Unlike a traditional telephone service, Internet telephone service or Voice over Internet Protocol allows the routing of voice conversations over the Internet by converting the sound of a voice into packets of data, sending it across the Internet, and reassembling it into sound on the other end of a call.

Emerging Technologies

According to law enforcement officials, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

Similarly, officials surveyed by the OIG identified pre-paid calling cards and pre-paid cell phones as the top two threats affecting their ability to conduct electronic surveillance. Of the 82 affirmative responses to our survey, law enforcement officials indicated that the following emerging technologies negatively affect their agencies' ability to conduct electronic surveillance:



Source: Law enforcement responses to the OIG survey

FBI Plans for Remaining CALEA Funding

As of November 2005, about $45 million in CALEA funds remain for the implementation of carrier technical solutions. As previously discussed, the FBI is in various stages of negotiating reimbursements to four carriers for the cost of deploying CALEA solutions on their pre-1995 wireline equipment. The FBI said that it plans to use any remaining funds to reimburse second-tier carriers for their implementation of CALEA solutions on pre-1995 wireline equipment.

We are concerned about how the FBI plans to use the remaining $45 million in CALEA funding. We recognize that CALEA allows the FBI to reimburse carriers for all reasonable costs associated with bringing pre-1995 wireline equipment, facilities, and services into compliance.

Nevertheless, because telecommunications technology has significantly advanced from the time of CALEA's enactment, and because of the increasing use of these new technologies by subjects of electronic surveillance, we believe the FBI should reexamine the future benefits of implementing CALEA on wireline systems.

Issues Requiring Resolution

The development, deployment, and maintenance costs associated with implementing CALEA and the related question of who should bear those costs continue to be controversial issues. In addition to cost issues, we found that carrier's limited customer service for law enforcement officials attempting to conduct electronic surveillance and the FBI's limited support provided to state and local law enforcement will also affect the future implementation of CALEA.

Costs Incurred by Carriers

Officials from the 10 carriers we interviewed indicated that they were committed to complying with CALEA and that they had, or were actively engaged in deploying CALEA solutions on their networks. However, these same officials advised us that the significant costs associated with making their networks CALEA compliant will hinder full CALEA implementation. Carrier representatives stated that the cost to develop, deploy, and maintain electronic surveillance capabilities has been significant, and that these costs are expected to increase as technology accelerates. For example, one carrier said that it spent about $40 million to make its network CALEA-compliant.[13]

Costs Incurred by Law Enforcement

From a law enforcement perspective, carrier wiretap fees, equipment costs, and delivery costs contribute to the high cost of conducting electronic surveillance.

Wiretap Fees. A traditional wiretap costs law enforcement about $250. However, while we found that fees vary widely, a wiretap with CALEA features costs law enforcement approximately $2,200, according to law enforcement officials and carrier representatives we interviewed. A law enforcement official noted that, "[w]ith CALEA, the

[13] This information was provided by carrier representatives and was not audited. Further, the reported carrier costs are not comparable because carrier networks vary greatly in size and switch type.

carriers do less work but it costs approximately 10 times as much to do a CALEA-compliant tap versus a traditional tap." While many law enforcement officials we interviewed agreed that the features provided by CALEA are valuable, we found that some law enforcement agencies said they cannot afford to conduct the number of CALEA wiretaps they would like to support their investigations. Instead, we found these agencies often conduct traditional wiretaps to avoid the high carrier fees associated with a CALEA wiretap.

Equipment Costs. In order to conduct CALEA intercepts, law enforcement must maintain or have access to a wireroom. A wireroom consists of a computerized system that intercepts, decodes, records, and plays back telephone communications. Law enforcement agencies across the country have spent between hundreds of thousands to several million dollars to equip their wirerooms. The equipment costs depend upon the desired capacity of simultaneous wiretaps and the need to accommodate carriers' various delivery methods. In addition to the initial purchase of wireroom equipment, some law enforcement agencies pay about $30,000 per year to equipment vendors to maintain their equipment. Further, law enforcement agencies said they spend additional funds to acquire hardware and software upgrades just to keep current with emerging technological improvements.

Delivery Methods. Many law enforcement officials noted that CALEA addresses what carriers need to provide law enforcement agencies without addressing how the data is to be delivered. Due to the potential delivery methods, law enforcement agencies must purchase additional equipment to receive the intercepted data from a carrier.

The four delivery methods are dial-out, virtual private network (VPN), frame relay, and T-1 lines. While dial-out and VPN are increasingly popular and favored among law enforcement agencies, some carriers only deliver data via a T-1 line which we found to be the most expensive delivery method. Using a T-1 line costs law enforcement agencies approximately $1,300 for each switch, and can take up to two months to install. One law enforcement official told us that his agency pays approximately $20,000 per month to carriers to maintain T-1 line connections.

However, for some law enforcement agencies delivery of wireline CALEA intercept data by T-1 line is impractical because of the number of T-1 lines required. Law enforcement officials in California and

Florida, for example, stated that carriers required T-1 lines to each switch in order to deliver CALEA features. These law enforcement officials explained that this concept is cost prohibitive considering the number of switches. Therefore the California and Florida law enforcement officials we interviewed said they conduct traditional intercepts on wireline switches rather than intercepts with CALEA features.

Limited Carrier Customer Service

Several law enforcement officials stated that they received poor customer service from the carriers when dealing with electronic surveillance issues, and believed some carrier employees lack CALEA training. In particular, carriers were criticized for interrupting wiretaps by upgrading switches without notifying law enforcement. In addition, law enforcement officials on the west coast stated that carriers on the east coast do not provide customer service after 5:00 p.m. EST. Another law enforcement official cited an example of when a carrier's switches were able to conduct the wiretaps but the carrier's technician did not know how to activate the switches. However, one carrier representative told us that his company investigated such law enforcement complaints and found that about half of the problems stem from law enforcement's lack of technical expertise in operating the collection equipment and not the carrier's lack of customer service.

FBI Support of State and Local Law Enforcement

State and local law enforcement officials stated that they feel unsupported by the FBI on electronic surveillance issues. These officials said a lack of FBI-provided CALEA training has negatively affected the quality of CALEA implementation. The law enforcement officials stated that the FBI should provide basic "hands-on" training for law enforcement agents and technical personnel on CALEA wiretaps.

In addition, law enforcement officials who attend FBI-sponsored Law Enforcement Technical Forums noted that the number of forums has declined over the last few years. Additionally, we were told that forums have become one-sided with the FBI simply presenting information, instead of an exchange of ideas between the FBI and law enforcement officials. Law enforcement officials also noted that the FBI should provide an opportunity and venue for vendors to showcase their equipment and analytical programs, and for meetings with carriers to voice their concerns.

Controversy over Technologies Covered by CALEA

In March 2004, the DOJ attempted to resolve many of the electronic surveillance problems faced by law enforcement officials with new technologies by filing a *Joint Petition for Expedited Rulemaking* with the FCC. The *Joint Petition* also sought to address longstanding implementation issues such as carrier extensions of time for complying with CALEA, enforcement for noncompliance, and fees charged by carriers. In response to the *Joint Petition*, on August 5, 2005, the FCC ruled that providers of facilities-based broadband Internet access service and interconnected (managed) VoIP services must be prepared to accommodate electronic surveillance within the scope of CALEA.[14] According to the FCC, these services essentially replace conventional telecommunications services currently subject to CALEA.[15] The FCC also found that the definition of "telecommunications carrier" encompasses providers of services that are not classified as telecommunications services under the Communications Act of 1934. The FCC stated that it is taking a two-step approach to focus debate on the implementation rather than the applicability of CALEA to providers of broadband Internet access services and VoIP services.

[14] The FBI describes "managed VoIP services" as those that offer voice communications calling capability where the VoIP provider acts as a mediator to manage the communication between end points and to provide call set-up, connection, termination, and party-identification features, often generating or modifying dialing, signaling, switching, addressing, or routing functions for the user. The FBI distinguishes managed communications from "non-managed" or "peer-to-peer" communications where people can communicate directly without going through a central telephone company.

[15] The Substantial Replacement Provision of CALEA allows the FCC to classify a person or entity as a telecommunication carrier if the FCC finds that it is providing a communication service that is a replacement for a substantial portion of the local telephone exchange service, and if it is in the public interest to deem the person or entity to be a telecommunication carrier (47 U.S.C. § 1001(8)(B)(ii)).

Conclusion

Ten years after its enactment, the FBI continues to encounter significant challenges in implementing CALEA. According to law enforcement officials we interviewed and surveyed, law enforcement has been significantly handicapped in its efforts to conduct electronic surveillance by a variety of technological innovations that have taken place in the telecommunications field, including the emergence and widespread availability of broadband Internet access services and VoIP services. Other impediments have included a contentious process of developing technical standards, continuous carrier requests for extensions, and extended negotiations with carriers over software activation agreements. In light of the FCC's August 2005 ruling, absent some change in existing CALEA requirements and corresponding changes in how the FBI exercises its responsibilities in overseeing CALEA implementation, the goals envisioned when CALEA was enacted will not be realized fully.

Recommendations

As a result of our review, we offer six recommendations for the FBI to consider in fulfilling its CALEA implementation responsibilities. The recommendations include improving liaison between law enforcement officials and carrier and manufacturer representatives; improving the methodology for gathering examples of criminal investigations that have been adversely impacted because of a carrier's inability to provide CALEA-compliant wiretaps; and revisiting the FBI's plans to spend the remaining $45 million in CALEA funds. In addition, we will continue to monitor recommendations made in prior OIG reports on CALEA, specifically that the FBI should collect and maintain data on the number of carrier switches that are CALEA-compliant, and submit to Congress legislative changes necessary to ensure that electronic surveillance is achieved in the face of rapid technological change.

THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA)

TABLE OF CONTENTS

INTRODUCTION

Criminal organizations and individuals frequently use telephones and other electronic communications devices to carry out criminal and terrorist acts. To combat and deter this activity, law enforcement and other authorized government agencies use court-authorized electronic surveillance for collecting information to investigate and prosecute criminals. According to the Federal Bureau of Investigation (FBI), electronic surveillance is a critical tool needed to meet its law enforcement, counterterrorism, and intelligence-collecting mandates.

What Is Electronic Surveillance?

Electronic surveillance consists of the acquisition of *call-identifying information* and the interception of communications *content.* Call-identifying information is defined as dialed number information that identifies the origin, direction, destination, or termination of any communication generated or received by a subject of surveillance. Normally, call-identifying information is collected via "pen registers" and "traps and traces."[16] Content is defined as the substance or meaning of a communication and is obtained by a wiretap.[17] For purposes of this report, the term electronic surveillance is used only in the sense of the real-time interception of information.

The use of electronic surveillance is strictly limited by law. Title III of the Omnibus Crime Control and Safe Street Act of 1968, as amended (Title III),[18] and portions of the Electronic Communications Privacy Act (ECPA),[19] as amended, serve as the primary laws

[16] Pen registers are surveillance devices that capture the phone numbers dialed on outgoing telephone calls, whereas trap and trace devices capture the numbers identifying incoming calls. These two devices are not supposed to reveal the content of communications, identify the parties to a communication, or whether a call was connected. Rather, they only convey that one particular phone dialed another phone. A pen register and trap and trace, which can be obtained separately or together, provide real-time call-identifying information.

[17] A wiretap provides real-time call-identifying and content information.

[18] Title III contains the procedures law enforcement must follow to obtain the necessary judicial authorization to conduct electronic surveillance. Congress subsequently amended the statute to confirm the government's authority to require providers of communications services to provide law enforcement with the "…technical assistance necessary to accomplish the interception…."

[19] The ECPA extended Title III coverage to the contents of electronic messages, such as e-mail, and to data transmissions from facsimiles and pagers.

governing electronic surveillance of criminal investigations. Rules regarding electronic surveillance conducted for foreign intelligence, counterintelligence, and terrorism investigations are derived from the Foreign Intelligence Surveillance Act (FISA), as amended.[20]

Changing Technology Challenges Law Enforcement

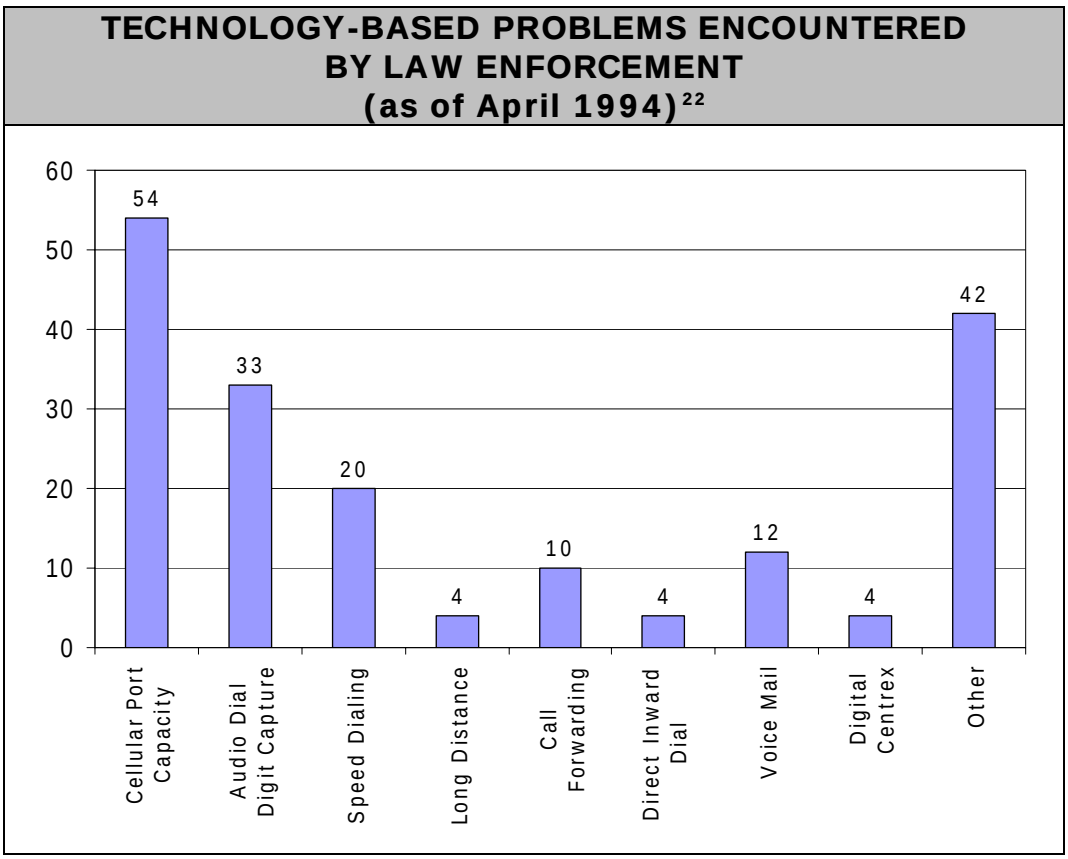
In the early 1990s, technology advances in the telecommunications industry began challenging the ability of law enforcement agencies to fully implement electronic surveillance. In March 1994, the FBI Director testified that an informal FBI survey of federal, state, and local law enforcement agencies identified 91 examples where technological impediments precluded full implementation of court orders for electronic surveillance. According to the FBI, the survey results revealed that 33 percent of the examples involved cellular systems (of which 11 percent were related to the limited capacity of cellular systems to accommodate a large number of simultaneous intercepts), and 32 percent involved custom-calling features like call forwarding, call waiting, and speed dialing.[21]

Subsequent to the hearing, the FBI worked with law enforcement agencies to identify further examples of such technological impediments. In April 1994, the FBI presented to the House and Senate Judiciary Committees details of 183 instances (including the original 91 examples) where the FBI, state, or local law enforcement agencies encountered problems with electronic surveillance, as shown in the following chart:

---

[20] FISA requires carriers to furnish "…all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference…" with the services of the target of electronic surveillance.

[21] Capacity is defined as the number of simultaneous call-content interceptions, pen registers, and trap and traces that law enforcement can conduct in a given geographical area.



Source: U.S. House of Representatives Report No. 103-827, October 4, 1994

By the mid 1990s, what was once a relatively simple matter of initiating a wiretap by attaching wires to terminal posts now required the expert assistance and cooperation of a telecommunications carrier.[23]

[22] Each technology-based problem is described in Appendix II.

[23] CALEA defines "telecommunications carrier" as a person or entity engaged in the transmission of communications as a common carrier for hire. It includes a person or entity engaged in providing communication services to the extent that the Federal Communications Commission (FCC) finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier. According to CALEA, the phrase "telecommunications carrier" does not include persons or entities insofar as they are engaged in providing information services, and any class or category of telecommunications carrier that the FCC exempts by rule after consultation with the Attorney General.

The Communications Assistance for Law Enforcement Act

To address law enforcement's difficulty in performing electronic surveillance in the face of new telecommunications and computer features, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994. The purpose of CALEA was to ensure that telecommunications carriers had the necessary technical capability and capacity to fulfill their Title III and FISA obligations in order to assist law enforcement in conducting electronic surveillance.

CALEA required that telecommunications carriers ensure that their equipment, facilities, or services provided the following four capabilities (assistance capability requirements):

1. expeditiously isolate the content of targeted communications transmitted within the carrier's service area;

2. expeditiously identify information regarding the originating and destination numbers of targeted communications, but not the physical location of the targets, except as could be determined by the phone number;

3. transmit to law enforcement intercepted communications and call-identifying information to a location away from the carrier's premises; and

4. carry out intercepts unobtrusively, so that targets of electronic surveillance were not made aware of the interception and in a manner that did not compromise the privacy and security of other communications.[24]

According to the FBI, CALEA was intended to bring about a fundamental shift in how the telecommunications industry viewed its electronic surveillance responsibilities. Although Title III and FISA required telecommunications carriers to provide any assistance necessary to accomplish an electronic interception, the question of whether telecommunications carriers had an obligation to design networks that facilitated an authorized interception had not been decided. In short, CALEA sought to ensure that the telecommunications industry considered law enforcement's need and

[24] A description of the CALEA statute by section can be found in Appendix III.

authority to conduct electronic surveillance as a basic element in developing its telecommunications products and in providing service.

Consequentially, CALEA assigned certain responsibilities to the Attorney General, the Federal Communications Commission (FCC), telecommunications carriers, telecommunications equipment manufacturers, and the Department of Justice (DOJ) Office of the Inspector General (OIG). In February 1995, the Attorney General delegated CALEA management to the FBI. The following table outlines the entities with CALEA responsibilities.

STATUATORY RESPONSIBILITIES UNDER CALEA

Entity	Responsibility
Federal Bureau of Investigation	Ensures the industry-wide implementation of the assistance capability requirements.
	Consults with state and local law enforcement agencies.
	Provides estimates to various telecommunications industry organizations on the number of interceptions, pen registers, and trap and traces devices that government agencies may need to conduct.
	Consults with the FCC regarding carrier petitions that seek a determination that compliance with the assistance capability requirements is not reasonably achievable.
	Establishes rules to facilitate carrier reimbursements.
	Allocates appropriated funds to carriers in a manner consistent with law enforcement priorities.
	Annually reports to Congress the amount of carrier payments during the preceding year and the projected payments for the current year.
Federal Communications Commission[25]	Determines which entities are telecommunications carriers and may exempt any entity class or category as a telecommunications carrier by rulemaking and consulting with the FBI.
	Establishes technical standards for compliance with assistance capability requirements if industry associations fail to issue technical standards, or if a government agency or any other person believes that industry-adopted standards are deficient.
	Reviews petitions for extensions.
Telecommunications Carriers (service providers)[26]	Ensures that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the CALEA assistance capability requirements.
Equipment Manufacturers	Makes available all features or modifications necessary to meet assistance capability requirements, including consulting with carriers over current and planned equipment.
Office of the Inspector General[27]	Reports to Congress biennially on (1) CALEA-compliant equipment, facilities, and services; (2) analysis of payments to carriers for CALEA-compliant modifications; and (3) future-cost projections for assistance capability requirement modifications.

[25] A summary of FCC actions related to CALEA can be found in Appendix IV.

[26] To meet their responsibilities under CALEA, some carriers have chosen to contract with *trusted third parties*. A trusted third party is a private company whose services include providing reviews of a carrier's CALEA-compliance, managing the intercept function, and serving as the custodian of record for the intercept information.

[27] See Appendix V for a summary of prior OIG audits.

In summary, effective implementation of CALEA's provisions relies on the shared responsibilities of the government agencies and the service providers and manufacturers subject to the law's requirements.

Controversy Over Technologies Covered by CALEA

Since CALEA's enactment in 1994, the telecommunications industry has lobbied Congress to change certain provisions of the law. Appendix VI presents a summary of these efforts. While the FBI has been successful in blocking these efforts, CALEA remains controversial.

According to its legislative history, CALEA was supposed to strike a balance between three competing national priorities: preserving law enforcement's ability to conduct electronic surveillance; protecting privacy; and promoting innovation. However, controversy surrounds these three priorities as discussed below:

- Preserving law enforcement's ability to conduct electronic surveillance. CALEA was an attempt by Congress to stop electronic surveillance from becoming obsolete. Law enforcement hoped that CALEA would preserve its ability to access evidence against suspected terrorists and criminals.

- Protecting privacy. Intercepted communications were required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception." These communications included unrelated, irrelevant, and non-criminal communications not specifically covered in the court order. Furthermore, advances such as "packet-mode" technology of Internet telephone service, also known as Voice over Internet Protocol (VoIP), confronted law enforcement with new surveillance challenges.[28] The packet-mode technology of Internet telephony is more difficult to intercept than traditional circuit-mode communications because the data packets are not readily identifiable.[29] Therefore, law enforcement may intercept packets of data

[28] Unlike a traditional telephone service, Internet telephone service allows the routing of voice conversations over the Internet by converting the sound of a voice into packets of data, sending it across the Internet, and reassembling it into sound on the other end of a call.

[29] Circuit-mode communications refers to the routing of voice communications through a traditional telephone service.

from subscribers who are not the subject of electronic surveillance.

- Promoting innovation. According to representatives from the Center for Democracy and Technology, applying CALEA to Internet telephone services would cause irreparable harm to the Internet by increasing consumer costs, impairing and delaying innovation and new services, and forcing telecommunications providers to develop Internet innovations outside of the United States.[30] These representatives explained that even if the FCC finds that Internet telephone services fall under CALEA, the statute would only apply to U.S. providers. This would place U.S. telecommunications providers at a competitive disadvantage because they are directly competing with foreign-based providers. Officials from telecommunications carriers we interviewed also raised these issues.

The collision of these national priorities created controversy. At the time of its passage, it was clear that CALEA covered wireline and cellular communications; network-based services such as call-forwarding and conference calling; and technologies such as pagers and satellite phones. However, CALEA does not cover "information services," and this exclusion has proven to be a major source of controversy.[31] According to the FBI, at the time of CALEA's enactment consumers used the Internet to obtain information, not as a telecommunications service. However, with the recent growth of Internet telephony, the question of whether CALEA applies to Internet Service Providers (ISP) or other VoIP providers continues to be widely debated.

An example of the controversy involves VoIP provider Vonage. In 2003, the Minnesota Public Utility Commission (MPUC) ruled that Vonage was a telephone service provider under Minnesota state law. As a result, Vonage was subject to certain state regulations, including those governing 911 emergency calling services. In September 2003,

[30] The Center for Democracy and Technology identifies itself as a public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media.

[31] According to CALEA, "information services" means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.

Vonage petitioned both the U.S. District Court in Minnesota for injunctive relief and the FCC for pre-emption of all state regulation on the grounds that Vonage is an ISP rather than a telephone service provider. In October 2003, the U.S. District Court in Minnesota ruled in favor of Vonage, concluding that Vonage is an ISP. The Minnesota Attorney General appealed on behalf of the MPUC. In December 2004, the U.S. Court of Appeals for the Eighth Circuit upheld the district court ruling that the MPUC may not regulate calls made through the Internet as it does calls made through traditional phone lines.

Meanwhile, the FCC sought comments on Vonage's petition. The FBI filed comments stating that Vonage could not qualify for relief because its VoIP service is a telecommunications service instead of an information service. In November 2004, the FCC issued its decision ruling that Internet phone services should not be governed by the same state regulations as traditional telephone companies. As a result, whether CALEA applied to Vonage and other Internet phone services remained controversial.

Joint Petition for Expedited Rulemaking

In March 2004, the DOJ, the FBI, and the Drug Enforcement Administration (DEA) attempted to resolve problems faced by law enforcement with these new technologies by filing a *Joint Petition for Expedited Rulemaking* with the FCC. The *Joint Petition* also sought resolution on issues pertaining to carrier extensions for complying with CALEA, enforcement for noncompliance, and carrier fees.[32] In the *Joint Petition*, the DOJ and other groups asked the FCC to:

1) identify both the types of services and entities that are subject to CALEA, as well as services that are considered "packet-mode services";

2) issue an initial Declaratory Ruling or other formal FCC statement, and ultimately adopt final rules that compel broadband access and telephony services be subject to CALEA;

3) reaffirm that push-to-talk service is subject to CALEA;

[32] We discuss extensions and enforcement in Finding II, and carrier fees in Finding IV.

4) adopt rules that provide for the easy and rapid identification of future CALEA-covered services and entities;

5) establish rules, benchmarks and deadlines for CALEA compliance with packet-mode and other future CALEA-covered technologies.

The FCC declined to issue a declaratory ruling, finding instead that it was necessary to compile a complete record on the factual and legal issues. Therefore, on August 4, 2004, the FCC issued a *Notice of Proposed Rulemaking* (NPRM) in response to the DOJ petition and sought comments on its tentative conclusions.[33] The comment period on the NPRM closed in December 2004. In response to the NPRM, interested parties filed about 650 comments with the FCC. Among the parties were DOJ; the carriers Verizon, Sprint, Bell South, and SBC; VoIP provider Vonage; ISP Earthlink; and "trusted third party" Verisign.[34]

In the opinion of carrier representatives with whom we spoke, the NPRM issues are, for the most part, already outdated. Carrier representatives stated that as technological change continues to accelerate, law enforcement agencies will have a harder time keeping up and electronic surveillance may suffer.

FCC Ruling

On August 5, 2005, the FCC ruled on the *Joint Petition*. The FCC stated that providers of facilities-based broadband Internet access service and interconnected (managed) VoIP services must be prepared to accommodate electronic surveillance within the scope of CALEA.[35]

---

[33] For additional information on the NPRM, see Appendix IV, August 4, 2004, *Notice of Proposed Rulemaking and Declaratory Ruling*.

[34] Appendix VII contains a summary of these comments.

[35] The FBI describes "managed VoIP services" as those that offer voice communications calling capability where the VoIP provider acts as a mediator to manage the communication between end points and to provide call set-up, connection, termination, and party-identification features, often generating or modifying dialing, signaling, switching, addressing, or routing functions for the user. The FBI distinguishes managed communications from "non-managed" or "peer-to-peer" communications where people can communicate directly without going through a central telephone company. The FCC requested comments on the appropriateness of this distinction between managed and non-managed VoIP communications for purposes of CALEA.

According to the FCC, these services essentially replace conventional telecommunications services currently subject to CALEA.[36] The ruling stated that the FCC's determination is limited to facilities-based broadband Internet access service providers and VoIP providers offering services that permit users to receive calls from, and place calls to, the public switched telephone network or PSTN, the publicly available dial-up telephone network.[37]

The FCC also found that the definition of "telecommunications carrier" encompasses providers of services that are not classified as telecommunications services under the Communications Act of 1934. With respect to a deadline for compliance, the FCC reasoned that because newly covered providers need a reasonable amount of time to come into compliance with all relevant CALEA requirements, a deadline of 18 months from the effective date of the FCC's Order would be appropriate.

In addition to ruling that certain broadband and managed VoIP services fall within the scope of coverage, the FCC adopted a Further NPRM seeking more information about whether certain classes or categories of facilities-based broadband Internet access providers (i.e., small and rural providers and providers of broadband networks for educational and research institutions) should be exempt from CALEA.

---

[36] The Substantial Replacement Provision of CALEA allows the FCC to classify a person or entity as a telecommunication carrier if the FCC finds that it is providing a communication service that is a replacement for a substantial portion of the local telephone exchange service, and if it is in the public interest to deem the person or entity to be a telecommunication carrier (47 U.S.C. § 1001(8)(B)(ii)). The FCC's Deputy Chief, Office of Engineering and Technology, testified before the House of Representatives Subcommittee on Telecommunications and the Internet September 8, 2004, that an "irreconcilable tension" could exist for service providers that find themselves at the same time subject to CALEA under the Substantial Replacement Provision and exempted from it by virtue of the information services exclusion.

[37] With this determination, the FCC confirmed its February 12, 2004, Memorandum Opinion and Order (see Appendix IV) wherein the FCC considered a peer-to-peer VoIP provider an "information service" and therefore exempt from CALEA. The decision to exempt peer-to-peer VoIP from CALEA is a source of contention within the industry as summarized in some of the comments to the NPRM in Appendix VII. Although the effect of this decision is too early to determine, in the opinion of a carrier representative to whom we spoke, peer-to-peer VoIP is the wave of the future, and these decentralized communications systems may present a challenge to law enforcement. [LAW ENFORCEMENT SENSTIVE INFORMATION REDACTED].

The FCC's ruling, however, does not address any of the other issues raised in the March 10, 2004, *Joint Petition* (e.g., cost of compliance to be borne by industry for post-January 1, 1995, equipment; extensions of the compliance date; enforcement; and the identification of future services). The FCC is expected to provide a final ruling on these issues in the near future.

In October 2005, telecommunications firms, nonprofit organizations, and educators challenged the FCC's August 5, 2005, ruling in the U.S. Court of Appeals in Washington, D.C. These groups are challenging the rules on both privacy grounds, and because they claim implementing the rules will be too expensive. In the OIG's April 2004 report, we recommended that the FBI submit to Congress legislative changes to CALEA it believed necessary to ensure that electronic surveillance is achieved expeditiously in light of rapid technological changes.[38] Despite the FCC's ruling, we continue to believe that legislative clarification of CALEA's intent is necessary.[39] As discussed in Finding II of this report, previous litigation over what should be required for law enforcement's wiretapping capabilities substantially delayed CALEA implementation, and we are concerned that this current litigation will delay CALEA implementation as it applies to new technologies.

[38] Department of Justice, Office of the Inspector General Audit Report Number 04-19, *The Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation*, April 2004.

[39] Although we do not repeat our previous recommendation in this report, we will continue to monitor the FBI's progress in pursuing legislative clarification through our audit follow-up process.

FINDINGS AND RECOMMENDATIONS

I. CALEA IMPLEMENTATION COSTS AND PROGRESS

After 10 years and the expenditure of over $450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant.[40] The FBI's strategy for spending these funds focused on identifying switches in locations of high-priority to law enforcement and first ensuring the CALEA-compliance of those switches. While the number of CALEA-compliant switches is based on the best available data, we cannot provide assurance on the accuracy of these estimates. Neither the FBI nor the FCC know the actual percentages of CALEA-compliance because the universe of carriers is unknown. In addition, as reported in previous OIG audits, the cost information provided to us by the FBI did not provide a basis to determine the reasonableness of the costs the FBI incurred.

CALEA Implementation Costs

To facilitate CALEA implementation, Congress authorized the appropriation of $500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995.[41] In general, costs for achieving compliance for equipment installed after January 1, 1995, were to be incurred by the telecommunications carriers. However, the legislation permitted the FBI, on application of a carrier, to pay that carrier for the additional reasonable costs of making equipment deployed after January 1, 1995,

[40] A switch is a telephone company device which "makes the connection" when a call is placed. Modern switches are specialized computers.

[41] According to the U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in a Digital Age*, the costs of the legislation and differences of opinion about who should bear those costs were highly controversial issues during the time leading up to passage of CALEA. The $500 million figure was a compromise among widely ranging estimates from the telecommunications industry and law enforcement agencies as to the costs of modifying a carrier's equipment and technology to make it CALEA-compliant. Both the telecommunications industry and law enforcement's estimates were based on assumptions about costs for modifying existing equipment and deploying the technology, but the estimates were generally not based on formal engineering cost analysis.

compliant with the assistance capability requirements. However, this applied only if the carrier's compliance could not be reasonably achieved if no payment occurred.

On September 30, 1996, the Omnibus Consolidated Appropriations Act of 1997 amended CALEA by adding Title IV which created the Telecommunications Carrier Compliance Fund (TCCF) and appropriated $60 million in initial funding. This fund is available without fiscal year limitation to the Attorney General for making payments to telecommunications carriers, equipment manufacturers, and providers of telecommunications support services. Additionally, CALEA authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF, subject to applicable congressional reprogramming requirements.

The following table illustrates the dollar amounts and timing of congressional appropriations and fund transfers from authorized agencies with law enforcement and intelligence responsibilities.

Telecommunications Carrier Compliance Fund Activity

Activity	Amount
FY 1997 Direct Appropriations	$60,000,000
FY 1997 Department of Justice Working Capital Fund	$40,000,000
FY 1997 U.S. Postal Inspection Service Transfer	$1,000,000
FY 1997 U.S. Customs Service Transfer	$1,580,270
FY 2000 Direct Appropriations	$15,000,000
FY 2000 Supplemental Appropriations	$181,000,000
FY 2001 Direct Appropriations	$200,976,876
Total Deposits	**$499,557,146**

Source: FBI, *Communications Assistance for Law Enforcement Act (CALEA) Ninth Annual Report to Congress*

Since 1994, the FBI has spent approximately $450 million to reimburse carriers for their purchase of CALEA-compliant software licenses (referred to throughout this report as Right-to-Use or RTU licenses). The software licensing agreements allowed the software to

be installed and activated on both pre- or post-1995 wireline and wireless equipment.[42]

Right-to-Use (RTU) Software Licenses

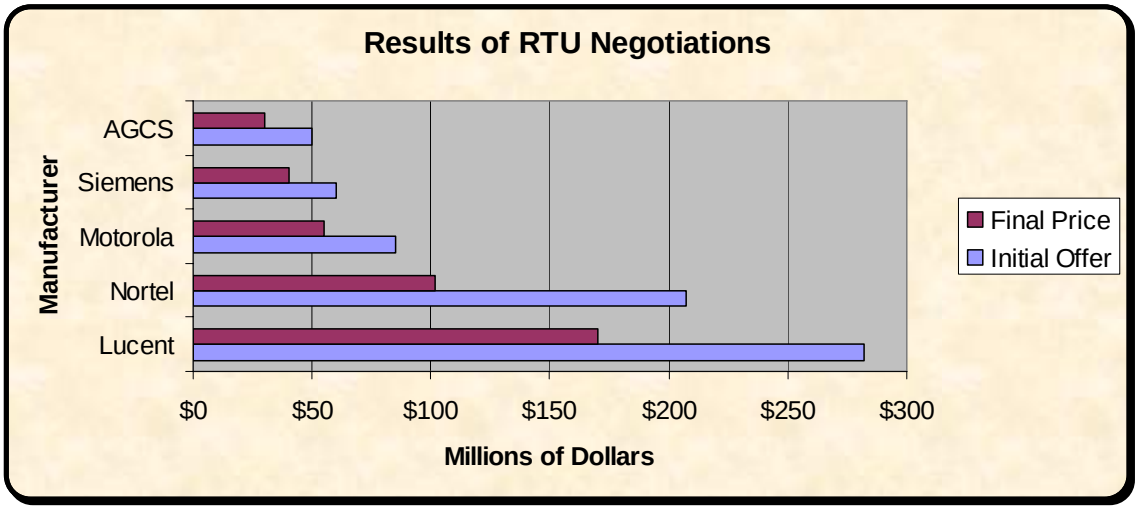
An important aspect of the FBI's implementation of CALEA was its nationwide buyout of RTU software licenses. The software allows carriers to meet CALEA intercept requirements by collecting and delivering to law enforcement pertinent call-identifying information, content, or both. The FBI negotiated with carrier and manufacturing representatives to determine the most appropriate way to arrange for carriers to obtain and deploy their CALEA-capability requirements. The FBI concluded that rather than reimbursing each carrier individually for the cost of the RTU licenses, entering into RTU software licenses with equipment manufacturers and their carrier partners would be the best utilization of the appropriated funds. The FBI reasoned that if carriers did not have to pay manufacturers individually for the software licenses, volume discounts could be achieved, thereby reducing deployment costs. This approach allowed carriers to receive, at no charge, CALEA electronic surveillance software.

After extensive negotiations, the FBI entered into several RTU license agreements to reimburse carriers for the purchase of RTU software licenses from certain manufacturers. The agreements were negotiated between February 1998 and April 2003 and allowed carriers to install and activate the CALEA software on either pre-1995 or post-1995 wireline and wireless equipment. By the time these agreements were completed, the FBI had paid approximately $400 million for the purchase of these licenses from various manufacturers, including Nortel, Lucent, Motorola, Siemens, and AG Communications.[43] Through its negotiations, the FBI negotiated substantially reduced

[42] In addition, the FBI incurred costs of about $93 million to administer the CALEA program. This included over $77 million in contract costs for the telecommunications technical expertise necessary to administer the program. These administrative costs do not include the significant costs incurred by the FBI to develop "ad hoc solutions" that are used to conduct electronic surveillance on switches where the carrier has not developed CALEA solutions. According to FBI officials, the cost of these ad hoc solutions, which are described in Appendix VIII, exceeded $40 million.

[43] These manufacturers account for over 90 percent of telecommunications equipment lines in the United States. The RTU license agreements specified that the software must pass FBI inspection before being disseminated to carriers. In this regard, the payments and obligations mentioned above include more than $500,000 for carrier assistance in testing the manufacturer's software.

costs for the RTU licenses compared to the initial cost proposals as shown in the following chart:



Source: *Determination and Findings Regarding the Implementation of the Communications Assistance for Law Enforcement Act (1999)*

The FBI also entered into additional RTU license agreements, totaling $50 million, to reimburse carriers for the purchase of RTU Enhanced Dial-Out software licenses from Siemens, Lucent, and Nortel for $19.8 million, $19.6 million, and $10.7 million, respectively.[44] The FBI determined that these RTU license agreements were the most cost-effective vehicles to reimburse the carriers for the use of the manufacturers' software.

As reported in previous OIG audits (see Appendix V), the cost information given to us by the FBI did not provide a basis to determine the reasonableness of the RTU licenses' costs. Accordingly, we offered no opinion.

---

[44] According to the FBI, technical electronic surveillance solutions developed by the telecommunications industry provided a limited set of options regarding transporting intercepted information to law enforcement. Technical electronic surveillance solutions required law enforcement to have in place necessary equipment, facilities, and services to transport intercepted information from a carrier's switching (or delivery) equipment to a collection site. The installation of these facilities (wirerooms) is both time-consuming (if not already in place, they must be ordered weeks or months in advance) and expensive. A "dial-out" solution takes advantage of the PSTN already in place between carrier equipment performing an intercept and a law enforcement collection site, and represented a dramatic departure from then-existing delivery mechanisms. However, as discussed in Finding IV of this report, delivery mechanisms remain an impediment for law enforcement to conducting CALEA wiretaps.

Estimates of CALEA-Compliance Progress

After 10 years and the expenditure of over $450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have the CALEA software activated and thus are considered CALEA-compliant.[45] The basis of the FBI's estimates on CALEA-compliant switches is its analysis of information provided by carriers that participated in the FBI's flexible deployment initiatives.

The FBI's Flexible Deployment Initiatives

Since 2000, the FBI has offered carriers the opportunity to participate in four flexible deployment initiatives that were designed to provide cost savings and operational flexibility to carriers while ensuring that deployment of CALEA solutions would occur. This approach resulted from recognition by the FBI of the challenges facing carriers and represented an attempt to minimize the costs and operational impact of CALEA-compliance on all carriers.

A carrier's participation in the flexible deployment initiatives allowed it to deploy its CALEA solution in accordance with its normal software upgrade cycle. Under the flexible deployment initiatives, the FBI supported a carrier's petition to the FCC for a time extension for complying with a CALEA deadline if the carrier provided the FBI with its projected CALEA deployment schedules for all switches in its network, as well as information pertaining to any recent electronic surveillance activity. The FBI supported the carriers' projected compliance schedules as long as the schedules did not delay the implementation of CALEA solutions in areas of high priority to law enforcement.[46] Carrier extensions have become a source of contention between the FBI and telecommunications industry, and this issue is discussed further in the *Carrier Extensions and Enforcement Orders for*

[45] A carrier's CALEA compliance is not demonstrated simply by installing the CALEA software on a switch. The software must be activated, engineering and provisioning practices developed, security policies implemented, and in some cases, external hardware must be deployed prior to a carrier being able to facilitate surveillance that utilizes the software.

[46] The FBI considers areas with the highest amount of switch intercept activity as high priority. As part of the flexible deployment initiatives, the FBI developed a system to rank the carriers' switches from highest to lowest priority to ensure that the CALEA-compliance of high-priority switches was addressed first.

Non-Compliance section of Finding II.

The chart below details how the four flexible deployment initiatives the FBI offered carriers addressed different FCC deadlines for CALEA-compliance. In addition, the chart details the number of carriers that filed extensions and the number of switches affected under each flexible deployment initiative:

Flexible Deployment Initiatives	Type of Technology Addressed	Opening Date to Participate	Closing Date to Participate	Seeking CALEA-Compliance Extension Until	No. of Carriers Filing Extensions	No. of Switches
FlexD I	wireline/ wireless	Jan. 2000	June 2000	June 30, 2002	1,400	10,784
FlexD II	packet-mode	Aug. 2001	Nov. 2001	Nov. 19, 2003	Canceled[47]	Canceled
FlexD III[48]	wireline/ wireless	May 2002	June 2002	June 30, 2004	607	7,317
FlexD IV[49]	wireline/ wireless	May 2004	June 2004	June 30, 2006	400	1,287

Source: Federal Bureau of Investigation

[47] The FBI discontinued FlexD II because of the scarcity of technical standards for packet-mode systems. Technical standards are discussed in more detail in the *Developing Technical Standards* section of Finding II.

[48] As discussed in the Carrier *Extensions and Enforcement Orders for Non-Compliance* section of Finding II, the FBI advised Verizon, BellSouth, and SBC that it would not support their petitions to the FCC under FlexD III because of their refusal to accommodate law enforcement's high-priority electronic surveillance needs.

[49] The FCC has not ruled on these petitions, even though the FlexD III extensions expired in June 2004.

The FBI estimated that as of June 2000 about 1,400 carriers filed for 2-year extensions with the FCC under FlexD I. These extensions exempted carriers from complying with CALEA during the 2-year period of the extension. Later, carriers filed for additional time extensions under FlexD III and FlexD IV. As part of FlexD IV, only about 400 carriers – as opposed to the original 1,400 carriers who participated in FlexD I – filed for a time extension with the FCC. Therefore, the FBI concluded that the 1,000 carriers who did not participate in FlexD IV must now be CALEA-compliant since they no longer filed for a time extension.

Further, the FBI used the Local Exchange Routing Guide prepared by the telecommunications industry to estimate the universe of wireline switches for the flexible deployment initiatives. Based on the FBI's review of the Routing Guide, it concluded that 80 to 85 percent of the wireline switches were included in the flexible deployment initiatives. According to the FBI, since all switches must be CALEA-compliant, and the carriers for the remaining 15 to 20 percent of the switches did not petition the FCC for an extension, the FBI concluded that those switches are CALEA-compliant.

As straightforward as this methodology sounds, we cannot provide assurance that it provides an accurate estimate for measuring CALEA compliance. We discussed the extent of CALEA compliance with FCC representatives, who stated that the universe of carriers is unknown, even to the FCC. Telecommunications carriers are licensed by states, not the federal government, and the FCC said that state records are not necessarily up-to-date. Therefore, the universe of carriers may not have been fully represented in the FBI's flexible deployment initiatives. In addition, an accurate estimate of the number of carriers participating in the flexible deployment initiatives is difficult to calculate based on FBI data. In particular, the 400 carriers that participated in FlexD IV were not necessarily a subset of the 1,400 that participated in FlexD I.

According to the FCC, some carriers, like Verizon, indicated that they conducted hundreds of wiretaps for the government and always responded to law enforcement's requests. Other carriers indicated that they never conducted wiretaps even though they were capable of doing so because they did not receive any requests. While CALEA directed carriers to become compliant, it did not require them to substantiate their compliance. Therefore, the FCC did not know if carriers were compliant, or whether they were taking a risk that they would not be called upon to respond to a wiretap request.

Therefore, although we acknowledge that the FBI bases its estimates on the best available data, neither the FBI nor the FCC know the actual percentages of CALEA-compliance because there is no requirement for carriers to report the number of switches that are compliant.

Carrier Information on Compliance

During our interviews with carrier representatives, we requested information regarding the number of switches maintained by the carriers and the CALEA-compliance of those switches.[50] The five wireline carriers we interviewed provided the following data regarding the CALEA-compliance of their pre- and post-1995 switches:

Carrier Estimates of CALEA-Compliance for Wireline Switches

Carrier	Pre-1995 Switches	Number CALEA-compliant	Percentage CALEA-compliant	Post-1995 Switches	Number CALEA-compliant	Percentage CALEA-compliant
Wireline A	1,900	0	0%	300	300	100%
Wireline B	634	634	100%	113	113	100%
Wireline C	-	-	-	*270	270	100%
Wireline D	1,311	989	75.44%	380	380	100%
Wireline E	290	1	0.34%	222	222	100%
TOTAL	**4,135**	**1,624**	**39.27%**	**1,285**	**1,285**	**100%**

Source: Carrier representatives

* Wireline C representatives stated that some of its 270 switches may be pre-1995, but, because many of these switches were inherited from other carriers, it is not sure how many.

Specifically, all of the wireline carriers stated that 100 percent of their post-1995 switches were CALEA-compliant, but only one wireline carrier stated that 100 percent of its pre-1995 switches were CALEA-compliant. The other carriers explained that they were awaiting reimbursement from the FBI to begin or complete activation of the CALEA software on their pre-1995 equipment.

We also interviewed representatives from three wireless carriers about the CALEA-compliance of their switches. These carriers maintain only post-1995 switches. All three wireless carriers stated that 100 percent of their switches were CALEA-compliant, as follows:

[50] Carrier names are omitted to protect proprietary information.

Carrier Estimates of CALEA-Compliance for Wireless Switches

Carrier	Post-1995 Switches	Number CALEA-compliant	Percentage CALEA-compliant
Wireless A/B[51]	535	535	100%
Wireless F	174	174	100%
Wireless H	163	163	100%
TOTAL	**872**	**872**	**100%**

Source: Carrier representatives

Some wireless carriers acknowledged that push-to-talk (PTT) service had been introduced without a CALEA solution and that as a result carriers were unable to perform electronic surveillance in some instances. These carrier officials advised that a PTT CALEA solution had recently been deployed in concert with vendors and law enforcement. The FBI, however, considers this to be an interim solution rather than permanent CALEA solution.

Providers of VoIP service stated that they had not received any request to conduct electronic surveillance on VoIP. One VoIP provider we interviewed was actively developing a CALEA solution. Other carrier representatives stated that an electronic surveillance capability that met both the "J-Standard and punchlist" requirements had been developed for their VoIP services.[52]

Prior OIG Audit Report

In our April 2004 report, we recommended that the FBI collect and maintain data on the number of carrier switches that are and are not CALEA-compliant. In response to the recommendation, the FBI noted that absent a regulatory or contractual requirement to submit such data, carriers are under no obligation to provide such information. As part of its *Joint Petition*, DOJ requested that the FCC establish rules to permit the FCC to request information regarding CALEA-compliance. As of November 2005, the FCC had not ruled on this issue.

[51] These wireless carriers merged; therefore, this table presents their combined results.

[52] The J-Standard is the industry published standard to meet the electronic surveillance capability requirements of CALEA. It is discussed in detail in the *Developing Technical Standards* section of Finding II.

In addition, the FBI developed a carrier survey to collect CALEA-compliance information from carriers on a voluntary basis from carriers. According to the FBI, the information collected in the survey will be used to evaluate the effectiveness of FBI programs for implementing CALEA solutions. Affected telecommunications providers will be asked to identify the extent to which they are CALEA-compliant, or the date when full CALEA-compliance will be achieved if they are not compliant. According to the FBI, the survey was mailed to telecommunications providers during November 2005 and requested responses within 60 days.

Conclusion

The FBI's strategy for spending the $500 million in CALEA funding focused on identifying switches in locations of high-priority to law enforcement and first ensuring the CALEA-compliance of those switches. According to FBI officials, its CALEA software deployment estimates are based on carrier participation in the FBI's flexible deployment initiatives. However, we cannot provide assurance that the FBI's methodology provides an accurate estimate for measuring compliance because, according to FCC representatives, the universe of carriers is unknown.

The FBI's estimate that only 10 to 20 percent of the wireline switches had the CALEA software activated is troubling because the technology surrounding the PSTN has been used for over 100 years. However, the FBI has encountered significant challenges in implementing CALEA as discussed in Finding II. As a result of the delayed implementation on wireline switches, the law enforcement community may be limited in the type of information it can gather through electronic surveillance. As discussed in Finding III, switches with activated CALEA software have provided federal, state, and local law enforcement with beneficial features to conduct electronic surveillance. However, these features generally have been realized on wireless rather than wireline systems.

II. IMPEDIMENTS TO IMPLEMENTING CALEA

The FBI has encountered significant impediments in implementing CALEA. These impediments included a contentious process of developing technical standards, continuous carrier requests for extensions and enforcement orders for non-compliance, and extended negotiations with carriers over software activation agreements.

Developing Technical Standards

Electronic surveillance standards provide the basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance. In accordance with CALEA, the FBI consults with carriers and manufacturers to determine what capabilities will be included in the CALEA standards. Developing electronic surveillance standards and obtaining agreement on their content by law enforcement, telecommunications carriers, and equipment manufacturers has been a lengthy process and is the primary reason that CALEA implementation has yet to be completed on wireline equipment.

"Punchlist" Litigation

In June 1996, the FBI issued the Electronic Surveillance Interface (ESI) Document. The ESI set forth law enforcement surveillance capabilities, which were developed in consultation with law enforcement officials and representatives from the telecommunications industry.[53]

In December 1997, an industry standards-setting group published Interim Standard J-STD-025 (J-Standard) to meet the electronic surveillance capability requirements of CALEA. The J-Standard incorporated many of the requirements set forth in the ESI, but excluded several electronic surveillance capabilities deemed

[53] Prior to issuance of the ESI, the FBI had issued electronic surveillance capabilities in both 1994 (prior to the enactment of CALEA) and 1995. These documents contained the punchlist capabilities.

necessary by law enforcement.[54] As a result, DOJ filed a deficiency petition with the FCC in March 1998 because the J-Standard did not meet the nine capabilities (punchlist) that law enforcement was seeking (see Appendix IV - Public Notice dated April 20, 1998).[55]

In September 1998, the FCC granted an extension to carriers for complying with CALEA capability requirements (see Appendix IV - Memorandum Opinion and Order dated September 10, 1998). For equipment installed or deployed after January 1, 1995, the FCC extended the deadline from October 28, 1998, to June 30, 2000. The FCC granted this extension because no technology available permitted carriers to deploy the minimum industry-developed J-Standard. According to CALEA, carriers are deemed to be CALEA-compliant with respect to equipment installed or deployed on or before January 1, 1995, unless the FBI agrees to reimburse carriers for all reasonable costs necessary to bring such equipment into compliance.

[54] According to the June 13, 2002, *Petition for Further Extensions of Time of CALEA Deadlines* filed on behalf of Qwest Corporation; Malheur Home Telephone Company; Qwest Wireless, LLC; and TW Wireless, LLC; the "core" J-Standard provided law enforcement approximately 95 percent of the capabilities required by CALEA.

[55] The nine punchlist capabilities are to: (1) provide the content of subject-initiated conference calls supported by the subject's service, (2) identify the active parties of a multi-party call, (3) provide access to all dialing and signaling information available from the subject including a subject's use of features (e.g., the use of flash-hook and other feature keys), (4) notify the law enforcement agency when a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy), (5) provide timing information to correlate call-identifying information with the call content of a communications interception, (6) provide digits dialed by the subject after the initial call "cut-through" is completed to another carrier, (7) send a message to a law enforcement agency that an interception is still functioning on a subject, (8) alert the law enforcement agency via electronic continuity-check tone if the facility used for delivery of call content has failed or lost continuity, and (9) notify the law enforcement agency if the subject modifies his subscribed features.

In August 1999, the FCC ruled that carriers must comply with six of the nine punchlist requirements sought by the FBI and not included in the J-Standard (see Appendix IV – Third Report and Order dated August 26, 1999).[56] The FCC also mandated that carriers provide the capability to intercept packet-mode communications by September 30, 2001. The telecommunications industry appealed the FCC's decision to the U.S. Court of Appeals for the District of Columbia Circuit.

On August 21, 2000, the Court of Appeals remanded four of the challenged punchlist features to the FCC for further proceedings. In an April 11, 2002, Order on Remand, the FCC reiterated its August 1999 decision that all six punchlist capabilities were required under CALEA and must be provided by wireline, wireless, and broadband carriers by June 30, 2002.

Current Standard-Setting Efforts

To ensure that carriers meet their CALEA responsibilities and to promote effective liaison with the telecommunications industry, the FBI participates in several domestic and international standards-setting groups. As part of these groups, the FBI educates carriers and manufacturers about law enforcement's technical assistance capability requirements, and informs the carriers and manufacturers of their CALEA responsibilities with regards to emerging technologies.

The FBI has been, or is currently, involved in several domestic standards-setting groups, including:

[56] The FCC ruled that carriers must comply with punchlist items 1 through 6 identified in footnote 55 and described in more detail in Appendix IX.

Standards Group	Service Type	Type of Technology
Alliance for Telecommunications Industry Solutions	Voice	Wireline
		Universal Mobile Telecommunications System/General Packet Radio Service
	Data Access	Wireline
		Universal Mobile Telecommunications System/General Packet Radio Service
	Push-to-talk	Universal Mobile Telecommunications System/General Packet Radio Service
Telecommunications Industry Association	Voice	Wireline/Wireless
		Code Division Multiple Access 2000
	Data Access	Code Division Multiple Access 2000
	Push-to-talk	Code Division Multiple Access 2000
American Association of Paging Carriers	Paging	Traditional Paging, Advanced Messaging, and Ancillary Services
American Mobile Telecommunications Association	Push-to-talk	Enhanced Specialized Mobile Radio

Source: The Federal Bureau of Investigation

In addition, the FBI has been involved with international standards groups, including the European Telecommunications Standards Institute, the International Softswitch Consortium, and the Third Generation Partnership Project. An FBI official explained that the FBI participates in these groups because many of the equipment manufacturers are based in countries other than the United States. The FBI focuses its involvement in standards groups for technologies in which law enforcement has encountered problems. For example, the FBI does not participate in a standards group addressing satellite telephony because law enforcement has not reported electronic surveillance difficulty with this technology.

Due to the rapid emergence of packet-mode technology and the associated introduction of VoIP and broadband services to the public, the FBI is primarily devoting its resources to setting electronic surveillance standards for packet-mode technologies. As part of this approach, beginning in 2001 the FBI issued three documents setting forth some of law enforcement's needs with regard to electronic surveillance in a packet mode environment: Packet Surveillance

Fundamental Needs (PSFN), Carrier Grade Voice over Packet (CGVoP), and Public Internet Protocol Network Access Services (PIPNAS). The PSFN was issued in October 2001 to define the general requirements necessary for the effective delivery of both call-identifying and content data.[57] The CGVoP was issued in January 2003 to define what call-identifying and content data requirements are needed by law enforcement.[58] The PIPNAS was issued in September 2003 to set forth law enforcement needs for access to public Internet Protocol (IP) networks and the necessary infrastructure support services.[59]

Work on a packet-mode electronic surveillance standard, J-STD-025B (25B standard) began in October 2001. The 25B standard is only for wireless broadband data access service and was prepared by the Telecommunications Industry Association's (TIA) TR45 Lawfully Authorized Electronic Surveillance Ad Hoc Group. The FBI initially participated in the 25B standard setting effort, but withdrew in February 2003 from active participation in this process. According to FBI officials, their opinion of a proposed standard only counts as one vote at these standard-setting groups, and their contributions to the process were rejected several times. The FBI is considering filing a deficiency petition with the FCC over this standard, as well as for wireline VoIP, wireless VoIP, and wireless broadband access, due to

---

[57] According to the FBI, the PSFN document neither addressed any procedures for enabling access to a subject's communications nor requirements for how call-identifying information is accessed in a service provider's network. Rather, the document provided a set of high-level needs considered necessary by law enforcement regardless of the service being offered by the provider over a packet-based network. The PSFN Document did recognize that each packet-based service would require a more detailed set of needs based on the specifics of the service and architecture.

[58] According to the FBI, this document defined what communications-identifying information and communications content are needed by law enforcement to conduct electronic surveillance, but did not define how a service provider should access that information. CGVoP service can be defined as the utilization of packet technology to offer voice services that parallel the services provided through the PSTN and that strive to achieve quality, reliability, security, and connectivity comparable to the PSTN.

[59] Personal communication has traditionally been carried via wireline circuits. Advances in computer hardware and software technology have enabled personal communications to be carried via data packets over a network. This method of communication requires both access to a public IP network (e.g., the Internet) and accompanying network infrastructure support services. Network access can be attained from a PIPNAS provider and the necessary network support services can be provided by a PIPNAS provider, application service provider, local exchange carrier, wireless service provider, or some combination thereof.

the standards groups' failure to develop a CALEA standard for these technologies that is acceptable to law enforcement. Despite the FBI's belief that the 25B standard is deficient, some carriers we spoke with noted that it is the only official packet-mode standard available and therefore they are upgrading their systems to comply with the 25B standard.

Carrier Representatives

Carrier representatives noted the following problems with the standards development process:

- Slow Vendor Development Time. According to one carrier, CALEA software solutions development time is generally 18 to 24 months. Therefore, the sooner law enforcement requirements are defined, the sooner CALEA electronic surveillance capabilities can be developed and deployed. Some carrier officials expressed frustration with what they viewed as the slow development of law enforcement requirements. One carrier official stated that the FBI should focus its efforts more on the development of law enforcement requirements and less on the development of ad hoc solutions. An FBI official noted that it is important for the FBI to focus its efforts in both areas because, in some instances, there are no alternative carrier or manufacturer solutions available to conduct the requested electronic surveillance. According to state and local law enforcement officials, the development of ad hoc solutions primarily benefits federal law enforcement because the FBI is not always able to share its technology with state and local law enforcement.[60] Officials representing a wireless carrier viewed the FBI's development of ad hoc solutions as a hindrance to the development of CALEA solutions because carriers and manufacturers do not always have access to these solutions to understand what hardware and software is needed.

[60] Attorney General Order 1945-95 states in part: "It is the policy of the Department of Justice that the loans of electronic surveillance equipment to state and local law enforcement agencies are generally to be discouraged. . . ." The order also states that a "State agency receiving loaned equipment may not disclose the existence or use of such equipment without authority of the FBI Director. . . ." According to the FBI, state and local recipients of FBI ad hoc solutions cannot always protect the details of this sensitive law-enforcement technique against subsequent criminal discovery.

- Lack of an Adequate Forum. Carrier officials explained that there was not an adequate forum available for law enforcement, carrier, and manufacturer representatives to meet and discuss mutual concerns. (Law enforcement personnel we interviewed also shared these concerns, which we discuss in Finding IV.) One carrier official noted that carrier and manufacturer's technical staff need to hear law enforcements' concerns firsthand to understand how new technologies impact investigations. The underlying problem often is not understood by the technicians and the result is often that law enforcement needs are viewed as overreaching. Another carrier official stated that current industry standards groups are too technically oriented for law enforcement.

- Flawed CALEA Solutions. Carrier officials stated that in the past, manufacturers provided flawed CALEA solutions that a carrier had to fix later at significant expense. Carrier officials suggested that the federal government provide a facility for manufacturers to test CALEA solutions prior to dissemination to carriers.[61] These officials believe that current standard-setting bodies are not good vehicles for this process because they are primarily concerned with standards for commercial applications for the telecommunications industry. Carrier officials said that CALEA is not a high-priority to standard-setting groups and carriers are dependent on the equipment vendors to deliver CALEA-compliant solutions each time a new feature or service is offered. They also stated that only the federal government has the clout to ensure that vendor-developed equipment and software meet CALEA requirements.

[61] CALEA solutions are developed by engineers who rely on telecommunications industry published standards to guide them. According to an FBI official, "[s]ince CALEA standards are intentionally broad, this causes software developers to sometimes incorrectly assume the intent of the standard." Complicating the development process is the fact that a different CALEA solution is needed for every combination of carrier and manufacturer in the telecommunications industry, and that some carriers use different manufacturers for the same equipment in different parts of the country.

- Acceptance of Standards. Representatives from one carrier noted that the FBI appears to oppose the acceptance of standards until all of its requirements are accepted, and this ultimately slows progress. According to these representatives, the FBI may benefit more if it progressed slowly through the standards process instead of requesting "everything" in the beginning which some manufacturers and carriers may oppose. For example, one representative stated that the FBI should start with base requirements, get them approved, and then move to addendums that add more requirements and capabilities.

FBI Response to Carriers' Comments

The FBI concurred that the standards development process is slow, and offered comments in the following areas:

- Industry Controls the Standards-Development Process. The FBI agreed that the standards development process is slow and contentious. According to the FBI, law enforcement's electronic surveillance needs are known to industry standards groups and only change to reflect the changes made in services offered by providers. For example, law enforcement's need for location information is non-existent in a wireline environment but paramount for a wireless service. As a service provider offers more features, a provider's ability to furnish information regarding those features may need to increase. However, CALEA gives the lead role in setting electronic surveillance standards to the telecommunications industry. This delegation has created considerable tension between the FBI and the telecommunications industry throughout the standards development process. In its CALEA Implementation Plan of August 2003, the FBI discusses providing greater authority to law enforcement for determining technical requirements. According to the FBI, CALEA allows the telecommunications industry to decide what law enforcement needs. If the FBI believes a standard is deficient, it has to challenge the standard by filing a deficiency petition with the FCC. Instead of having to explain why law enforcement needs a particular feature or service, the FBI's preference would be to place the onus on the telecommunications industry to explain why a feature or service that law enforcement wants is not feasible.

- Forum for Discussing Law Enforcement Requirements. The FBI said that the current state of interaction between the telecommunications industry and the FBI is the result of continuous evolution. Over the last decade, various forums have been held regarding the CALEA required capabilities such as telecommunications industry sponsored legal summits, the FBI sponsored Service Specific Document Summits, and conferences and summits held by various organizations (industry and privacy groups). These meetings have allowed participants to express their views – often contentious and contradictory to each other.

- Testing CALEA Solutions. An FBI official believes that the FBI is best suited to test technical solutions from a law enforcement perspective. If, however, the FBI agrees to the carriers' suggestion that it oversee testing, then it is important to define the nature of that testing. Testing for all permutations of the effects of manufacturers' solutions within all providers' networks would impose an enormous burden. Also, it is important to consider how testing is conducted for other services and features made available by equipment manufacturers. For example, large carriers such as Verizon have staffs devoted to extensive testing of the effects of manufacturer-supplied software. For smaller carriers or members of the cable industry, testing has been conducted by the telecommunications industry on a consortium basis. For example, the telecommunications industry often used Telcordia Technologies, Inc. to conduct testing on manufacturer software, and the cable industry used CableLabs to test equipment and software.[62]

  The FBI stated that the question of adequate testing may best be answered by government-sponsored testing using existing industry mechanisms. For example, FBI-facilitated testing would provide key benefits such as learning how each solution works and the impact solutions have on law-enforcement

[62] Telcordia Technologies, Inc. is a provider of telecommunications network software and services for IP, wireline, wireless, and cable companies. CableLabs is a research and development consortium of cable television system operators that conducts and funds research and development projects to help cable companies plan for the future and apply technology to meet consumers' needs.

collection equipment.[63] Unfortunately, CALEA does not provide funding for such testing. In addition, the FBI believes that certain legal issues may need to be addressed before such testing could occur. The FBI stated that most carriers test solutions on their own networks or on test networks populated with stored data. In the past, proposals for FBI participation in testing have raised concerns that such participation could be characterized as involving the interception of either real-time or stored communications of a carrier's subscriber. Although not problematic for the carrier who has broad interception authority if necessarily incident to the rendition of a service, there is no statutory exemption in Title III that authorizes law enforcement to conduct, or participate in, intercept testing that involves real-time or stored subscriber communications. Therefore, it is unclear whether a statutory amendment would be required in order to provide the FBI with authority to conduct, or participate in, CALEA testing that involves real-time or stored subscriber communications.

- Success with Individual Telecommunications Providers. Although the CALEA standard development process has been slow and contentious, the FBI believes that it has been successful in discussions with individual providers and manufacturers. This is because of the inherent desire on the part of these companies to keep proprietary equipment and network information closely held. For example, an ISP representative noted that his company was launching a VoIP service that was in testing at the time of our audit. According to this representative, his company worked closely with the FBI to ensure that VoIP-CALEA requirements were integrated into its service.

Carrier Extensions and Enforcement Orders for Non-Compliance

Two controversial issues regarding CALEA implementation are carrier extensions and enforcement orders for not complying with CALEA.

[63] The FBI funded testing of solutions only in connection with the nationwide RTU licenses as a contractual condition and not as a part of a comprehensive testing regimen.

Carrier Extensions

Under CALEA, the FCC has the power to grant carriers extensions for complying with the CALEA capability requirements. Section 107 of CALEA provides for time extensions for complying with the statute for up to two years if the FCC determines that compliance is not reasonably achievable through available technology. Under Section 109, if the FCC finds that compliance is not reasonably achievable, the Attorney General may, upon petition of the carrier, agree to pay the carrier to make the modifications in order to make compliance reasonably achievable. If the Attorney General does not agree to pay these costs, the carrier will be deemed in compliance with the capability requirements.[64] Unlike Section 107, there is no maximum time limit on Section 109 extensions. Since June 2000, the FCC has granted hundreds of Section 107 extensions in conjunction with the FBI's flexible deployment initiatives, but never has granted a Section 109 extension.

The Section 107 extensions that were granted to carriers by the FCC are a source of contention between the FBI and the telecommunications industry. According to the FBI, carriers can delay the implementation process by continuing to seek extensions from the FCC. The FCC first issued extensions to wireline and wireless carriers for complying with CALEA until June 30, 2002, and then to June 30, 2004. Furthermore, in 2004 carriers began filing for time extensions for complying with CALEA until June 30, 2006.

Despite the FBI's concerns, carriers argued that extensions were warranted. For example, SBC noted in one of its petitions for an extension that:

[64] In granting a Section 109 extension, the FCC also considers the following factors: (1) the effect on public safety and national security; (2) the effect on rates for basic residential telephone service; (3) the need to protect the privacy and security of communications not authorized to be intercepted; (4) the need to achieve the capability assistance requirements of Section 1002 of this title by cost-effective methods; (5) the effect on the nature and cost of the equipment, facility, or service at issue; (6) the effect on the operation of the equipment, facility, or service at issue; (7) the policy of the United States to encourage the provision of new technologies and services to the public; (8) the financial resources of the telecommunications carrier; (9) the effect on competition in the provision of telecommunications services; (10) the extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995; and (11) such other factors as the Commission determines are appropriate.

In conversations with the FBI, SBC has been led to believe that the FBI will assert that there are no technical reasons why the Siemens Plan C solution cannot be accepted and deployed by SBC. SBC strongly disagrees, and submits that its technical experts are better suited to judge the compatibility of any proposed CALEA solution with SBC's network. It is SBC's understanding that the FBI's opinion is based on testing conducted with a small rural carrier, whose network architecture, personnel, maintenance, and security concerns are vastly different in nature and scope than those faced by SBC. SBC also respectfully suggests that CALEA itself prohibits the FBI or any other government agency from dictating SBC's network architecture, and that forcing adoption of a solution deemed currently unacceptable by SBC's network experts would amount to exactly that.[65] *SBC has worked in good faith with all concerned parties for over a year in an attempt to make the Siemens solution viable for SBC's network, and will continue to do so. Nevertheless, because significant issues remain untested at this time, compliance with CALEA's requirements in SBC's Siemens switches by June 30, 2002 is not reasonably achievable.*

A telecommunications industry representative noted that while the FBI blames the FCC for granting carriers repeated extensions, the FBI approached the FCC and suggested the flexible deployment initiatives. He also noted that the extensions were approved in conjunction with the FBI's flexible deployment initiatives, and that an implementation strategy that included hundreds of extensions was "good enough at the time" for the FBI.

In response to the requests for Section 107 extensions, DOJ requested in its *Joint Petition* that the FCC outline criteria for granting both Section 107 and Section 109 extensions for future covered technologies. In response to DOJ's request, the FCC in its Notice of Proposed Rulemaking (NPRM) proposed limiting the availability of time extensions by:

- Restricting the availability of compliance extensions under Section 107, particularly in connection with packet-mode requirements.

[65] 47 U.S.C. § 1002(b).

- Seeking comments regarding supporting information and documentation that should accompany Section 107 petitions if carriers are not participating in the flexible deployment initiatives, if the FBI opposes the petition of a carrier participating in the program, or if the FBI were to terminate the flexible deployment initiatives.

- Tentatively concluding that the requirements of Section 109 would not be met by a petitioning carrier that merely asserted that CALEA standards had not been developed, or that solutions were not readily available from manufacturers. The FCC noted that if standards or solutions do not exist, the petitioning carriers would still need to demonstrate why they could not negotiate system-specific CALEA solutions with manufacturers or with third-party CALEA service providers.

- Tentatively concluding that carriers may not assert the lack of available standards or solutions to support a showing under Section 109. Instead, carriers filing Section 109 petitions will be expected to demonstrate active and sustained efforts at developing and implementing CALEA solutions for their operations. In addition, the FCC tentatively concluded that it should require Section 109 petitioners to submit detailed information about discussions and negotiations with switch manufacturers, other equipment manufacturers, and third-party CALEA service providers, both before and after the FBI announced the termination of the flexible deployment initiatives in connection with packet-mode technology. Furthermore, the FCC tentatively concluded that unless it was persuaded that petitioners have engaged in sustained and systematic negotiations with manufacturers and third-party providers to design, develop, and implement CALEA solutions, it should reject the submitted petitions.

Enforcement Orders for Non-Compliance

Until this point, the FBI's pursuit of legal remedies for carrier non-compliance with CALEA has not included filing enforcement actions. Under Section 108 of CALEA, an order enforcing CALEA may be issued by the court that approved the electronic surveillance order with which the carrier failed to comply or upon the application of the Attorney General through a civil action. Enforcement orders may only

be issued if a court finds that: (1) another carrier's facilities are not reasonably available to conduct the authorized electronic surveillance, and (2) the electronic surveillance is reasonably achievable with available technology.[66] A court issuing an enforcement order must allow reasonable time for compliance and may impose a civil penalty not to exceed $10,000 per day for each day of violation of the enforcement order.

The FBI explained that it has not sought enforcement orders for two reasons: (1) pre-1995 equipment is deemed CALEA-compliant until the FBI agrees to reimburse carriers for their deployment costs, and (2) post-1995 equipment has been covered under FCC time extensions that were granted because CALEA-compliance was not reasonably achievable through existing technology. FBI officials summed up the current status by saying that it cannot file suit to enforce CALEA because the carriers currently do not have to comply with the law given the extensions. Instead, the FBI is asking the FCC to use the enforcement powers it has been granted under the Communications Act of 1934 to compel carriers to comply with the FCC-imposed deadlines. According to FBI personnel, the FCC has used these enforcement powers over carriers for other purposes, such as enforcing local number portability and enhanced 911 service.

Telecommunications industry representatives cited law enforcement's failure to file these enforcement actions as evidence that carrier non-compliance is not a concern. Specifically, one industry representative noted that:

> *[d]espite the crisis atmosphere fostered by the government, the Justice Department and law enforcement have never once used the enforcement powers that CALEA gives them. The only logical conclusion is that there has never been a single case – not one, not anywhere in the country, and not at any time in the last decade – in which the Justice Department thought it could prove that a carrier had failed to meet its CALEA obligation and that important evidence was being lost as a result.*

[66] A carrier could defend itself by showing that full wiretap capability was not reasonably achievable in its system, or that law enforcement could obtain the same information elsewhere.

This representative also indicated that carriers were not protected from enforcement action because the FCC had not ruled on the latest extension requests. However, several state and local law enforcement agencies said their failure to file CALEA enforcement actions was a matter of practicality. If they already know a carrier does not have the ability to conduct the electronic surveillance, the agency does not bother going through the trouble and expense of obtaining the court order. In addition, one local law enforcement official noted that although a local judge would be willing to issue an Order to Show Cause against a carrier, the agency would have to wait three months for a hearing. Given that the intercept is needed immediately, the official said the law enforcement agency instead will often pursue a traditional wiretap.[67]

Accordingly, in its *Joint Petition*, DOJ requested that the FCC establish procedures for FCC enforcement actions against entities that do not comply with their CALEA obligations. In the proposed rulemaking, the FCC sought comment from interested parties on how it could enforce the CALEA assistance capability requirements. In addition, the FCC sought comment on whether its general enforcement procedures were sufficient for purposes of CALEA enforcement.

Activation Negotiations on Pre-1995 Equipment

As noted in Finding I, entering into the RTU agreements did not guarantee that CALEA-compliant solutions were made operable and available for use by law enforcement. The agreements only ensured that the RTU licenses for CALEA software were made available to carriers; additional monies are needed to fully deploy the solutions.[68] While some wireline carriers stated that the RTU software had been activated on pre-1995 equipment in whole or in part, other carriers explained that they were awaiting reimbursement from the FBI to begin or complete activation of the RTU software on their pre-1995 equipment. During mid-2003, the FBI began negotiating reimbursement agreements with four carriers for the cost of deploying

---

[67] CALEA offers additional features not available through a traditional wiretap. These additional features are the “punchlist” features described in Appendix IX.

[68] CALEA software is considered deployed when it is activated, engineering and provisioning practices developed, security policies implemented, and in some cases, external hardware is deployed prior to a carrier being able to facilitate surveillance that utilizes the software.

CALEA solutions on their pre-1995 equipment.[69]

According to the FBI, it concluded negotiations with two carriers in September 2005 for a total cost of $4.5 million. The first carrier agreed to the FBI's counter-offer of $2.9 million to cover 1,158 switches (including dial-out solution software) for an average per switch price of $2,530. The second carrier agreed to the FBI's counter-offer of $1.6 million for 667 switches (including dial-out solution software) for an average switch price of $2,410.

The FBI temporarily discontinued negotiations with the two other carriers. According to the FBI, substantial personnel turnover at the third carrier has made negotiations difficult and discussions were postponed. The negotiation process recently resumed with this carrier. The FBI has also discontinued negotiations with the fourth carrier because they said the carrier's initial proposal of $170 million appears to be completely unjustified and it far exceeded the amount of the remaining CALEA funding.

Conclusion

The FBI has encountered significant challenges in implementing CALEA. Although new technologies that blur the historical boundaries of telecommunications have emerged, the FBI continues to implement CALEA on wireline systems. The development and implementation of the initial standards, which was slowed significantly by litigation, is the primary reason implementation has been delayed. In addition, repeated requests from carriers for time extensions has been a controversial issue to CALEA implementation. As further discussed in Finding III, the anticipated benefits of CALEA on wireline systems have not materialized.

Recommendation

We recommend that the FBI:

1. Coordinate with the DOJ and the telecommunications industry to determine the legality and feasibility of FBI-sponsored development and testing of manufacturers' CALEA solutions prior to their dissemination to carriers.

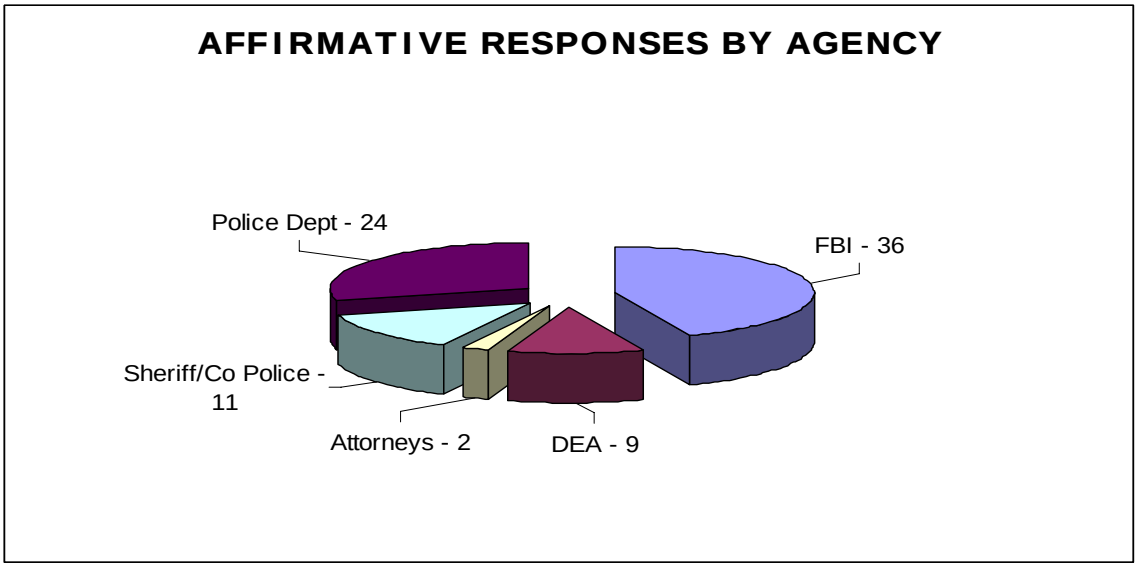
[69] The FBI estimates that entering into software activation agreements with these four carriers would make about 90 percent of the wireline switches CALEA-compliant.

III. EFFECTS OF DELAYED CALEA IMPLEMENTATION

CALEA has provided the law enforcement community with beneficial features to conduct electronic surveillance, and has greatly reduced the amount of time it takes to initiate a wiretap. However, these features generally have been realized on wireless rather than wireline systems. Nevertheless, we believe the following factors mitigate the effects of the slow implementation on wireline systems: (1) the growing popularity of Internet telephony, (2) the limited number of wireline intercepts, (3) the apparent limited effect on criminal investigations, and (4) emerging technologies. With the remaining $45 million in CALEA funding, the FBI plans to reimburse major wireline carriers for activating the CALEA solution software on their systems. However, considering the changing dynamics of the telecommunications industry and the fact that almost 90 percent of intercepts are conducted on wireless systems, we believe the FBI should reexamine the future benefits of activating CALEA software solutions on wireline systems before expending any additional funding in that effort.

Methodology for Measuring CALEA's Impact

We reviewed the FBI's methodology for measuring CALEA's impact and identifying issues and concerns that affect law enforcement's ability to conduct electronic surveillance. In addition, we interviewed federal, state, and local law enforcement officials from five states who had switches that were identified as high-priority by the FBI, and who were provided coverage by a different carrier in each state. We also prepared a written survey that was mailed to 1,396 federal, state, and local law enforcement officials regarding their electronic surveillance activity and use of CALEA features (see Appendix X for a copy of the survey). Of the 723 responses we received to our survey, 82 agencies from 38 states indicated they conduct electronic surveillance. The following chart illustrates the affirmative responses by agency:



Source: Law enforcement responses to the OIG survey

Of the 723 responses received, 641 (89 percent) agencies said they did not conduct electronic surveillance in 2004. The agencies indicated that they did not conduct electronic surveillance for the reasons illustrated below:

NEGATIVE RESPONSES

AGENCY	NEGATIVE RESPONSES	REASON DID NOT CONDUCT ELECTRONIC SURVEILLANCE				
		NOT NECESSARY	COULD NOT AFFORD	CARRIER UNABLE TO CONDUCT	DON'T KNOW HOW TO CONDUCT	OTHER
FBI	0	0	0	0	0	0
DEA	0	0	0	0	0	0
ATTORNEYS	87	80	7	0	11	0
SHERIFF/CO POLICE	107	83	32	1	17	0
POLICE DEPT	447	363	107	7	65	2 (MANPOWER)
TOTAL	**641**	**526**	**146**	**8**	**93**	**2 (MANPOWER)**
%		**82.06%**	**22.78%**	**1.25%**	**14.51%**	**0.31%**

Source: Law enforcement responses to the OIG survey

As shown above, FBI and DEA officials responding to the survey indicated that they conducted electronic surveillance in 2004 while responses from 82 percent of the state and local officials indicated that electronic surveillance was not necessary in their cases. Additionally, 23 percent of the state and local agencies responding to the survey indicated that electronic surveillance was not affordable.

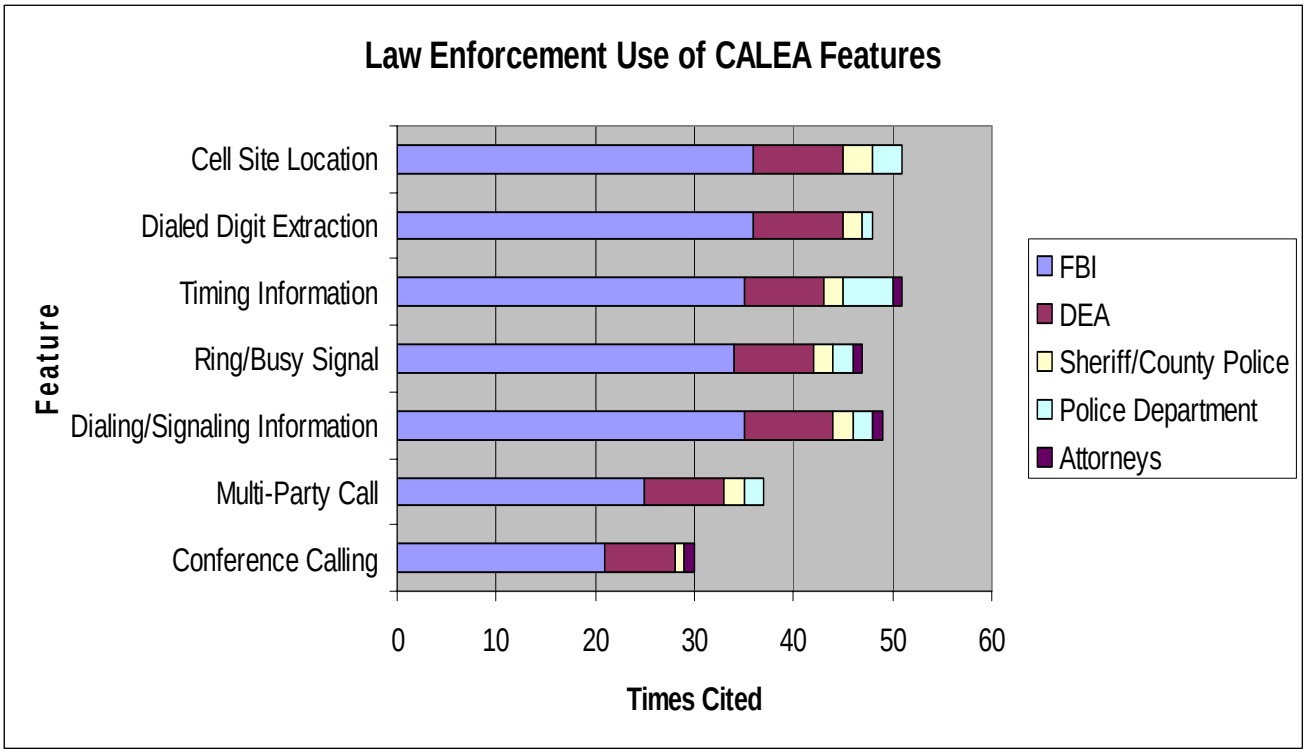
Benefits of CALEA

For the switches with activated CALEA software, we found that CALEA has provided federal, state, and local law enforcement with beneficial features to conduct electronic surveillance, and has greatly reduced the amount of time it takes to initiate a wiretap.

CALEA Punchlist Features

As discussed in Finding II, the primary reason for the delayed implementation of CALEA was the litigation over the punchlist features. As noted in Qwest's June 13, 2002, *Petition for Further Extensions of Time of CALEA Deadlines*, the punchlist features represented 5 percent of the capabilities required by law enforcement. We surveyed law enforcement to determine the extent various CALEA features are utilized.[70] Of the 82 agencies that responded that they performed electronic surveillance, the following chart shows a breakdown of law enforcement's use of the CALEA features:

[70] For a description of the CALEA punchlist features, see Appendix IX.



Source: Law enforcement responses to the OIG survey

Timeliness of Electronic Surveillance

Law enforcement officials stated that CALEA greatly reduced the amount of time it took carriers to initiate a wiretap once a court order was accepted by the carrier. For example, a New York law enforcement official noted that his agency can now initiate a wiretap on a wireless phone within a day. He also said that the carriers have greater capacity to conduct more wiretaps simultaneously. This was reiterated by one carrier official, who noted that prior to deployment of the CALEA solution, provisioning (the providing of electronic surveillance service by the carrier) of electronic surveillance was time-consuming and expensive. In addition, both carrier and law enforcement officials had to be physically present at the switch location during the electronic surveillance, and previously it could take up to several weeks to receive intercept data from a carrier.

With the implementation of CALEA, provisioning is completed remotely from a central location for all electronic surveillance in a carrier's network. This process has significantly reduced carrier and law enforcement travel costs and time, and has facilitated electronic surveillance. Under CALEA, law enforcement agencies can now make a single connection to the carrier's network, and can deal with carrier

staff whose positions are dedicated to provisioning electronic surveillance. These changes mean that law enforcement agencies have faster access to electronic surveillance data, often within a day.

Mitigating Factors

We believe the following factors mitigate the effects of the delayed implementation on wireline systems.

Growing Popularity of Internet Telephony

Internet telephony and Internet telephony service providers are a growing segment of the telephone industry. An April 2005 report from research firm International Data Corporation (IDC) predicts that U.S. residential VoIP customers will grow from 3 million in 2005 to 27 million by the end of 2009. An example of this trend is Comcast Corporation, which is the nation's largest cable company. Comcast plans to offer its Internet-based phone service to its 28 million cable and high-speed Internet customers by mid-2006. In addition, a carrier representative we interviewed reiterated a widely held belief that the Internet will swallow up the conventional telephone network, and that Internet Telephony will essentially replace traditional telephone service in the United States in the near future.

Limited Number of Wireline Intercepts

According to the April 2005 *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*, the most common location specified in wiretap applications authorized in 2004 was "portable device, carried by/on individual."[71] According to the report, 88 percent of all wiretaps authorized involved portable devices such as portable digital pagers and cellular telephones. The report noted that since 2000 – the first year that the "portable device, carried by/on individual" category was

[71] The Omnibus Crime Control and Safe Street Act of 1968 required the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The statute requires that specific information be provided to the AO, including the offense(s) under investigation; the location of the intercept; the cost of the surveillance; and the number of arrests, trials, and convictions that directly result from the surveillance.

used – the proportion of wiretaps involving fixed locations has declined as the use of mobile communications devices has become more prevalent.[72] The report also noted that only 5 percent of all intercept devices were authorized for personal residences, and 2 percent were authorized for business establishments such as offices, restaurants, and hotels.

In addition, our discussions with four wireline carriers in areas of the country with high amounts of intercept activity revealed that from 2002 to 2004 a limited number of court orders for wiretaps requiring CALEA features were requested:

- Wireline A. 1.2 percent of the court orders it received for intercepts required CALEA features.

- Wireline B. Less than 1 percent of the court orders it received for intercepts required CALEA features.

- Wireline D. 6.25 percent of the court orders it received for intercepts required CALEA features.

- Wireline E. 3.5 percent of the court orders it received for intercepts required CALEA features.

According to the Federal, state, and local law enforcement officials we interviewed and surveyed, their agencies do not request intercepts requiring CALEA features for several reasons (i.e., the high cost charged by carriers, carrier noncompliance, or the investigation only required a traditional wiretap).

The Apparent Limited Effect on Criminal Investigations

The FBI measures the investigative impact of CALEA and identifies issues and concerns of law enforcement in a variety of ways. Representatives from the FBI speak with law enforcement at various events including the FBI's Law Enforcement Technical Forum, the FBI's Law Enforcement Executive Forum, meetings of the International Association of Chiefs of Police, and meetings of the Law Enforcement

[72] The FBI acknowledged that over 80 percent of intercepts are conducted on cellular or wireless switches.

Executive Development Association.[73] During these events, FBI officials said that law enforcement representatives raise with them issues that affect their ability to conduct electronic surveillance, such as carrier compliance and emerging technologies. Federal, state, and local law enforcement representatives also convey their issues and concerns through Threat Assessment Surveys distributed by the FBI.

The FBI also measures the impact of CALEA on law enforcement by reviewing help desk reports. The FBI maintains a help desk that law enforcement officials can call when they have difficulty conducting electronic surveillance or if they have questions. In addition, the FBI website (www.askcalea.net) provides a help desk database that describes difficulties encountered with CALEA solutions. Law enforcement officials can submit problems to the help desk, such as difficulties they encounter while conducting a CALEA intercept. Law enforcement officials can review the help desk's database to determine if other law enforcement agencies have encountered the same difficulty and identify what action was taken.

FBI's Threat Assessment Survey

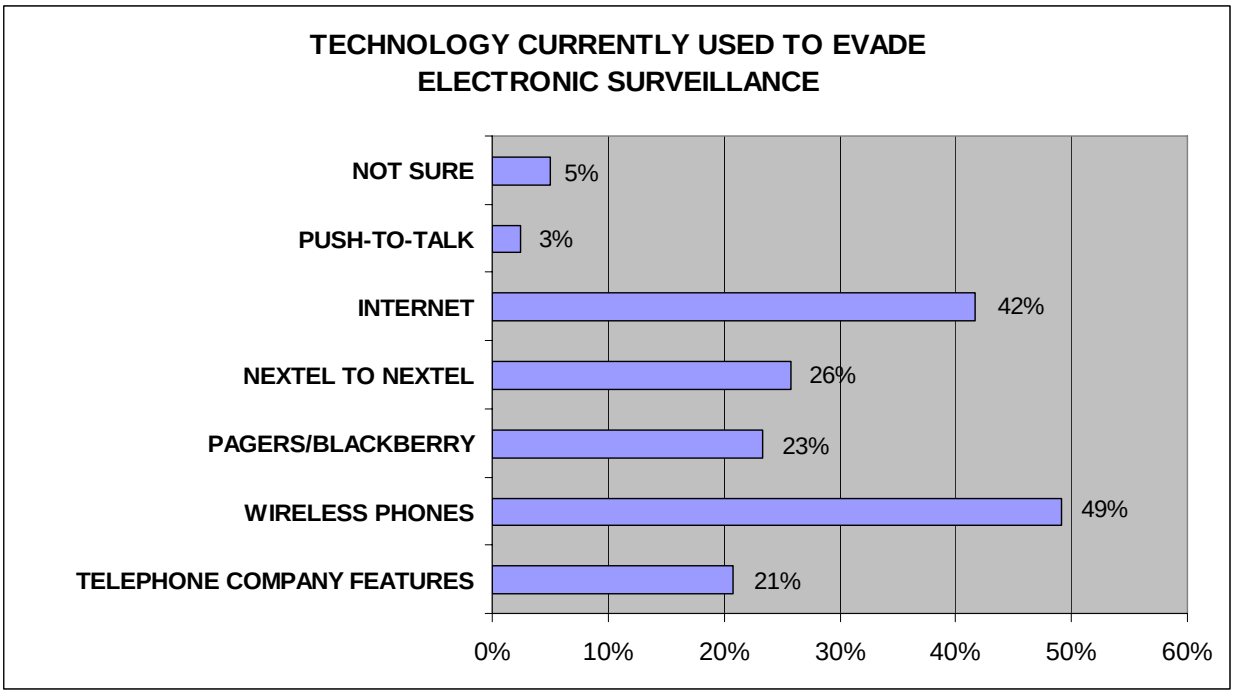
We reviewed the FBI's 2004 Threat Assessment Survey Report and the individual threat assessment surveys used to prepare the report. The 2004 Threat Assessment Survey was developed to better understand and anticipate future threats to law enforcement. The survey was conducted from November 2003 through September 2004 at the national and regional meetings of the National Technical Investigator Association, and at various DEA and FBI training sessions.

Our review of the surveys found that they are useful in helping the FBI measure CALEA's impact and for identifying issues and concerns that affect law enforcement's ability to conduct electronic surveillance. However, the number of survey participants was limited, and therefore may not adequately represent the full law enforcement community.

The FBI collected 120 surveys from federal, state, and local law enforcement officers from 57 different federal, state, and local agencies and departments. Our review of the surveys revealed that 77 of the 120 participants (64 percent) indicated that criminals have

[73] The FBI formed the Law Enforcement Technical Forum and the Law Enforcement Executive Forum to solicit the technical and programmatic exchange of information with the law enforcement community on CALEA implementation and electronic surveillance challenges.

the ability to evade law enforcement's electronic surveillance efforts. Of the 120 participants, 59 participants (49 percent) believed that criminals evaded surveillance using wireless phones, and 50 participants (42 percent) believed the use of the Internet allowed criminal evasion of electronic surveillance. The following chart provides the results of our review:

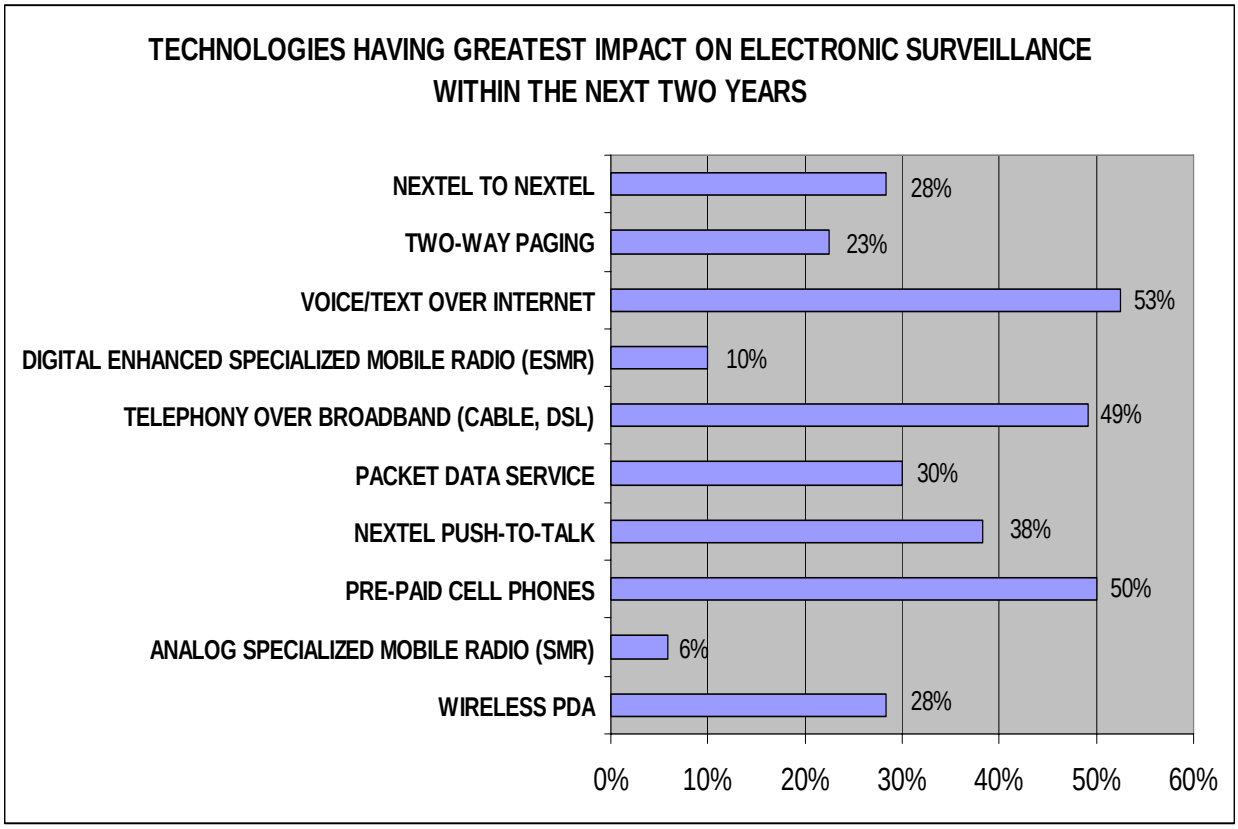


Source: OIG analysis of 120 FBI Threat Assessment Surveys

We noted that 25 participants (21 percent) believed criminals used telephone company features (call-forwarding, voice mail, 3-way calling) to evade electronic surveillance. However, because the survey responses were general in nature, we were unable to determine the specific features, if any, that were problematic to law enforcement or the extent of the problem. In our judgment, this is a shortcoming in the FBI's survey because it does not identify whether the problem results from a non-CALEA compliant carrier, or the law enforcement agency does not possess the resources to acquire the CALEA features.[74] For example, two law enforcement officials informed us that their agency cannot afford the expense of installing a T-1 line, which is the delivery method to receive the CALEA features (this issue is discussed further in Finding IV).

[74] During our audit we noted other discrepancies regarding the collection and tabulation of survey responses that resulted in the FBI reissuing a corrected 2004 Threat Assessment Survey Report.

The surveys also requested participants to prioritize current, new, or emerging technologies having the greatest impact on their agency's ability to perform electronic surveillance. As shown in the following chart, law enforcement officers indicated that pre-paid cell phones, telephony over broadband, and voice or text over the Internet would have the greatest impact on their department's electronic surveillance activities within the next two years.



Source: OIG analysis of 120 FBI Threat Assessment Surveys

Our review of the FBI's Threat Assessment Surveys revealed that the law enforcement community is less concerned over the ability to perform electronic surveillance on wireline equipment, and more concerned over new and emerging technologies. In addition, we believe the FBI should obtain a larger audience of survey participants to include more state and local law enforcement representatives and provide comprehensive examples of the electronic surveillance problems law enforcement is encountering.

Case Examples

During our audit, we requested specific examples that illustrate existing intercept problems. The FBI provided us with a document entitled *FBI Investigative Technology Division CALEA Law Enforcement Case Examples* dated October 29, 2004. In addition, a DOJ official provided a memorandum, dated March 30, 2005, describing instances where law enforcement has encountered problems with emerging technologies. According to the memorandum, these examples underscore "the importance of addressing vulnerabilities *before* they have matured into widespread problems that have an irreversible significant detrimental impact on law enforcement and national security interests."

The FBI's document contained a total of 57 case examples representing federal, state, and local law enforcement experiences with CALEA wiretaps. Twenty-seven of the examples described intercepts that were successful, 23 described intercepts that were unsuccessful, and the remaining 8 provided general comments that did not specifically address either a successful or unsuccessful intercept (e.g. information from informants regarding the use of push-to-talk (PTT) and VoIP). None of the examples, however, noted electronic surveillance problems for wireline intercepts. The unsuccessful intercepts were as follows:

- Sixteen of the case examples described unsuccessful PTT intercepts, with the most recent example occurring in August 2004.[75] The carriers cited and the number of instances where law enforcement was unable to conduct electronic surveillance were as follows: [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- Three of the case examples described unsuccessful VoIP intercepts. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- Two case examples cited pre-paid calling card or pre-paid cell phone for the cause of an unsuccessful intercept. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

[75] [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- Two case examples cited carrier issues regarding lack of audio as the cause of an unsuccessful intercept. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

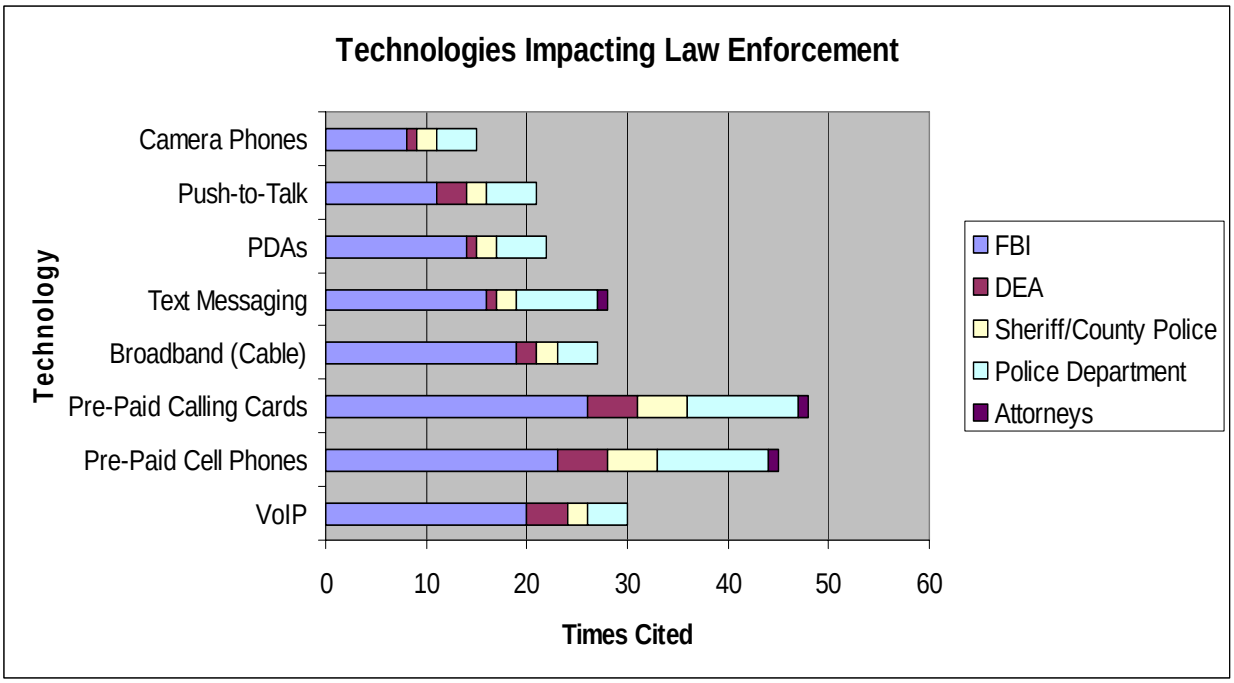
In our judgment, these examples are not necessarily indicative of emerging technology that is negatively impacting law enforcement's ability to conduct electronic surveillance. According to an FBI official, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

Emerging Technologies

Depending on the law enforcement agency, emerging technology impacts their ability to conduct electronic surveillance to varying degrees. A New York law enforcement official stated that the technology is changing at such a high rate of speed that law enforcement needs the FCC to step in. He also noted that "the carriers are doing what the criminals couldn't do – putting law enforcement out of business," by releasing technology without a solution and by charging fees that make electronic surveillance cost prohibitive (this issue is discussed further in Finding IV).

According to law enforcement officials, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED]. A law enforcement official stated that his agency has experienced [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] before the target has changed phones. Therefore, he believes that law enforcement's ability to conduct a wiretap should be tied to the individual, rather than the phone line, to make the process quicker for switching the line that the wiretap is on. Law enforcement officials noted [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] through the carrier. Additionally, targets are able to evade electronic surveillance by using cell phones purchased in Mexico or by traveling into Mexico to place calls, even if the target uses a U.S. carrier. A law enforcement official noted that calls made on cell phones purchased in Mexico or calls initiated in Mexico are not wiretapped because of security concerns related to working with carriers' international divisions.

Of the 82 affirmative responses to the OIG survey, law enforcement officials indicated that the following emerging technologies negatively affect their agencies' ability to conduct electronic surveillance:



Source: Law enforcement responses to the OIG survey

According to the FBI, Internet "hotspots" such as cyber cafés that provide anonymity with multiple access points, third-party calls using calling cards, and toll free numbers are a "technologically unsolvable problem." These services can only be addressed through investigative techniques, rather than through the application of CALEA. In addition, FBI officials said that commercially available electronic encryption will also hinder law enforcement's ability to collect information from electronic intercepts.[76] According to the FBI, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

[76] Under CALEA, carriers are not responsible for decrypting, or ensuring the government's ability to decrypt any communication encrypted by a customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

FBI's Plans for Remaining CALEA Funding

About $45 million in CALEA funds remain for the implementation of CALEA-compliant solutions. As previously discussed, the FBI is negotiating reimbursement agreements with two carriers for the cost of deploying CALEA solutions on their pre-1995 equipment. The funds remaining upon completion of negotiations with the two carriers will be used to reimburse second-tier carriers (e.g., large independent carriers and competitive local exchange carriers serving smaller metropolitan areas such as Cincinnati Bell and Alltel). The FBI expects to exhaust the remaining CALEA funds reimbursing second-tier carriers.

We are concerned about how the FBI plans to use the remaining $45 million. We recognize that CALEA permits the FBI to reimburse carriers for all reasonable costs associated with bringing pre-1995 equipment, facilities, and services into compliance. Nevertheless, because CALEA implementation was delayed, and because technology has significantly changed from the time of CALEA's enactment, we believe the FBI should reexamine the future benefits of activating CALEA software solutions on wireline systems before expending any additional funding. The basis for our concern revolves around: (1) the growing popularity in Internet telephony, (2) the limited number of intercepts performed on wireline equipment, (3) the apparent limited effect on criminal investigations, and (4) the discussion on emerging technologies. Our conclusion in this area is not only limited to the above discussion, but is also based on the costs of the equipment needed to obtain CALEA-covered wiretaps, the wiretap fees charged by carriers, and the delivery method (as discussed in Finding IV).

Although this list is not all-inclusive, the FBI should consider the following factors prior to expending the remaining $45 million in CALEA funding:

- law enforcement's priorities as they pertain to emerging technologies;
- the number of intercepts conducted under Title III and FISA;
- the number of CALEA-covered intercepts conducted in prior years and the number expected to be performed in the future;
- the ability of law enforcement in the coverage area to equip a wireroom and pay for the intercept;

- the length of time needed to negotiate with carriers, and for carriers to deploy and activate the software;

- the carriers' schedule for replacing or significantly upgrading their pre-1995 equipment, facilities, or services;[77] and

- the delivery method the carrier will require law enforcement to accept.

Conclusion

As technology advances at an ever-increasing pace, law enforcement officials must be prepared to deal with emerging technologies. For example, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

When considering the changing dynamics of the telecommunications industry, the limited number of CALEA-covered wiretaps reported by four carriers in high-priority locations, and the fact that almost 90 percent of authorized wiretaps are conducted on portable devices, we believe the FBI should consider alternative uses for the remaining CALEA funds.

[77] According to CALEA, if the FBI has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of Section 103, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of Section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification.

Recommendations

We recommend that the FBI:

2. Expand the audience of state and local law enforcement representatives participating in its Law Enforcement Technical Forums and the FBI Threat Assessment Surveys. This would allow for a more comprehensive understanding of the electronic surveillance threats to law enforcement.

3. Improve the methodology used to gather accurate and current data regarding the adverse impact on criminal investigations arising from carriers' inability to provide CALEA-compliant wiretaps or access to call-identifying information. This can be accomplished by soliciting detailed information on adverse responses to the Threat Assessment Survey, and through the CALEA helpdesk.

4. Reexamine the benefits of activating CALEA solutions on wireline systems prior to the expenditure of the remaining $45 million in CALEA funding.

IV. ISSUES REQUIRING RESOLUTION

The development, deployment, and maintenance costs associated with implementing CALEA and who should bear those costs continue to be controversial issues. The 10 carrier officials we interviewed believed that these significant costs will hinder full CALEA-compliance. For law enforcement, electronic surveillance is expensive, and includes wiretap fees charged by carriers, equipment costs, and costs associated with the delivery method. In addition to these costs, law enforcement's ability to conduct electronic surveillance is also hampered by poor customer service by carriers, and the FBI's ability to provide assistance and training on electronic surveillance to state and local law enforcement agencies. As technology advances, carrier and law enforcement costs will increase, and their limited assistance could negatively affect law enforcement's ability to conduct electronic surveillance.

Costs Incurred by Carriers

The 10 carrier officials we interviewed indicated that they were committed to complying with CALEA and that they had, or were actively engaged in deploying, CALEA solutions on their networks. However, these same officials advised us that significant costs will hinder full CALEA-compliance. Specifically, carrier representatives stated that the cost to develop, deploy, and maintain electronic surveillance capabilities have been significant, and that these costs are expected to increase as technology advances. The following are just four examples of what the carriers told us:[78]

- A VoIP provider contracted to pay approximately $100,000 to a trusted third party (TTP) to develop its CALEA solution. In addition, the TTP will charge a monthly fee of $14,000 to $15,000 and $2,000 for each intercept. These amounts do not include the cost of labor for writing code into the software to accommodate the CALEA solution. In addition, officials from this provider discussed with us "opportunity" costs, in that programmers working on CALEA could be developing new features for its customers. Furthermore, the officials were concerned that the government would mandate that every

[78] We present this information because the cost of CALEA compliance remains a controversial issue and a concern for carriers. This information was provided by carrier representatives we interviewed and was not audited.

new feature would have to be CALEA-compliant prior to being offered to the public. Such a restriction would cost the company revenue and place them at a disadvantage in comparison to non-U.S. based providers, who do not have to comply with CALEA.

- A wireless carrier stated that it had spent about $14 million on standards-based voice and data CALEA solutions. These costs were primarily capital and ongoing labor costs, with the bulk of the money going towards developing Personal Communications Services (PCS) voice interception and second-generation packet-mode service. Furthermore, because all of the carrier's equipment is post-1995, the carrier must bear all costs. This carrier also discussed "hidden costs." For example, resources are pulled from revenue-generating projects to work on CALEA projects. In addition, interaction with vendors to develop CALEA solutions and providing technical assistance to law enforcement is very costly.

- Another wireless carrier estimated that it spent about $40 million to make its network CALEA-compliant. Again, virtually all of this carrier's equipment was post-1995 and, therefore, its costs were not recoverable from the FBI.

We also obtained the costs that some carriers incurred to deploy their CALEA solutions on a "per switch" basis. Specifically, one wireline carrier stated that the company spent nearly $24,000 per switch to deploy its CALEA solution on 747 switches. Another wireline carrier stated that its CALEA-compliance cost was over $33,000 per switch on 222 switches. However, the reported carrier costs, both in the aggregate and on a per switch basis, are not comparable because carrier networks vary greatly in size and switch type.

One carrier representative stated that his company believes law enforcement is frustrated by the new communications technology, but does not fully understand the total cost and complexity of obtaining CALEA wiretaps in a wireline and wireless environment. The representative also said that the costs and complexity involved will be exponentially greater with packet mode technology. He further stated that law enforcement wants the CALEA functionality but is largely unaware of the expense and technical impediments to full

implementation. This official believed that the problems for law enforcement must be solved before CALEA is implemented on a larger scale.

Costs Incurred by Law Enforcement

From a law enforcement perspective, conducting electronic surveillance is expensive and includes wiretap fees charged by carriers, equipment costs, and costs associated with the delivery method.

Wiretap Fees Charged by Carriers

Law enforcement's biggest complaint regarding CALEA is the relatively high fees charged by carriers to conduct electronic surveillance. A traditional wiretap costs law enforcement approximately $250. However, a wiretap with CALEA features costs law enforcement approximately $2,200 according to law enforcement officials and carrier representatives we interviewed. A law enforcement official noted that, "[w]ith CALEA, the carriers do less work but it costs approximately 10 times as much to do a CALEA-compliant tap versus a traditional tap." Law enforcement officials agree that the features provided by CALEA are valuable. However, some law enforcement agencies cannot afford to conduct the number of wiretaps they believe is necessary to support their investigations. We found that other agencies have chosen to conduct traditional wiretaps because of the high carrier fees associated with the CALEA features. In addition, we found that carrier fees varied widely.

During our site visits to federal, state, and local law enforcement agencies, we obtained carrier fee schedules and invoices. The carrier invoices were not itemized, which is a source of contention between law enforcement and the carriers. Law enforcement officials stated that the carriers refuse to provide their agencies with itemized bills that detail the charges for each intercept (i.e., initiation fee, maintenance fee, "pinging" fee, and cost of reports). The agency can verify that the wiretap was active on the dates indicated on the bills, but not what the total cost listed on the bill is based on. Therefore, we were unable to determine if the carriers are passing capital costs on to

law enforcement.[79] However, as previously noted, one carrier informed us that most of the costs it billed to law enforcement are for overtime and recovery of capitalized hardware and software costs. These representatives stated that capital costs are the major costs incurred by a carrier, and that these costs are entirely proper for carriers to recover. These representatives also stated that capital costs will continue to grow as technology accelerates.

One law enforcement official noted that prosecutors are unable to challenge the carriers' costs during the course of the electronic surveillance because to do so would be a civil matter and the wiretap orders are sealed by the criminal court. The prosecutor would have to wait until the criminal matter was completed. The law enforcement official stated that at that point the electronic surveillance is no longer needed and the prosecutors do not have time to pursue the issue.

Using the wireless carrier fee schedules provided by law enforcement, we calculated a total base cost per intercept to illustrate the cost variances by carrier for the same type of electronic surveillance and the cost variances charged to different law enforcement agencies by the same carrier.[80] As depicted in the following tables, we received fee schedules within the same state for four carriers (Carriers A, B, G, and H).

Since some carriers charge a flat fee while others charge an initiation fee plus a daily maintenance fee, we based our calculations for pen register fees on a 60-day period and Title III wiretap fees on a 30-day period since that is the timeframe covered in court orders. In addition to the base calculation provided in the tables, additional fees may be charged by the carriers including monthly maintenance fees,

---

[79] According to DOJ's *Joint Petition*, the FCC should clarify the costs that can be included in intercept provisioning costs and determine who bears financial responsibility for such costs. Although carriers are permitted under Title III to pass on to law enforcement their provisioning costs, a growing number of law enforcement agencies expressed concern over the significant provisioning costs in carriers' bills. These costs make surveillance more difficult, especially for smaller law enforcement agencies. To permit carriers to include their CALEA implementation costs in their provisioning costs would not only violate Title III, but will also make it increasingly cost-prohibitive for law enforcement to conduct intercepts. Although Title III provides for carriers to be compensated for costs associated with intercept provisioning, nothing in either Title III or CALEA authorizes carriers to include CALEA implementation costs in their provisioning costs.

[80] Wireline fee schedules were not provided by law enforcement because the majority of intercepts are conducted on wireless phone.

per switch set-up fees, additional switch fees, uninterrupted continuation fees, call-bridging fees, extension fees, and fees for activity reports.

BASE FEE FOR A 60-DAY PEN REGISTER (WIRELESS)					
	NY	**FL**	**AZ**	**CA**	**NV**
CARRIER A	$1,775			$1,775	$1,775
				$2,600	$2,200
CARRIER B			$1,775	$1,775	$600
				$2,075	
				$2,600	
CARRIER C		$1,400			
CARRIER D				$600	$1,200
CARRIER E (Telephone)	$1,750	$1,750	$1,750	$1,750	
CARRIER E (Push-To-Talk)	$2,000	$2,000	$2,000	$2,000	
CARRIER F			$1,750	$1,750	$1,750
CARRIER G	$350			$250	$400
				$350	$450
				$3,100	
CARRIER H (New Order)	$1,135		$1,135	$1,025	$1,135
				$1,135	
CARRIER H (Renewal)	$820		$820	$820	$820
CARRIER I	$350				
CARRIER J					$250

Source: Carrier fee schedules provided by individual law enforcement agencies

BASE FEE FOR A 30-DAY TITLE III (WIRELESS)					
	NY	FL	AZ	CA	NV
CARRIER A	$1,775			$1,775	$1,775
				$2,600	$2,200
CARRIER B			$1,775	$1,775	$600
				$2,600	
CARRIER C		$1,600			
CARRIER D				$600	$1,200
CARRIER E (Telephone)	$1,750	$1,750	$1,750	$1,750	
CARRIER E (Push-To-Talk)	$2,000	$2,000	$2,000	$2,000	
CARRIER F			$1,000	$1,000	$1,000
CARRIER G	$350			$100	$350
				$350	$400
				$3,100	
CARRIER H (New Order)	$940		$940	$575	$940
				$940	
CARRIER H (Renewal)	$675		$675	$675	$675
CARRIER I	$350				
CARRIER J					$250

Source: Carrier fee schedules provided by individual law enforcement agencies

The above fee calculations illustrate that carriers' fees range from $250 to $3,100 to conduct pen registers and Title III wiretaps. Carrier fees are also inconsistent among law enforcement agencies and states. For instance, Carrier B charges a Nevada law enforcement agency $600 for a Title III wiretap while the same carrier charges a California law enforcement agency $1,775 and another California law enforcement agency $2,600.

The cost to conduct electronic surveillance for one case can quickly rise. For example, if law enforcement needs to conduct electronic surveillance beyond the 30- and 60-day timeframes, a new court order requesting an extension must be obtained and, in most cases, the law enforcement agencies are charged the same fees again by the carriers. In addition if another target is identified during the monitoring of the initial target, another court order is obtained to initiate an additional wiretap. A law enforcement official stated that a

typical case for his agency usually involves five to six targets. If a target uses more than one phone, the cost to law enforcement rises proportionately.

From the 82 responses to our survey from law enforcement officials indicating that their agency conducts electronic surveillance, 31 agencies (38 percent) indicated that the number of intercepts conducted is hindered by the costs charged by carriers.

In its March 2004 *Joint Petition*, DOJ requested that the FCC:

1. confirm that carriers bear sole financial responsibility for CALEA implementation costs for post-January 1, 1995, communications equipment, facilities and services;

2. permit carriers to recover their CALEA implementation costs from their customers; and

3. clarify the cost methodology and financial responsibility associated with intercept provisioning.

In its NPRM, the FCC sought comment on:

- Cost recovery options that could reduce CALEA-related burdens otherwise imposed on carriers and their customers, including options that more equitably spread costs among the general public. For example, the FCC questioned whether CALEA costs should be recovered directly from consumers by means of an FCC-mandated, flat monthly charge; and

- Whether the FCC should distinguish carrier recovery of CALEA incurred capital costs generally from recovery of specific intercept-related costs. In addition, the FCC sought comment on the costs that can be included in intercept provisioning costs and the entities that should bear financial responsibility for those costs.

Equipment Costs

In order to conduct CALEA wiretaps, law enforcement agencies must maintain or have access to a wireroom. A wireroom consists of a computerized system that intercepts, decodes, records, and plays back telephone communications. The installation of these facilities is both time-consuming if not already in place (it must be ordered weeks or months in advance) and expensive. Depending upon the number of wiretaps conducted and available funding, law enforcement agencies may elect to maintain their own wireroom, maintain a wireroom in conjunction with another agency, or request the temporary use of a wireroom maintained by another agency. Although law enforcement officials noted that their wirerooms are also available for use by other law enforcement agencies in their general vicinity, the smaller law enforcement agencies are limited in conducting electronic surveillance due to the fees charged by carriers.

Of the 82 responses to our survey from law enforcement officials indicating that their agency conducts electronic surveillance, 48 agencies (59 percent) maintain their own wireroom. Law enforcement officials representing the 82 agencies indicated that the number of intercepts conducted by their agencies is hindered by the cost to purchase equipment (16 of 82 responses) and the cost of equipment maintenance (11 of 82 responses).

According to law enforcement officials we interviewed and those who responded to our survey, law enforcement agencies have spent between hundreds of thousands to several million dollars to equip their wirerooms. The equipment costs depend upon the desired capacity of simultaneous wiretaps and the need to accommodate the carriers' various delivery methods (as discussed in the following section). A typical wireroom, as pictured below, consists of the following equipment:

- Monitor and playback stations (PCs)

- Servers (the number of servers required is dictated by the carrier's delivery method)

- An audio recorder (known as a jukebox) which saves the data on a magnetic drive

- Routers (the number of routers required is dictated by the carrier's delivery method)

- A system administration computer

Source: SyTech brochure (permission granted)

As an example, the equipment listed below was located in one of the wirerooms that we visited. This particular wireroom has the capacity to conduct eight regular wiretaps or four [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] wiretaps simultaneously.

- 8 computer workstations;
- 3 servers (one to conduct regular cell phone intercepts, one to conduct [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] intercepts, and one to conduct pager and Internet intercepts);
- 1 jukebox, which saves the data on a magnetic drive;
- 1 separate router for [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] intercepts (all other carriers are on a Virtual Private Network (VPN)); and
- 1 computer monitor to switch between the 3 servers.

In addition to the initial purchase of equipment, law enforcement agencies also pay approximately $30,000 per year in maintenance fees to their equipment vendor. Law enforcement agencies said they spend additional funds for hardware and software upgrades to keep up with

improvements and emerging technology.

Equipment costs for collecting the large amount of data will continue to be a major impediment for law enforcement. As technology changes and electronic surveillance becomes more complex, law enforcement will need to carefully consider how they will receive large volumes of data, especially with broadband intercepts. The collection equipment required by law enforcement will be more complex and costly, and law enforcement will also need to develop the technical expertise to operate the equipment.

Delivery Methods

During our site visits, many law enforcement officials noted that CALEA addresses what carriers need to provide to law enforcement agencies without addressing how data is delivered. For example, CALEA does not address whether carriers can use digital or audio phone lines to deliver the audio portions of intercepts. As a result, the delivery method of intercepted data varies by carrier. Due to the various delivery methods, law enforcement agencies must purchase additional equipment to receive the intercepted data from a carrier. The four delivery methods are dial-out, VPN, frame relay, and T-1 lines.

Dial-out. A dial-out solution takes advantage of the PSTN already in place between the carrier equipment performing an intercept and a law enforcement collection site. A dial-out solution only requires a regular telephone line.

VPN. For VPN, carriers use a “secure tunnel” VPN to conduct electronic surveillance over the Internet. The VPN secure tunnel method uses law enforcement’s existing connectivity to the Internet to connect to a specific point in the carrier’s network. Firewalls and encryption keys are used to authenticate the law enforcement agency before any intercepted call-identifying information or content is delivered from the carrier’s network. This method keeps the information secure when traversing the Internet, and does not require the law enforcement agency’s connection to the Internet to be dedicated to a specific carrier or to receiving CALEA information. The best features of a VPN-type connection are that the law enforcement agency can use the same connection to the Internet for multiple applications such as web browsing, e-mail, and CALEA connectivity.

Frame Relay. A frame relay connection consists of three parts: (1) the connection from the law enforcement agency to the carrier's frame relay, which is a private, specific-use circuit that connects a single law enforcement agency location to the carrier's network. This represents the maximum rate at which a law enforcement agency can accept packets from a carrier; (2) the frame relay, which is a network of routers that allow communication from point-to-point without having a dedicated circuit end-to-end; and (3) the connection from the frame relay, which is a private, specific-use circuit that connects multiple law enforcement agencies to the carrier's network. The value of the frame relay connection is its ability to handle large amounts of data, up to the bandwidth of the connection facility, but still not have to pay for that bandwidth point-to-point.

T-1 Line. A T-1 line is a higher capacity circuit using a fiber optic or copper line. A T-1 line can carry 24 digitized voice channels and about 192,000 bytes per second – roughly 60 times more data than a normal residential modem. It is also much more reliable than an analog modem.

One law enforcement official we interviewed stated that he would like to see DOJ mandate the dial-out solution as the delivery method because it is less expensive. A carrier official stated that with dial-out, the line can be connected in two or three days and only costs $60 per line. However, carriers also noted that not all of the CALEA features are available when dial-out is used because the "pipe" is not large enough for the data stream. Although dial-out is a viable option for receiving call-identifying information and call-content for circuit-mode calls, it may not be a viable option for packet-mode calls. This is because the low connection speed of the dial-out delivery method may not be able to handle the delivery of intercepted packets for law enforcement agencies that handle multiple simultaneous surveillances.

While dial-out and VPN are increasing in popularity, and favored among law enforcement agencies, some carriers only deliver data via a T-1 line. For some law enforcement agencies, T-1 line delivery for a wireline CALEA intercept is impractical. A T-1 line costs law enforcement agencies approximately $1,300 for installation, and can take up to two months to install. One law enforcement official told us that his agency pays carriers approximately $20,000 per month to

maintain its T-1 connections. He explained that the agency pays $575 to $1,800 per month for each circuit.[81]

A law enforcement official in California stated that his office was informed by two in-state wireline carriers that they are CALEA-compliant but law enforcement would need to build a T-1 line to each of the carriers' switches. The law enforcement official explained that this concept is unreasonable considering his agency's jurisdiction has about 95 switches from one carrier and about 130 switches from the other. Therefore, it would cost his agency about $292,500 to install T-1 lines to each of the switches.[82] This scenario would not be cost beneficial to his agency because a T-1 line is only used for wireline intercepts, and approximately 70 percent of this agency's wiretaps are performed on wireless phones. The law enforcement official stated that there are numerous agencies in California with authority to conduct intercepts and each agency would be required to install a T-1 line to each of the carriers' switches to conduct a CALEA intercept. Another law enforcement official in California estimated that 99 percent of their wiretaps are performed on wireless phones.[83] Furthermore, a law enforcement official in Florida also experienced the same situation with one of the carriers noted above. Due to the prohibitive cost of wireline carrier's CALEA solution, the California and Florida law enforcement agencies conduct traditional wiretaps that could not take advantage of CALEA features.

Law Enforcement Assistance Concerns

In addition to monetary issues that affect carriers and law enforcement, we identified assistance concerns that will also affect the successful implementation of CALEA.

---

[81] Another option is to lease access to the carrier's T-1 lines through the law enforcement agency's equipment vendor. Equipment vendors gain permission from the carrier to place a collection box on the carrier's server through which the vendor receives the intercepted data and subsequently passes the data onto the requesting law enforcement agency. A law enforcement official stated that his agency leases access to the carrier's T-1 line through their vendor at a rate of $750 per month.

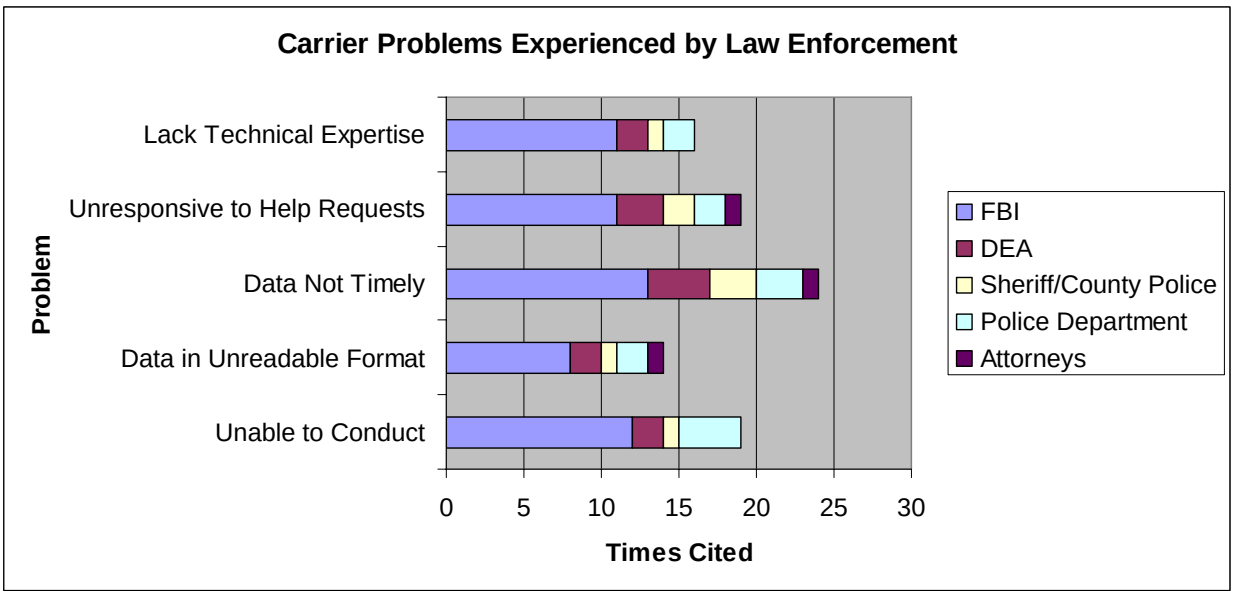
[82] Calculation is based on the assumption it would cost $1,300 per switch for installation.

[83] The difference between the two agencies' percentage of wiretaps performed on wireless phones was attributed to the types of cases each agency conducts; in particular, more wirelines are wiretapped in homicide cases than in drug cases.

Limited Carrier Customer Service

Several law enforcement officials stated that they received poor customer service from the carriers, and believe some carrier employees lack training on initiating and maintaining a CALEA wiretap. In particular, carriers were criticized for bringing down intercepts by upgrading their switches in the middle of the night without notifying law enforcement. In addition, west coast law enforcement officials stated that carriers do not provide customer service after 5:00 p.m. EST. One law enforcement official said that many of the carriers' representatives "have no clue" what law enforcement is talking about when they call with a problem and that he does not think they care or are encouraged to care about law enforcement's problems. Another law enforcement official offered examples when the carrier's switches were able to conduct the intercepts but the carrier's technician did not know how to activate the switches. In addition, law enforcement cited problems with carriers being unable to see the data being sent to law enforcement's monitors until hours later. Although law enforcement receives real-time information, the carriers' service representatives receive the same data hours later, which hinders the carriers' service representatives from providing timely assistance.

Of the 82 affirmative responses to our survey, law enforcement officials indicated the following problems with carriers:



Source: Law enforcement responses to the OIG survey

Meanwhile a carrier representative told us that most law enforcement agencies blame the carrier if something goes wrong with the intercept. The representative stated that when a law enforcement agency calls with a collection problem, the carrier will deliver the intercept data to its own collection equipment to determine if any problems exist with the delivery of the intercept. When the carrier investigates complaints, about 50 percent of the time it refers the law enforcement agency to the equipment vendor because the problems can be traced to a lack of technical expertise of the law enforcement agency in operating the collection equipment rather than the carrier's lack of customer service.

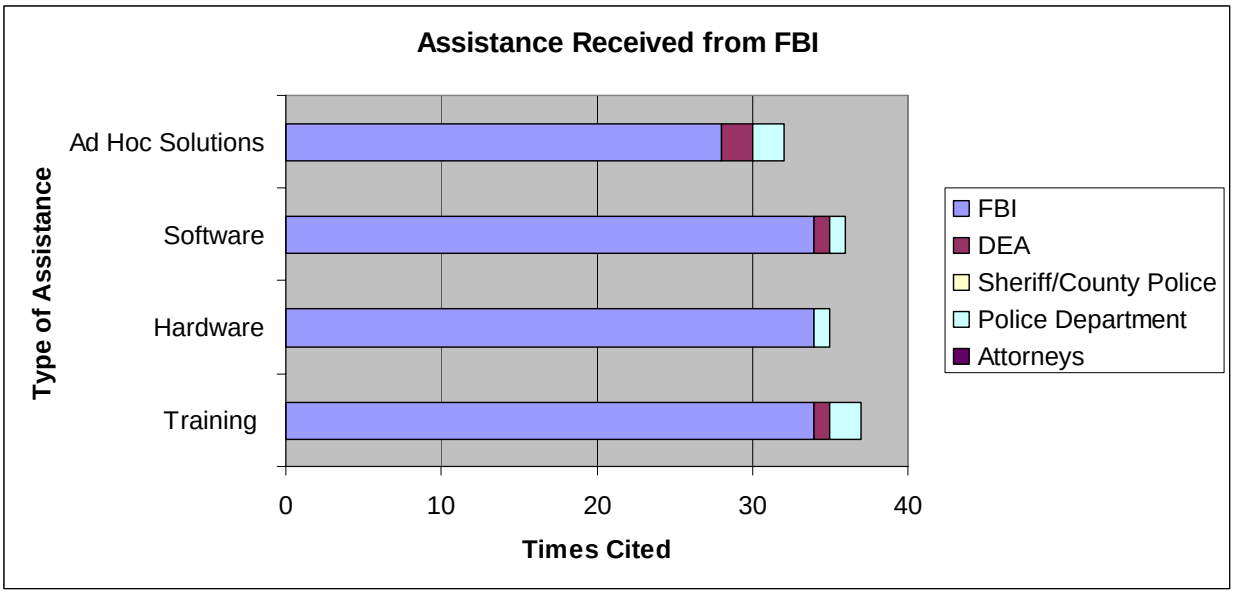
FBI Support of State and Local Law Enforcement

State and local law enforcement officials indicated that they feel disconnected and unsupported by the FBI on the issue of electronic surveillance. These officials believe that the FBI should provide basic training facilities for law enforcement agents and technical personnel to receive hands-on training on how to conduct CALEA intercepts. During our site visits, we met with state and local wireroom technical agents who were trained as law enforcement officers, but had no prior electronic surveillance experience. However, they were tasked with setting up a wireroom for their agencies, which included dealing with equipment vendors and learning how to conduct electronic surveillance. We believe that state and local agents' learning curves could be reduced dramatically if the FBI provided training. However, the FBI stated they may be limited by Attorney General Order 1945-95 (see footnote number 60) in the level of assistance and training they can provide.

Law enforcement officials who attended the FBI-sponsored Law Enforcement Technical Forums noted that the number of the forums has declined over the last few years. Additionally, we were told that forums have become one-sided with the FBI simply presenting information, instead of an exchange of ideas between the FBI and law enforcement. Law enforcement officials also noted that the FBI should provide an opportunity and venue for vendors to showcase their equipment and analytical programs. Law enforcement officials further mentioned they would like a forum to meet with representatives from the telecommunications carriers in order to voice their concerns. We discussed with the FBI the possibility of the vendors and carriers attending the Law Enforcement Technical Forums. However, FBI officials disagreed with this suggestion, citing security concerns with vendor and carrier personnel.

Our audit also found that some of the state and local law enforcement officials we interviewed were unaware of the resources available to them through the FBI, such as the FBI's CALEA website or its help desk. If law enforcement agencies are unaware of the CALEA website then they are unable to request membership in the Law Enforcement Technical Forum. Members receive invitations to the Law Enforcement Technical Forums where law enforcement representatives can discuss their issues and concerns as well as participate in the Threat Assessment Surveys.

Of the 82 affirmative responses to our survey, 42 (51 percent) law enforcement officials (mostly from the FBI) indicated that their agency had contacted the FBI's CALEA Implementation Unit (CIU) or Engineering Research Facility (ERF) for assistance.[84] All of the agencies that had contact with the CIU or ERF were satisfied with the assistance provided. The 42 officials noted that the FBI provided ad hoc solutions, software, hardware, and training to their respective agency, as shown in the table below:



Source: Law enforcement responses to the OIG survey

[84] After a series of reorganizations, responsibility for CALEA implementation now rests within the FBI's Investigative Technology Division (ITD). Within the ITD, the CIU and ERF are tasked with developing overarching CALEA implementation strategies and developing ad hoc solutions.

Conclusion

Law enforcement officials uniformly believe that electronic surveillance is a vital investigative tool and that the CALEA features are extremely beneficial. However, law enforcement agencies are hindered in their ability to conduct the desired number of wiretaps by the cost-prohibitive delivery path offered by some carriers as well as the intercept fees charged by carriers and the costs to set up and maintain a wireroom. While a carrier may be considered CALEA-compliant, it is of no use to law enforcement if the agency cannot afford the delivery path to receive the intercepted data or simply cannot afford the intercept fees.

In addition, we found that state and local law enforcement agencies often do not have the necessary resources to conduct effective electronic surveillance. As a result, state and local law enforcement officials we interviewed indicated they often feel disconnected and unsupported by the FBI, and would benefit greatly from a closer working relationship with the FBI on these issues.

Law enforcement officials said they have experienced poor customer service from some carriers, further complicating their ability to conduct electronic surveillance. For instance, carriers were criticized for bringing down intercepts by upgrading their switches in the middle of the night without notifying law enforcement. In addition, our survey indicated that law enforcement was not provided the intercept data in a timely manner and that the some carriers were unresponsive to requests for assistance.

Recommendations

We recommend that the FBI:

5. Provide training for state and local law enforcement agents and technical personnel on how to conduct CALEA intercepts. In conjunction with this recommendation, the FBI should pursue legal clarification of Attorney General Order 1945-95 from the DOJ.

6. Improve liaison between law enforcement officials and carrier and manufacturer representatives by providing a forum to address electronic surveillance issues. This would enhance carrier customer service and law enforcement officials' technical knowledge.

STATEMENT ON INTERNAL CONTROLS

In planning and performing the audit of the Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, we considered aspects of the FBI's internal controls for the purpose of determining our auditing procedures. This evaluation was not made for the purpose of providing assurance on the FBI's internal controls as a whole.

As discussed in the Findings and Recommendations section of this report, we believe the FBI can strengthen its internal controls by reexamining the benefits of activating CALEA solutions on wireline systems prior to the expenditure of the remaining $45 million in CALEA funding.

Because we are not expressing an opinion on the FBI's internal controls as a whole, this statement is intended solely for the information and use of the FBI in managing the CALEA program. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

This audit assessed the implementation of CALEA. In connection with the audit, as required by the standards, we reviewed management processes and records to obtain reasonable assurance concerning the FBI's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on FBI operations. Compliance with laws and regulations applicable to the FBI's management of CALEA is the responsibility of the FBI's management.

Our audit included examining evidence about laws and regulations. Specifically, we conducted our review against relevant portions of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001 et. seq.

Our audit identified no areas where the FBI was not in compliance with the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001 et. seq.

SCHEDULE OF DOLLAR-RELATED FINDINGS

	AMOUNT	PAGE
Funds Put to Better Use		
Amount Remaining in the TCCF	$45 million	51

FUNDS PUT TO BETTER USE are future funds that could be used more efficiently if management took actions to implement and complete audit recommendations.

Appendix I

Objectives, Scope, and Methodology

Our objectives were to: (1) review CALEA implementation costs and progress; (2) review the impediments to CALEA implementation, including the effects of emerging technologies; and (3) determine how the implementation of CALEA, or lack thereof, has impacted federal, state, and local law enforcement in their ability to conduct electronic surveillance. We conducted our audit in accordance with the *Government Auditing Standards* and included such tests as were considered necessary to accomplish our objectives. Our audit covered the implementation of CALEA since its inception.

As part of our audit, we obtained an understanding of CALEA and its history by reviewing the Communications Assistance for Law Enforcement Act (P.L. 103-414; 47 USC § 1001 et. seq.) and the major judicial and legislative actions that preceded CALEA including Berger v. New York, 388 S.Ct. 1873 (1967), Katz v. United States, 88 S.Ct. 507 (1967), and the Electronics Communication Privacy Act. Additionally, we reviewed the FCC actions related to CALEA including their Notice of Proposed Rulemaking and Declaratory Ruling (NPRM) and select comments to the NPRM from interested parties. To assess the FBI's strategy for implementing CALEA, we reviewed the FBI's Strategic Plan 2004-2009, the CIU's Program Plan FY 2004-FY 2008 and documentation pertaining to the Right-to-Use software negotiations.

We analyzed data provided in the FBI's Flexible Deployment Initiatives to assess the FBI's methodology in estimating CALEA compliance. In addition, we reviewed the *FBI Investigative Technology Division CALEA Law Enforcement Case Examples*, the Criminal Division's examples of intercept problems, and the FBI's 2004 Threat Assessment Report, with the corresponding individual survey responses, to gain an understanding of issues encountered by law enforcement while conducting electronic surveillance.

We conducted interviews with various officials from the FBI's Investigative Technology Division, including the Deputy Assistant Director; the Section Chief, Electronic Surveillance Technology Section; the Unit Chief, CALEA Implementation Unit; and the FBI and DEA Supervisory Special Agents for CALEA Implementation. We also conducted interviews with various officials from the DEA, including the Assistant Administrator, Operational Support Division; the Deputy

Assistant Administrator, Office of Investigative Technology; the Chief, Telecommunication Intercept Support Section; and the Telecommunication Attorney. In addition, we interviewed a Senior Counsel to the Assistant Attorney General for the Criminal Division of the Department of Justice and representatives from the following organizations:

- The Center for Democracy and Technology;
- The FCC;
- Steptoe & Johnson, LLP;
- Fiducianet, Inc.;
- Bell South;
- Verizon;
- Qwest;
- Verizon Wireless;
- SBC;
- Sprint;
- Cingular;
- Vonage;
- America Online; and
- Comcast.

We interviewed federal, state, and local law enforcement from five states with switches that were identified as high-priority by the FBI, and who were provided coverage by a different carrier in each state. To focus our review on switches with a higher priority, we used the FBI's Flexible Deployment III database to identify switches with a priority score of 80 or higher. The database identified 512 switches with a priority score of 80 or higher and the switches are located in 18 different states as follows:

	State	Number of High-Priority Switches	Main Carrier
1	Alaska	2	ACS Wireless
2	Arizona	40	Qwest
3	California	116	SBC/Verizon
4	D.C.	12	Verizon
5	Florida	51	Bell South
6	Hawaii	4	Verizon
7	Illinois	28	SBC
8	Indiana	1	Cingular
9	Louisiana	3	Bell South
10	Maryland	46	Verizon
11	Michigan	26	SBC
12	Nevada	11	Sprint
13	New Jersey	2	Voice Stream Wireless
14	New York	95	Verizon
15	Ohio	11	SBC
16	Pennsylvania	18	Verizon
17	Rhode Island	5	Verizon
18	Texas	41	SBC
	TOTAL	**512**	

In order to select states that had a significant number of high-priority switches, and to ensure that we reached the major carriers, we selected the following five states:

	State	Number of High-Priority Switches	Targeted Carrier
1	California	116	SBC
2	New York	95	Verizon
3	Florida	51	Bell South
4	Arizona	40	Qwest
5	Nevada	11	Sprint
	TOTAL	**313**	

We reviewed the listing of switches within each state and visited the cities that the majority of the switches covered. We conducted interviews with law enforcement officials from the following agencies:

- **New York**

  White Plains
  - New York State Attorney General's Office
  - Westchester County District Attorney's Office
  - U.S. Attorney's Office

  Flushing
  - New York Police Department
  - Suffolk County District Attorney's Office

- **Florida**

  Tampa
  - Tampa Police Department
  - Hillsborough County Sheriff's Office
  - State Attorney's Office
  - Florida Department of Law Enforcement
  - FBI

  Miami
  - Broward County Sheriff's Office
  - Miami-Dade Police Department
  - Florida Department of Law Enforcement

- **Arizona**

  Phoenix
  - State Attorney General's Office
  - Maricopa County Attorney's Office
  - Phoenix Police Department High Intensity Drug Trafficking Areas (HIDTA)
  - U.S. Attorney's Office

  Tucson
  - Pima County Attorney's Office (HIDTA)
  - Tucson Police Department
  - Pima County Sheriff's Department

- **California**

  San Diego
  - DEA
  - San Diego District Attorney's Office
  - FBI

  Los Angeles
  - Los Angeles District Attorney's Office
  - DEA
  - Los Angeles Clearinghouse (HIDTA)

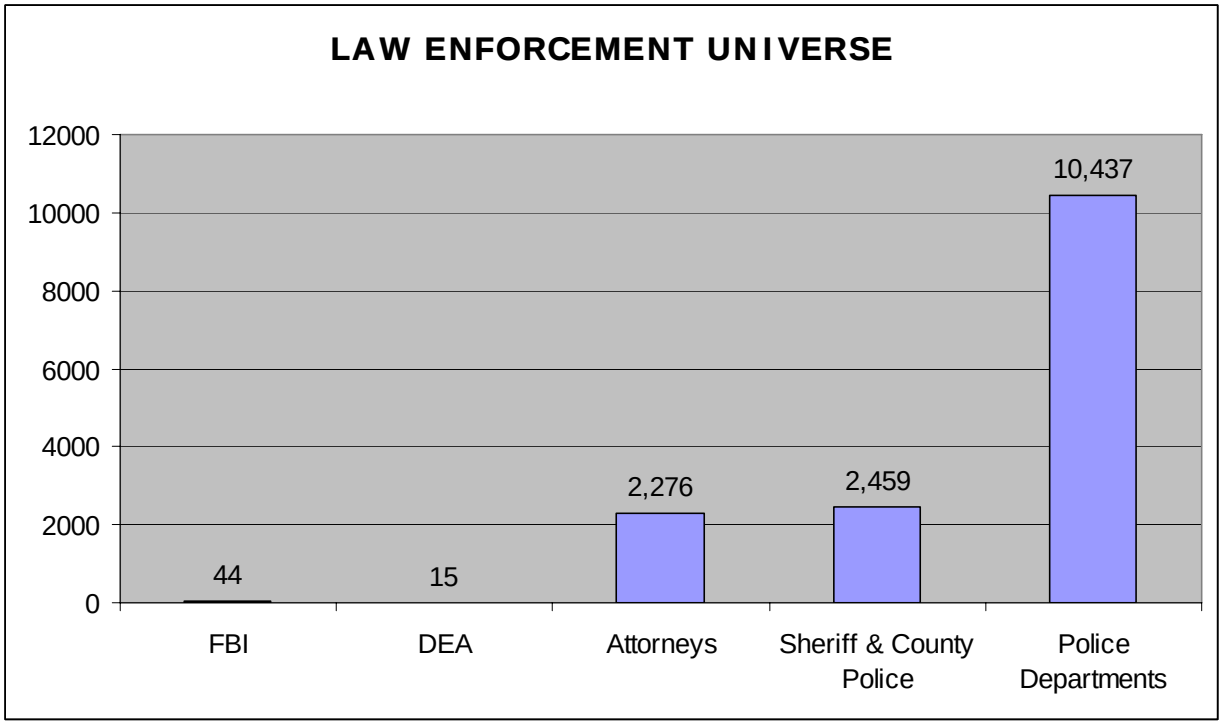
  Fresno
  - Central Valley (HIDTA)

- **Nevada**

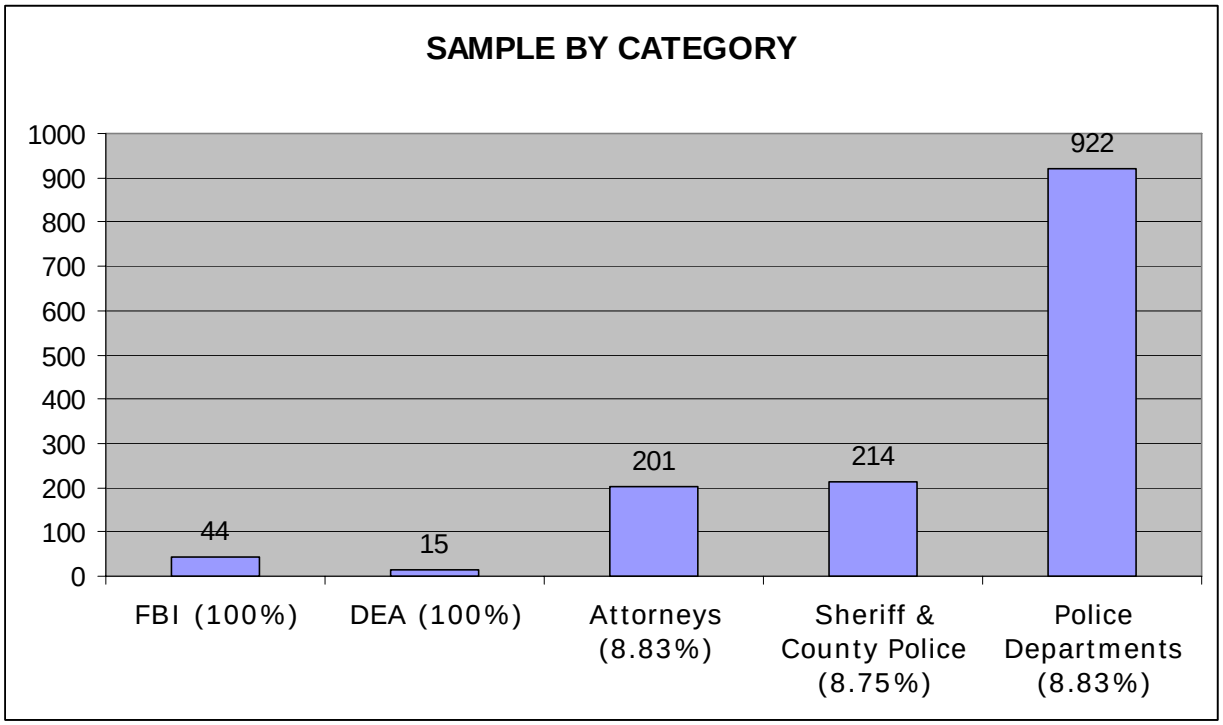
  Las Vegas

  - Las Vegas Metro Police Department
  - State Attorney General's Office
  - FBI

Based on our interviews with law enforcement from the five states listed above, we prepared a written survey to mail to a sample of federal, state, and local law enforcement officials. We obtained the universe of federal, state, and local law enforcement officials from the National Law Enforcement Administrators Directory. In selecting our sample, we did not include law enforcement officials from the states visited or the six states that do not have a wiretap law (Alabama, Arkansas, Kentucky, Michigan, Montana, and Vermont). Our universe of 15,231 federal, state, and local law enforcement agencies included the following categories:



We selected the following sample which totals 1,396 (9.17 percent of the universe):



Of the 1,396 surveys mailed, we received 723 responses (51.79%). An analysis of the responses received is illustrated in the following table.

RESPONSE RATES

AGENCY	SAMPLE	RESPONSES	AFFIRMATIVE RESPONSES	NEGATIVE RESPONSES	RESPONSE RATE	AFFIRMATIVE RESPONSE RATE
FBI	44	36	36	0	81.82%	81.82%
DEA	15	9	9	0	60.00%	60.00%
ATTORNEYS	201	89	2	87	44.28%	1.00%
SHERIFF/CO PD	214	118	11	107	55.14%	5.14%
POLICE DEPT	922	471	24	447	51.08%	2.60%
TOTAL	**1396**	**723**	**82**	**641**	**51.79%**	**5.87%**

We received responses from 82 agencies from 38 states that conduct electronic surveillance. The following table illustrates the affirmative responses by state and agency:

AFFIRMATIVE RESPONSES BY STATE AND AGENCY

	STATE	FBI	DEA	ATTORNEYS	SHERIFF/ CO POLICE	POLICE DEPT	TOTAL
1	AK	1					**1**
2	AL	2					**2**
3	AR	1					**1**
4	CO		1			1	**2**
5	D.C.	1	1				**2**
6	GA	1	1		1		**3**
7	HI	1					**1**
8	IA				1	1	**2**
9	IL	1	1		1	3	**6**
10	IN				1		**1**
11	KS					1	**1**
12	KY	1					**1**
13	LA	1				1	**2**
14	MA	1					**1**
15	MD	1					**1**
16	MI	1	1				**2**
17	MN	1				3	**4**
18	MO	2	1			1	**4**
19	MS	1					**1**
20	NC	1					**1**
21	NE	1					**1**
22	NJ		1	1			**2**
23	NM	1					**1**
24	OH	1			2	5	**8**
25	OK	1					**1**
26	OR	1					**1**
27	PA	1	1			3	**5**
28	PR	1					**1**
29	RI					1	**1**
30	SC	1				1	**2**
31	TN	2				3	**5**
32	TX	3	1				**4**
33	UT	1			1		**2**
34	VA	2					**2**
35	WA	1					**1**
36	WI	1		1	2		**4**
37	WV				1		**1**
38	WY				1		**1**
	TOTAL	**36**	**9**	**2**	**11**	**24**	**82**
	%	**43.90%**	**10.98%**	**2.44%**	**13.41%**	**29.27%**	

Appendix II

Description of Technology-Based Problems Encountered by Law Enforcement

Cellular Port Capacity – Limited capacity of cellular systems to accommodate a large number of intercepts simultaneously.

Audio Dial Digit Capture – Cellular provider unable to capture dialed digits contemporaneous with audio.

Long Distance – Cellular provider could not intercept long distance calls (or provide call setup information) to or from a targeted phone.

Speed Dialing/Voice Dialing/Call Waiting – Provider unable to deliver the actual number dialed when these features are used.

Call Forwarding – Provider unable to deliver the actual number dialed when these features are used.

Direct Inward Dial – Provider unable to isolate target's communications or provide call set-up information to the exclusion of all other customers.

Voice Mail – Provider unable to provide access to the subject's audio when forwarded to voice mail or retrieve messages.

Digital Centrex – Provider unable to isolate all communications associated with the target to the exclusion of all others.

Other – Including other calling features such as call back, provider unable to: provide trap and trace information; isolate the digital transmissions associated with a target to the exclusion of all other communications; comprehensively intercept communications, and provide call set-up information.

Appendix III

CALEA Legal Provisions

This appendix provides a summary breakdown of the CALEA statute by section.

47 USCA §1001 (or Sec. 102) – This section describes eight definitions that apply to CALEA. Two of the definitions have been the subject of much dispute: *information services* (#6) and *telecommunications carrier* (#8).

47 USCA §1002 (or Sec. 103) – This section sets up the requirement that telecommunications carriers ensure that their equipment, facilities, or services are able to: 1) expeditiously isolate the content of targeted communications transmitted within the carrier's service area; (2) expeditiously identify information regarding the originating and destination numbers of targeted communications, but, in the case of pen registers or trap and trace devices, not the physical location of the targets, except as can be determined by the phone number; (3) provide intercepted communications and call-identifying information to law enforcement in a format such that they may be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets of electronic surveillance are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications. These requirements are often referred to as CALEA's "assistance capability requirements." These requirements however do not apply to *information services* or to equipment, facilities, or services used for the sole purpose of interconnecting telecommunications carriers. This section also prevents law enforcement from requiring that telecommunications carriers adopt specific designs of equipment, facilities, services, or features; and prevents law enforcement from prohibiting the telecommunications industry to adopt any equipment, facilities, services, or features it wants to.

47 USCA §1003 (or Sec. 104) – This section required the Attorney General to publish a notice in the *Federal Register* by October 25, 1995, describing the number of communication intercepts, pen registers, and trap and trace devices, that the government estimated it may conduct and use simultaneously by October 25, 1998, and a notice describing the maximum capacity needed to accommodate all of the communication intercepts, pen registers, and

trap and trace devices the government could conduct and use simultaneously after October 25, 1994. This section also required telecommunications carriers, by October 25, 1998 at the latest, to ensure that its systems were capable of simultaneously accommodating the number of intercepts, pen registers, and trap and trace devices estimated by the government, and capable of expanding to the maximum capacity needed by the government.

47 USCA §1004 (or Sec. 105) – This section requires that telecommunications carriers ensure that only their employees can activate intercepts, and not employees of the government agency seeking the electronic surveillance.

47 USCA §1005 (or Sec. 106) – This section requires telecommunications carriers to consult with telecommunications manufacturers and support service providers to ensure that current and planned equipment, facilities, and services comply with the assistance capability requirements described in Sec. 103. In addition, the section requires manufacturers and support service providers to offer the features or modifications needed for the carriers to comply with the assistance capability requirements in a reasonable amount of time and at a reasonable charge.

47 USCA §1006 (or Sec. 107) – This section establishes a "safe harbor" provision which allows telecommunications carriers to be found in compliance with the assistance capability requirements if they are in compliance with "publicly available technical requirements or standards adopted by an industry association or standard-setting organization," or with standards developed by the FCC. The FCC can develop its own standards through its rule-making process if the industry associations or standard-setting organizations fail to issue their own standards or if another party petitions the FCC that the industry-developed standards are deficient. This section also allows telecommunications carriers to petition the FCC for extensions of up to two years maximum for complying with the assistance capability requirements if the FCC, after consultation with the Attorney General, determines that compliance with the assistance capability requirements is not reasonably achievable through the use of available technology.

47 USCA §1007 (or Sec. 108) – This section describes the findings a court must make to order a non-compliant carrier to meet the requirements of CALEA. Specifically, the court must find that: (1) law enforcement has no reasonably available alternative for

implementing the order through other technologies or through another carrier or service provider, and (2) compliance with CALEA is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken. This section also references the CALEA enforcement powers described in 18 USC § 2522.

47 USCA §1008 (or Sec. 109) – This section describes when telecommunications carriers can receive reimbursement for modifications made to equipment, facilities, and services as a direct result of complying with CALEA. The Attorney General may agree to pay for all reasonable costs associated with bringing pre-1995 equipment, facilities, and services into compliance. For post-1995 items, the FCC will determine, upon petition, whether compliance with the assistance capability requirements is reasonably achievable. If the FCC finds that compliance is not reasonably achievable, the Attorney General may, upon petition of the carrier, agree to pay the carrier to make the modifications in order to make compliance reasonably achievable. If the Attorney General does not agree to pay these costs, the carrier will be deemed in compliance with the capability requirements. This section also requires the Attorney General to develop regulations for ensuring timely and cost-efficient payments to carriers.

47 USCA §1009 (or Sec. 110) – This section authorized an appropriation of $500 million to carry out CALEA for FYs 1995, 1996, 1997, and 1998. Such sums are authorized to remain available until expended.

47 USCA §1010 (or Sec. 112) – This section established the requirement that the Attorney General submit a report to Congress by November 30th of each year describing the amounts paid to telecommunications carriers under Sections 1003 and 1008 during the preceding fiscal year. This section also requires the Department of Justice, Office of the Inspector General to submit a report to Congress every two years that addresses certain issues.

Appendix IV

Federal Communications Commission Actions Related to CALEA

October 2, 1997
Notice of Proposed Rulemaking

This notice of proposed rulemaking proposes and seeks comment on rules that the FCC should adopt to implement CALEA, and requested interested third parties to submit proposed rules to implement CALEA.

April 20, 1998
Public Notice

The purpose of this Public Notice was to solicit comments on six petitions:

- On March 26, 1998, the Center for Democracy and Technology files a petition for rulemaking, requesting the FCC intervene in the implementation of CALEA. The Center for Democracy and Technology contends that the interim industry standard goes too far in enhancing location tracking capabilities and fails to protect the privacy of packet-switched communications, and that additional surveillance enhancements being sought by the FBI are not required under CALEA and would further render the industry standard deficient. The Center for Democracy and Technology also states that compliance with the industry standard is not reasonably achievable and requests that the FCC indefinitely delay implementation of CALEA while a more narrowly focused standard consistent with the intent of CALEA is developed.

- On March 27, 1998, FBI and DOJ jointly file a petition for expedited rulemaking, asking the FCC to correct deficiencies in the industry standard by establishing additional technical requirements and standards that meet the requirements of CALEA. DOJ and FBI claim that the interim standard adopted by the telecommunications industry is deficient because: (1) it does not ensure that law enforcement will be able to receive all of the communications content and call-identifying information that carriers are obligated to deliver under CALEA; and (2) it fails to ensure that information will be

delivered in a timely manner. DOJ and FBI set forth, as a proposed rule, the features they believe should be added to the interim standard to correct its deficiencies.

- On April 2, 1998, TIA files a petition for rulemaking, asking the FCC to resolve the dispute as to whether the industry standard is over-inclusive or under-inclusive and to provide guidance to telecommunications equipment manufacturers. TIA requests that the FCC: (1) immediately announce suspension of enforcement of CALEA until the FCC issues its final determination; (2) establish, at the beginning of the rulemaking, a reasonable compliance schedule of at least 24 months to implement the FCC's final decision; (3) undertake an expedited schedule for addressing the issues; and (4) remand any further technical standardization work to the TIA subcommittee that issued the interim industry standard.

- On March 30, 1998, AT&T Wireless Services, Lucent Technologies, and Ericsson file a petition seeking an extension of CALEA's October 25, 1998, compliance date until at least October 24, 2000. The parties contend that an extension is necessary because CALEA-compliant hardware and software would not be available within the compliance period. The parties further state that developing an industry solution in the face of the unstable industry standard would expose the vendors to potentially enormous expense of money and engineering resources because any modification to the existing industry standard could require significant changes in Lucent's or Ericsson's individual CALEA solution.

- On a related matter, on July 16, 1997, the Cellular Telecommunications Industry Association (CTIA) submits a petition for rulemaking requesting the FCC establish standards to implement the assistance capability requirements of CALEA. CTIA contends that the industry standard-setting process is at an impasse between industry and law enforcement over capabilities that should be included in a standard.

- On March 27, 1998, the FBI and DOJ file a joint motion requesting the FCC to dismiss CTIA's petition on the grounds that the adoption of the interim industry standard now renders the CTIA petition moot and that the joint petition filed by the FBI and DOJ supersedes it in terms of relevancy and accuracy.

September 10, 1998
Memorandum Opinion and Order

The FCC grants a blanket extension for compliance with CALEA to June 30, 2000, based on the determination that compliance with the assistance capability requirements is not reasonable for telecommunications carriers because of the lack of equipment for meeting the requirements.

October 22, 1998
Further Notice of Proposed Rulemaking

The FCC addresses deficiencies in industry-developed technical requirements for wireline, cellular, and broadband Personal Communications Services (PCS) carriers to comply with CALEA's assistance capability requirements. The FCC is petitioned to establish the capability requirement by rule because of the differences between the industry's interim standard and law enforcement's punchlist. The FBI's objections to the industry-developed standards center on a list of technical capabilities that it contends are necessary to meet CALEA's requirements, but that were not included in the industry interim standard. In this Further Notice of Proposed Rulemaking, the FCC tentatively concludes that six punchlist items are technical requirements that fall within the scope of terms defined under CALEA's assistance capability requirements.

January 29, 1999
Report and Order

On October 10, 1997, the FCC releases an NPRM focusing on the specific responsibilities imposed upon the FCC to implement certain sections of CALEA. Since that time, the FCC has addressed two very significant CALEA implementation issues by granting a blanket extension of CALEA's October 25, 1998, compliance deadline for all telecommunications carriers until June 30, 2000, and by initiating a Further NPRM to resolve the dispute regarding the industry's interim standard. In this order, the FCC establishes the systems security and integrity regulations that telecommunications carriers must follow to comply with CALEA. The FCC concludes that telecommunications

carriers must ensure that "any interception of communications or access to call-identifying information affected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier."

February 26, 1999
Order

The FCC approves requests for confidential treatment of specific cost estimates filed by five telecommunications equipment manufacturers on December 14, 1998, in response to the Further NPRM. Manufacturers, Alcatel, Lucent, Motorola, Nortel Networks, and Siemens, previously had filed specific cost data with a request that the data be treated as confidential material.

In that Notice, the FCC strongly encourages commenters to provide it with information as detailed and specific as possible regarding the costs of adding a feature to a telecommunications carrier's network and what, if any, impact such costs will have on residential ratepayers. Commenters are to consider the costs to manufacturers in developing the equipment or software needed to implement the technical requirement, as well as the cost to carriers to install and deploy such equipment. Commenters are to be specific as to which entities would incur the cost of adding particular features; e.g., manufacturers, local exchange carriers, interexchange carriers, or commercial mobile radio service providers. Commenters are also to be specific as to what costs would be incurred for hardware, as opposed to software upgrades to carriers' networks, and whether some of these upgrades would have other uses in the networks. If costs are likely to be passed on to residential ratepayers, those costs are to be identified, as well as specific mechanisms that could be used to minimize such costs.

May 7, 1999
Public Notice

The FCC requests comment on aggregated revenue estimates prepared by the FCC from confidential carrier submissions for compliance with CALEA:

Estimated[85]			
Capability	**Total Revenue[86] ($millions)**	**Wireless Revenues ($millions)**	**Wireline Revenues ($millions)**
J-STD-025	$916	$348	$569
Subject-initiated conference calls	$37	$15	$22
Party hold, join, drop messages	$64	$42	$22
Subject-initiated dialing and signaling	$35	$27	$8
In-band and out-of-band signaling	$57	$30	$27
Timing Information	$20	$13	$8
Surveillance status messages	$37	$24	$13
Continuity check tones	$3	$3	$0
Feature status messages	$40	$19	$21
Dialed digit extraction	$121	$60	$60
Total Punchlist	$414	$234	$180

July 16, 1999
Order on Reconsideration

In the January 29, 1999, Report and Order, the FCC sets forth carrier recordkeeping requirements concerning interceptions, and establishes record retention periods of 10 years for call-identifying information and unauthorized interceptions, including the content of such interceptions, and a carrier-determined "reasonable" period for the call content of authorized interceptions.

[85] Sums in the table may not add to totals due to rounding. Also, the total punchlist figures include $500,000 in estimated wireless revenues that cannot be attributed to any individual punchlist capability.

[86] Revenues are the prices the manufacturers plan to charge multiplied by the quantities they anticipate selling, and may include profits. Some of the manufacturers supplied price and quantity data, thus enabling revenues to be calculated, while others supplied revenue data directly. None of the manufacturers supplied profit data.

After the release of the Order and prior to publication of the rules in the *Federal Register*, the FCC receives letters from CTIA and AirTouch stating that the new rules erroneously require carriers to retain records of call-identifying information and unauthorized interceptions, including the content of such interceptions, and also erroneously required carriers to retain records of content of authorized interceptions.

Subsequently, the FBI sends the FCC a letter supporting the position taken by CTIA and AirTouch on this issue, stating that those requirements are not mandated by CALEA, and that, in some respects, compliance with the requirements could cause a carrier to violate federal electronic surveillance laws since those laws do not require or entitle carriers to acquire and retain such information, but merely direct them, according to lawful court orders and other authorizations, to provide the technical assistance necessary to aid law enforcement in making intercepts.

Therefore, the FCC rules that carriers should not retain the content or call-identifying information of any intercepts and that carriers only need retain a certification of the intercept for a reasonable period of time, rather than for 10 years.

August 26, 1999
Second Report and Order

The FCC addresses the definition of "telecommunications carrier" set forth in Section 102 of CALEA that determined which entities and services are subject to the assistance capability and other requirements of CALEA. After considering the definition set forth in CALEA and the relevant legislative history, the FCC discusses how the definition applies to various types of service providers. Further, the FCC provides guidance regarding the factors it will consider in making determinations under Section 109 of CALEA. The guidance looks at whether compliance with CALEA's assistance capability requirements is reasonably achievable for particular carriers, and the showings it expects entities to make when filing petitions under Section 109.

August 26, 1999
Third Report and Order

The FCC adopts technical requirements for wireline, cellular, and broadband Personal Communications Services (PCS) carriers to comply with CALEA's assistance capability requirements. Specifically, the FCC requires that all capabilities of J-STD-025 (interim standard) and six of the nine punchlist capabilities requested by DOJ and the FBI be implemented by wireline, cellular, and broadband PCS carriers. While the FCC also requires that a packet-mode capability be implemented by such carriers, it does not adopt technical requirements for packet-mode communications, but permits packet-mode data to be delivered to law enforcement under the interim standard pending further study of packet-mode communications by the telecommunications industry.

June 30, 2000
Public Notice

The FCC requests public comments on petitions from carriers seeking deadline extensions for complying with CALEA. According to the Public Notice, most of the petitioners satisfy the requirements set out in the CALEA Public Notices for a preliminary determination that their circumstances warrant an extension of the compliance deadline. Accordingly, those petitioners are deemed to have an extension of the deadline for complying with CALEA Section 103 until March 31, 2001.

November 20, 2000
Public Notice

The FCC requests public comments on petitions from additional carriers, who were not covered by the June 30, 2000, Public Notice, seeking deadline extensions for complying with CALEA. According to the Public Notice, the petitioners satisfy the requirements set out in the CALEA Public Notices for a preliminary determination that their circumstances warrant an extension of the compliance deadline. Accordingly, the petitioners are deemed to have an extension of the deadline for complying with CALEA Section 103 until March 31, 2001.

February 22, 2001
Public Notice

The FCC requests public comments on petitions from more carriers seeking deadline extensions for complying with CALEA. According to this Public Notice, on November 20, 2000, preliminary extensions for complying with CALEA are granted to about 1,000 carriers until March 31, 2001.

In this Public Notice, the FCC finds that additional carriers have satisfied the requirements warranting an extension of the compliance deadline. The FCC concludes that a carrier's participation in the FBI's Flexible Deployment Initiatives enables the FCC to satisfy its statutory obligation to consult with the FBI, and assists the FCC in determining whether an extension is warranted and the length of any extensions of the compliance deadline. Therefore, the March 31, 2001 deadline is further extended until June 30, 2001.

March 15, 2001
Public Notice

Pursuant to a recommendation from the FBI and a letter in support filed by the CITA, the FCC extends the preliminary determination period for wireless carriers seeking extensions of the deadline for complying with CALEA from March 31, 2001, to September 30, 2001.

April 9, 2001
Second Order on Reconsideration

This Order resolves two petitions for reconsideration of the January 29, 1999, Report and Order and the August 26, 1999, Second Report and Order. The FCC declines to make most of the proposed changes, but does adopt minor changes to its CALEA rules regarding recordkeeping and points of contact.

May 31, 2001
Public Notice

The FCC requests public comments on more petitions from wireline carriers seeking deadline extensions for complying with CALEA. The FCC has previously granted extensions from March 31, 2001, to June 30, 2001, for these wireline carriers and the carriers requesting extensions in the Public Notices from November 20, 2000, and February 22, 2001.

June 22, 2001
Public Notice

The FCC requests public comments on wireline carriers's petitions seeking extensions for complying with CALEA. The FCC has previously granted extensions from June 30, 2001, to September 30, 2001, for the wireline carriers requesting extensions in the Public Notices from November 20, 2001, February 22, 2001, and March 15, 2001.

August 14, 2001
Order

Approximately 700 wireline carriers are granted extensions of the deadline for complying with the CALEA assistance capability requirements. The FCC finds that compliance with the assistance capability requirements is not reasonably achievable.

In January 2000, the FBI establishes a Flexible Deployment Initiative to assist telecommunications carriers in meeting certain requirements of CALEA. In its Flexible Deployment Assistance Guide, the FBI requests that carriers voluntarily submit certain information, and explains under what circumstances, based on a review of that information, the FBI might support a carrier's petition for an extension filed with the FCC.

A carrier's participation in the FBI's Flexible Deployment Initiative enables the FCC to satisfy its statutory obligation to consult with the FBI, and assists the FCC, both in determining whether an extension of the compliance deadline and the length of any extension are warranted. Under the initiative's procedures, the FBI, among other things, independently reviews each carrier's extension request in light of the CALEA priorities of law enforcement agencies. If, after reviewing the information, the carrier and the FBI are able to arrive at a mutually agreeable CALEA deployment schedule, the FBI issues a letter of support stating whether the FBI supports an extension request and, if so, the length of such extension. Each carrier covered by this order participates in the FBI's Flexible Deployment Initiative and receives a letter of support.

September 18, 2001
Order

The FCC temporarily suspends the September 30, 2001, compliance date for wireline, cellular, and broadband PCS carriers to implement two punchlist electronic surveillance capabilities mandated by the Third Report and Order dated August 26, 1999. In that Order, the FCC required that wireline, cellular, and broadband PCS carriers implement all electronic surveillance capabilities of the industry interim standard, J-STD-025 – including two contested features of the interim standard, i.e., a packet-mode communications capability and a location information requirement – and six of nine additional capabilities requested by the FBI, known as the punchlist capabilities.

The FCC notes that the U.S. Court of Appeals for the District of Columbia Circuit has vacated and remanded four of the six punchlist capabilities because the FCC failed to explain its decision-making process in the Order. In addition, it states that there is broad agreement among industry and law enforcement to suspend the September 30, 2001, compliance deadline for two unchallenged punchlist capabilities, pending final action by the FCC on what punchlist capabilities will be required. The FCC agrees with the majority of commenters that retaining the deadline for two of the punchlist capabilities prior to determining the disposition of the four punchlist capabilities vacated by the court could result in major inefficiencies for carriers. The FCC states that it will establish a new compliance date for all required punchlist capabilities of no later than June 30, 2002.

The FCC also states that it found no need to extend the September 30, 2001, compliance deadline for packet-mode communications in a blanket manner. The FCC finds that implementation of this capability is unrelated to the implementation of the punchlist capabilities, and that only a small percentage of telecommunications carriers use packet-mode technology. Nonetheless, the FCC decides, due to the imminence of the September 30, 2001 deadline, to give carriers a brief period of time to upgrade their systems to incorporate the packet-mode capability or to avail themselves of established petition procedures for individual relief under Section 107 of CALEA.

September 27, 2001
Order

This Order provides an extension of the deadline date, or the preliminary extension period, as applicable, to December 31, 2001, for the carriers listed in the August 14, 2001, Order to comply with the assistance capability requirements based on the FCC's determination that compliance was not reasonably achievable through application of technology available.

September 28, 2001
Public Notice

This Public Notice provides an explanation of the petitioning process for carriers seeking an extension of the CALEA compliance deadline with respect to packet-mode communications by the November 19, 2001, deadline.

February 28, 2002
Order

This Order provides an extension of the deadline date, or the preliminary extension period, as applicable, to March 31, 2002, for the carriers listed in the Appendices of the Order to comply with the assistance capability requirements. The FCC determines that compliance was not reasonably achievable through application of available technology.

April 5, 2002
Order on Remand

The FCC responds to a decision issued by the U.S. Court of Appeals for the D.C. Circuit that vacated four punchlist electronic surveillance capabilities mandated by the Third Report and Order. The FCC determines that the four punchlist capabilities were authorized by CALEA and must be provided by wireline, cellular, and broadband PCS telecommunications carriers, along with the two non-disputed punchlist capabilities by June 30, 2002.

February 12, 2004
Memorandum Opinion and Order

The FCC rules, based on a petition of Pulver.com, that Pulver.com's Free World Dialup (FWD) (a broadband Internet service allowing worldwide users to communicate with one another through video or text), is an information service under CALEA, rather than a telecommunications carrier. Through FWD, Pulver offers users of broadband Internet access services the opportunity to join other such users in becoming members of the FWD community in order to communicate directly with one another over the Internet.

August 4, 2004
Notice of Proposed Rulemaking and Declaratory Ruling

In response to DOJ's *Joint Petition,* the FCC tentatively concludes that: (1) Congress intended the scope of CALEA's definition of "telecommunications carrier" to be more inclusive than that of the Communications Act; (2) facilities-based providers of any type of broadband Internet access service, whether provided on a wholesale or retail basis, are subject to CALEA; (3) "managed" VoIP services are subject to CALEA; (4) the phrase in CALEA stating "a replacement for a substantial portion of the local telephone exchange service" calls for assessing the replacement of any portion of an individual subscriber's functionality previously provided via "plain old telephone service;" and (5) call-identifying information in packet networks is "reasonably available" under CALEA if the information is accessible without "significantly modifying a network." The FCC requests comments on: (1) the feasibility of carriers relying on a trusted third party to manage their CALEA obligations and to provide law enforcement agencies the electronic surveillance information they require in an acceptable format; and (2) whether standards for packet technologies are deficient and should not serve as safe harbors for complying with Section 103 capability requirements.

The FCC also proposes mechanisms to ensure that telecommunications carriers comply with CALEA by restricting the availability of compliance extensions under CALEA Section 107 and clarifying the scope of CALEA Section 109, which addressed the cost payments to carriers to comply with CALEA capability requirements.

The FCC also discusses whether, in addition to the enforcement remedies made through the courts that are available to law enforcement agencies under CALEA Section 108, the FCC may take separate enforcement action against carriers that fail to comply with CALEA. The FCC tentatively concludes that carriers are responsible for

CALEA development and implementation costs for post-January 1, 1995, equipment and facilities; seeks comment on cost-recovery issues for wireline, wireless and other carriers; and refers to the Federal-State Separations Joint Board cost-recovery issues for carriers subject to Title III of the Communications Act. In the Declaratory Ruling, the FCC clarifies that commercial wireless "push-to-talk" service continues to be subject to CALEA, regardless of the technologies that Commercial Mobile Radio Service providers choose to apply in offering them.

August 5, 2005
First Report and Order and Further Notice of Proposed Rulemaking

In response to the DOJ's *March 2004 Joint Petition*, the FCC concludes that CALEA applies to facilities-based broadband Internet access providers and providers of interconnected VoIP service. The FCC will release another Order that addresses the assistance capabilities required of the providers covered by this Order, compliance extensions and exemptions, cost recovery, identification of future services and entities subject to CALEA, and enforcement. The FCC states that it is taking a two-step approach to focus debate on the implementation rather than the applicability of CALEA to providers of broadband Internet access services and VoIP services. By clarifying the applicability of CALEA to these providers now, the FCC can enable them to begin planning to incorporate CALEA compliance into their operations. This will also ensure that the appropriate parties become involved in ongoing discussions among the FCC, law enforcement, and telecommunications industry representatives to develop standards for CALEA capabilities and compliance.

In this *Further Notice*, the FCC seeks comment on two aspects of the conclusions it reached in the Order. First, with respect to interconnected VoIP, the FCC seeks comment on whether it should extend CALEA obligations to providers of other types of VoIP services. Second, some commenters argued that certain classes of facilities-based broadband Internet access providers – notably small and rural providers and providers of broadband networks for educational and research institutions – should be exempt from CALEA. The FCC does not reach conclusion in this Order on these issues because it believes that additional information is necessary. In this *Further Notice*, the FCC seeks comment on the appropriateness of requiring something less than full CALEA compliance for certain classes or categories of providers, as well as the best way to impose different compliance standards.

PRIOR OIG REPORTS

In March 1998, the OIG reported that the FBI and the telecommunications industry disagreed over what capabilities had to be provided for a carrier to be CALEA-compliant and eligible for reimbursement (see OIG Report No. 98-13). At that time, the carriers had not modified any equipment pursuant to CALEA, and the FBI had not made any payments to the carriers.

In March 2000, the OIG reported that the FBI had begun negotiations with carrier and manufacturer representatives to determine the most appropriate way to arrange for carriers to meet the assistance capability requirements (see OIG Report No. 00-10). The OIG reported that the FBI had entered into RTU license agreements with a manufacturer (Nortel) and certain carriers to permit all carriers who were using specified Nortel equipment, the use of the CALEA software solutions developed by Nortel. The FBI negotiated a price of $101.8 million for carrier purchase of these RTU software licenses, with payments made to Nortel on behalf of all carriers who used the Nortel equipment specified in the agreement.

In March 2002, the OIG reported that the FBI had paid or obligated about $400 million for carrier purchases of the RTU software licenses to: Lucent Technologies - $170 million, Nortel - $102 million, Motorola - $55 million, Siemens AG - $40 million, and AG Communications - $30 million (see OIG Report No. 02-14). The OIG also reported that the FBI had not entered into any agreements to reimburse carriers for activation of the software developed under the RTU agreements. At that time, the FBI estimated that for each additional $100 million in funding, capability solutions could be deployed in at least 25 percent of the locations prioritized by the FBI. The FBI had previously identified carrier equipment locations with high electronic surveillance activity and determined these to be priority locations for the deployment of the electronic surveillance standards.

In April 2004, the OIG reported that after more than nine years and nearly $450 million in payments or obligations, deployment of CALEA technical solutions for electronic surveillance remained delayed. The FBI did not collect and maintain data on carrier equipment that was CALEA-compliant. Nevertheless, FBI personnel estimated that CALEA-compliant software had been activated on approximately 50

percent of pre-January 1, 1995, and 90 percent of post-January 1, 1995, wireless equipment. In addition, according to FBI estimates, CALEA-compliant software had been activated on only 10 to 20 percent of wireline equipment.

FBI personnel advised us that law enforcement agencies were unable to properly conduct electronic surveillance on equipment for which the CALEA-compliant software had not been activated. However, the FBI was unable to demonstrate the extent to which lawful electronic surveillance had been adversely impacted by the lack of CALEA implementation. The OIG concluded that it was critical that the FBI collect data on carrier compliance and the impact of non-compliance on enforcement to determine the extent to which electronic surveillance was being compromised.

The OIG also reported that although the FBI had made about $450 million in payments and obligations to equipment manufacturers for RTU licenses, except for a one-time payment of $2.2 million, the FBI had not yet made any payments from CALEA funds to telecommunications carriers for activation of CALEA-compliant software.[87] Furthermore, cost estimates from the FBI suggested that the current funding level of $500 million for CALEA was insufficient. In December 2003, the FBI estimated that about $204 million in additional funds might be required; however, because cost estimates for CALEA implementation varied widely, and technological change continued to occur at a rapid pace the OIG was skeptical of the accuracy of the FBI's estimates or whether CALEA's implementation cost could be determined with any specificity.

[87] The FBI entered into a $6.2 million agreement with Qwest to ensure that its network in Salt Lake City was CALEA-compliant for the 2002 Winter Olympics. Of this amount, $4 million came from FBI Counterterrorism funds and $2.2 million came from CALEA funding.

Appendix VI

Unsuccessful Proposed CALEA Amendments

March 1998
H.R. 3321

This measure, in its original form, would have drastically altered CALEA by expanding 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 have also extended 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 would not perform modifications that qualify for years to come.

April 1998
Proposed Amendment to the House Judiciary Committee

In April 1998, an amendment was proposed to the House Judiciary Committee to change certain aspects of CALEA. The amendment, very similar in language to H.R. 3321, was withdrawn following dialogue with the Chair of the House Judiciary Committee's Subcommittee on Crime. According to the FBI, 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."

June 1998
H.R. 3303

In June 1998, the Chairman of the House Judiciary Committee introduced an amendment to change the two dates specified in CALEA. The amendment was passed by the Full House of Representatives. As part of the Department of Justice's Appropriations Authorization Bill, H.R. 3303 would have extended the October 25, 1998, capability compliance deadline to October 1, 2000. It would also have extended the January 1, 1995, financial demarcation date to October 1, 2000.

July 1999
H.R. 916

In July 1999, the House of Representatives passed H.R. 916. The bill would have drastically altered many of the provisions of CALEA under the guise that it was introduced to make technical amendments to Section 10 of Title 9 of the U.S. Code and "for other purposes."

H.R. 916 would have amended CALEA by adding separate definitions of the terms “installed” and “deployed” that incorporate the phrase “commercially available anywhere” with no consideration to whether a specific piece of equipment is in use and providing service. H.R. 916 also added a definition of the term “significantly upgraded or otherwise undergoes a major modification” to apply to a carrier’s *entire* network and not to specific pieces of equipment such as switches. H.R. 916 eliminated CALEA’s Section 107 (a)(3) in its entirety. Section 107(a)(3) is the only provision within CALEA that mandates industry comply with the obligations of CALEA “in the absence of technical standards.” Absent this provision, industry has no incentive to develop technical standards. H.R. 916 would have moved the reimbursement eligibility date from January 1, 1995, forward to June 30, 2000.

April 2004

VoIP Regulatory Freedom Act of 2004 (S. 2281)

The overarching aim of S. 2281 was to significantly reduce the regulatory burden that may otherwise have been imposed on voice communications employing this technology. The bill preempted the states from regulating the service. Importantly, S. 2281 addressed law enforcement access to VoIP applications. However, the bill only mandated law enforcement’s access to information be “not less than that required of information service providers.” The bill also stated that information service providers are explicitly exempt from the requirements of CALEA, and therefore do not have any affirmative obligation to design into their services the capabilities law enforcement needs to conduct electronic surveillance. According to the FBI, with no inherent electronic surveillance capability, all levels of law enforcement would have been placed in the position of expending incalculable resources, or foregoing the use of electronic surveillance, in any investigation involving VoIP services.

Summary of Comments to the Notice of Proposed Rulemaking

Department of Justice

- The FCC should conclude that CALEA is applicable to providers of broadband Internet access service and certain types of VoIP because it serves the public interest and is consistent with Congress's intent.

- Most commenters do not favor any special legal status for TTP solution vendors. Telecommunications vendors must remain fully involved in designing CALEA solutions for their telecommunications carrier customers. TTPs should not be used to determine whether call-identifying information is reasonably available. TTP solutions are not comparable to safe-harbor solutions. TTPs should not be used to shift financial responsibilities from carriers to law enforcement. Special security and privacy safeguards are needed for TTPs.

- The FCC was correct in concluding that Section 107(c) extensions are not available to cover equipment, facilities, or services installed or deployed after October 25, 1998.

- There is a broad consensus among commenting parties that the FCC has the authority to impose CALEA compliance deadlines.

- The FCC has the authority to adopt and enforce CALEA rules under Section 229 of the Communications Act.

- The comments filed in this proceeding demonstrate that specific rules regarding carrier responsibility for CALEA development and implementation costs for post-January 1, 1995, equipment and facilities are needed to ensure compliance.

- The FCC should consider all viable proposals for carrier recovery of CALEA development and implementation costs, but should not adopt any proposal that would permit carriers to recover such costs from law enforcement.

- Without adequate evidence of the scope of CALEA costs, the FCC should not allow carriers to continue to use cost as an excuse for non-compliance with CALEA.

- The information provided by commenters shows that CALEA compliance costs are manageable.

- Carriers should not be allowed to use lack of government funding as an excuse for non-compliance with CALEA.

- The comments filed in this proceeding make clear that the FCC must distinguish between CALEA implementation costs and CALEA intercept costs.

Verizon

- The FCC should affirm its tentative conclusion that whether CALEA applies to a particular service is independent of how such a service is classified for regulatory purposes under Title I or Title II of the Communications Act. Any approach that attempted to read the two statutes in parallel would contradict the plain language of CALEA by ignoring the "substantial replacement" provision of its definition of "telecommunications carrier" and would undermine the statute's purposes.

- The FCC should affirm its tentative conclusion that VoIP services fall within the substantial replacement provision of CALEA because they can be used to make voice phone calls that have traditionally been provided using local telephone exchange service.

- The FCC should not adopt its proposed "managed v. non-managed" test for determining which specific VoIP services are subject to CALEA. Instead, it should adopt a test by which any VoIP provider that uses equipment such as application servers, media gateways, or networks falls within CALEA, regardless of whether the service may be labeled as "non-managed" or "peer to peer."

- The FCC should make clear that any CALEA obligations fall equally on all competing providers of broadband access services.

- The FCC should reaffirm the admonition in CALEA's legislative history that CALEA was not intended to provide "one stop shopping" for law enforcement and that, to the extent broadband access service providers are subject to CALEA, in many cases the underlying network provider will not be the entity responsible for providing law enforcement with the relevant call-identifying information or content.

- The FCC should affirm its tentative conclusion not to require any "pre-approval" process. The FCC should also reject DOJ's proposed procedures and requirements for seeking CALEA rulings in advance of deploying new services, as well as its suggestion that carriers that do not employ such procedures will face more vigorous enforcement.

- The FCC should resolve technical issues relating to call-identifying information in the standards process instead of this proceeding and it should not require any carrier to use a "trusted third party" approach to CALEA compliance.

- The FCC should not create any additional enforcement procedures because they are both unnecessary and contrary to CALEA.

- The FCC should not adopt DOJ's suggestion that CALEA precludes any recovery of so-called "capital costs" for post-1995 equipment.

Sprint

- Sprint supports law enforcement CALEA objectives.

- Sprint also agrees with DOJ that the FCC should not address in this general rulemaking proceeding the sufficiency of any industry CALEA packet-mode standards.

- The FCC does not possess the authority to adopt a new CALEA enforcement regime in addition to one that Congress has already established.

- Section 107(b) authorizes the FCC to grant extensions for packet-mode services.

- The adoption of "one size fits all" Section 109(b) rules may not achieve the desired objective.

- Carriers can recover their CALEA "capital costs" from law enforcement agencies as a matter of law.

- There is no basis to adopt different rules for small carriers.

Bell South

- The industry should continue to take the lead in developing CALEA standards as intended by Congress.

- The scope of a provider's CALEA obligations varies with the type of service at issue.

- The FCC must adopt reasonable compliance deadlines that take into account the time necessary to develop standards, design products, and deploy CALEA solutions in carrier networks.

- The FCC's proposed framework for considering Section 109(b) petitions is far too stringent.

- CALEA enforcement lies exclusively with the federal courts.

- Requiring providers to bear the sole responsibility for CALEA implementation costs is inconsistent with CALEA.

- The FCC should allow, but not require, providers to use trusted third parties to satisfy their CALEA obligations.

SBC

- The FCC should seek extensive input from industry experts before addressing complex technical issues, such as the definitions of call-identifying information and call content.

- The FCC must give the communications industry a reasonable amount of time to develop and implement standards.

- The FCC must not limit the extension process to equipment, facilities, and services installed or deployed prior to October 25, 1998.

- The FCC should reject law enforcement's self-serving and legally suspect arguments regarding cost recovery.

Vonage

- The FCC should seek more specificity concerning problems faced by law enforcement.

- If CALEA is found to apply, the FCC must give effect to all of the statute's provisions including cost recovery and a reasonable compliance timeframe.

- Application of CALEA to VoIP providers based on a "managed/non-managed" distinction will leave doors wide open for bad actors, eliminating law enforcement benefit of CALEA application to VoIP and creating incentives for them to move to "non-managed" technologies.

Earthlink

- The FCC's tentative conclusion that the information services component of broadband Internet access services are subject to CALEA is in violation of the statute.

- The FCC may not write the "information services" exclusion out of CALEA.

- The FCC's reading of the "substantial replacement" provision in CALEA is not supported by the plain language of the statute.

- If the FCC's tentative conclusion is adopted in its current form, it will be successfully challenged in court, causing continued industry uncertainty and preventing law enforcement from getting the access it has requested.

Verisign

- The principal issue in this proceeding revolves around the question of who bears the costs for the imposed capability requirements.

- Almost every commenting party strongly supported the use of trusted third party service bureaus to meet the capability requirements.

- Although the time to act is now, the FCC can take additional actions to further reduce the burdens and costs.

- The FCC should treat additional significant law enforcement support capabilities in a subsequent phase of this proceeding.

FBI Ad Hoc Solutions

When technologies are not covered by CALEA, or when a covered technology is not CALEA-compliant, the FBI works to develop an "ad hoc solution" to allow law enforcement to conduct the electronic surveillance it needs. The FBI provided us with some examples:

- System DCS-3000. The FBI has spent nearly $10 million on this system. The FBI developed the system as an interim solution to intercept personal communications services delivered via emerging digital technologies used by wireless carriers in advance of any CALEA solutions being deployed. Law enforcement continues to utilize this technology as carriers continue to introduce new features and services.

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

- Red Hook. The FBI has spent over $1.5 million to develop a system to collect voice and data calls and then process and display the intercepted information in the absence of a CALEA solution.

Appendix IX

CALEA Punchlist Items

Content of Subject-Initiated Conference Calls (Conference Calling). Capability that enables law enforcement to access the content of conference calls supported by the subject's service (including the call content of parties on hold).

Party Hold, Party Join, Party Drop (Multi-Party Call). Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined, has joined or has been dropped from the call.

Access to Subject-Initiated Dialing and Signaling (Dialing/Signaling Information). Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook and other feature keys).

In-Band and Out-of-Band Signaling (Ring/Busy Signal). A message would be sent to law enforcement when a subject's service sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or busy.

Timing to Associate Call Data to Content (Timing Information). Information necessary to correlate call identifying information with the call content of a communications interception.

Post-Cut-Through Dialed Digits (Dialed Digit Extraction). Extraction and delivery on a call data channel of call-routing digits dialed by a subject after the initial call setup is completed.

Cell Site Location. Although cell site location was not part of the punchlist, many law enforcement representatives we spoke with found this feature extremely useful. Cell site location allows law enforcement to track the movement of a target by monitoring the locations of the cell towers accessed during the target's cell phone calls.

Appendix X

OIG Survey to Law Enforcement

U. S. Department of Justice

Office of the Inspector General
Washington Regional Audit Office
1300 North 17th Street, Suite 3400
Arlington, Virginia 22209

The U.S. Department of Justice, Office of the Inspector General, is reviewing the progress of the Federal Bureau of Investigation (FBI) and the telecommunications industry in implementing the Communications Assistance for Law Enforcement Act of 1994 (CALEA). The purpose of CALEA was to ensure that law enforcement could continue to conduct lawful electronic surveillance in the face of rapidly changing technology. As part of this review, we are asking law enforcement personnel to complete the following survey about their use of electronic surveillance, and identify any problems they experienced with telecommunication carriers.

Please fax your completed survey to the attention of the CALEA Audit Team at (202) 616-4581 by April 8, 2005.

Please contact the members of the CALEA Audit Team at (202) 353-1721 or at (202) 616-3685, if you have any questions. If your division does not conduct electronic surveillance, please forward this survey to the appropriate official. If the official completing this survey is other than listed on the label below, please provide the correct information in the space provided. We appreciate your cooperation and prompt responses.

****

Name/Title: _____
Telephone: _____
E-mail: _____
Agency: _____
Address: _____
_____
City: _____ State: ____ Zip Code: _____

****

1. Did your agency conduct any wiretaps, pen registers, or traps and traces during calendar year 2004?

   ☐ Yes ☐ No ☐ Don't Know

2. If your agency did not conduct any electronic surveillance during 2004, please indicate the reason(s) why:

	Yes	No	Don't Know
Not necessary	☐	☐	☐
Could not afford	☐	☐	☐
Carrier unable to conduct intercepts	☐	☐	☐
Don't know how to conduct	☐	☐	☐

Other _____

(If your agency does not conduct electronic surveillance, stop here. Please fax only this page to the CALEA Audit Team at (202) 616-4581.)

3. How many electronic surveillances did your agency start in calendar year 2004?

   a. wiretaps _____
   b. pen registers _____
   c. traps and traces _____

4. Does your agency:
   - ☐ own a wire room
   - ☐ own a wire room in conjunction with another agency
   - ☐ use a wire room maintained by another agency
   - ☐ other _____

5. If your agency does not own a wire room, why?

	Yes	No	Don't Know
Cost of equipment	☐	☐	☐
Cost charged by carriers	☐	☐	☐
Cost of manpower to monitor	☐	☐	☐

Other _____

6. If your agency owns a wire room, how many simultaneous intercepts can this equipment handle? _____

7. Is this capacity sufficient for your agency's needs?
   ☐ Yes ☐ No ☐ Don't Know

8. Who was the vendor for the equipment in your wire room? _____

9. During which calendar year did your agency purchase this equipment? _____

10. How much did your agency originally pay for this equipment?
    _____

11. Has your agency paid for any of the following?
    - ☐ software upgrades --- Cost $_____
    - ☐ hardware upgrades --- Cost $_____
    - ☐ annual maintenance --- Cost $_____ (per year)
    - ☐ other _____

12. What was the total cost your agency paid to carriers for electronic surveillances started during calendar year 2004? _____

13. How much does your agency pay carriers to conduct a single electronic surveillance without CALEA features? _____

14. Is the number of electronic surveillances your agency conducts hindered by any of the following?

	Yes	No	Don't Know
Cost charged by carriers	☐	☐	☐
Cost to purchase equipment	☐	☐	☐
Cost of equipment maintenance	☐	☐	☐

Other _____

15. Has your agency encountered any of the following problems with carriers?

	Yes	No	Don't Know
Unable to conduct intercept	☐	☐	☐
Data provided in unreadable format	☐	☐	☐
Data not provided timely	☐	☐	☐
Unresponsive to requests for help	☐	☐	☐
Lacked technical expertise	☐	☐	☐

Other _____

16. Does your agency use any of the following CALEA features?

	Yes	No	Don't Know
Content of conference call	☐	☐	☐
Identification of parties of multiparty call	☐	☐	☐
Access to all dialing and signaling information	☐	☐	☐
Notification of ringing or busy signal	☐	☐	☐
Timing information	☐	☐	☐
Dialed-digit extraction	☐	☐	☐
Cell site location information	☐	☐	☐

Other _____

17. Do the following emerging technologies negatively affect your agency's ability to conduct electronic surveillances?

	Yes	No	Don't Know
Voice over Internet Protocol (VoIP)	☐	☐	☐
Pre-paid cell phones	☐	☐	☐
Pre-paid calling cards	☐	☐	☐
Telephony over Broadband (Cable)	☐	☐	☐
Text Messaging	☐	☐	☐
PDAs (Blackberry)	☐	☐	☐
Push-to-talk	☐	☐	☐
Camera phones	☐	☐	☐

Other _____

18. Have you contacted the FBI's CALEA Implementation Unit (CIU) or Engineering Research Facility (ERF) to obtain assistance regarding electronic surveillance?

☐ Yes ☐ No ☐ Don't Know

(If you answered No or Don't Know, please stop here.)

19. Have you received any of the following in relation to electronic surveillance from the FBI?

☐ Training ☐ Hardware ☐ Software ☐ Ad hoc solutions ☐ Don't Know
☐ None ☐ Other _____

20. Are you satisfied with the assistance provided by the FBI's CIU or ERF? If No, please discuss on a separate page the areas where the FBI can provide better assistance.

☐ Yes ☐ No ☐ Don't Know

Appendix XI

FBI RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

January 25, 2006

Mr. Troy Meyer
Regional Audit Manager
Washington Regional Audit Office
Office of the Inspector General
U.S. Department of Justice
1300 North 17th Street
Suite 3400
Arlington, VA 22209

RE: RESPONSE TO THE DRAFT REPORT OF THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

Dear Mr. Meyer:

The Federal Bureau of Investigation (FBI) has prepared comments and recommendation responses to the draft report of *The Implementation of the Communications Assistance for Law Enforcement Act* (Enclosure 1). Both the aforementioned and the draft report have undergone classification reviews (Enclosure 2). In addition, a Record of Sensitivity Review (Enclosure 3) and an electronic copy (Enclosure 4) of the recommendation responses are enclosed.

Please contact Ann G. S. Schultz of my staff should you have any questions. Ms. Schultz can be reached at (202) 324-6268.

Sincerely yours,

Charlene B. Thornton
Assistant Director
Inspection Division

Enclosures (4)

1 - Mr. Richard P. Theis
Director
Audit Liaison Group
U.S. Department of Justice
1425 New York Avenue, NW
Washington, DC 20005

Responses to Recommendations

The following paragraphs provide initial responses to each of the recommendations contained within the OIG Draft Report.

1. Testing

OIG Recommendation: *Coordinate with the DOJ and the telecommunications industry to determine the legality and feasibility of FBI-sponsored development and testing of manufacturers' CALEA solutions prior to their dissemination to carriers.*

The FBI will coordinate with DOJ to determine the legality of FBI-sponsored testing of CALEA solutions. The FBI believes it is well suited to test technical solutions from a law enforcement perspective. In fact, the FBI regularly tests solutions with manufacturers (including third-party solution providers) to ensure developed solutions meet the needs of law enforcement and provide all applicable call-identifying information and call content. The FBI established a testing program in conjunction with the reimbursement of the industry for nationwide Right-to-Use (RTU) software licenses and continues to dedicate those resources to the testing of industry-developed solutions. With respect to testing associated with the reimbursement of technical solutions, the FBI's testing program worked with carrier partners of sufficient size to be representative of networks adopting broad usage of those technical solutions.

As stated in the Draft Report, the FBI has concerns regarding carriers' suggestion that it oversee testing (from perspectives other than law enforcement's). Testing for all permutations of the effects of manufacturers' solutions within all providers' networks would impose an enormous burden on any organization. Further, the FBI neither believes it is well suited to conduct this type of testing, nor that the industry would agree to have the results of such FBI testing validate the efficacy of any manufacturer's solution and provide any level of indemnification regarding those solutions.

Finally, as also stated in the Draft Report, the FBI believes it is important to consider how testing is conducted for other services and features made available by equipment manufacturers. The FBI understands the industry makes use of a number of different testing models and will consult with DOJ regarding the appropriateness of using any of these industry models for future testing.

2. Expand State and Local Law Enforcement Participation

OIG Recommendation: *Expand the audience of state and local law enforcement representatives participating in its Law Enforcement Technical Forums and the FBI Threat Assessment Surveys. This would allow for a more comprehensive understanding of the electronic surveillance threats to law enforcement.*

The FBI generally agrees that more expansive participation by all levels of the law enforcement community would assist in the implementation of CALEA with respect to the development of a more comprehensive understanding of the electronic surveillance threats to law enforcement. The FBI remains dedicated to the continued involvement of law enforcement in the implementation of CALEA and has allocated significant resources since the enactment of CALEA to ensure the participation of the law enforcement community.

The FBI agrees with this recommendation and will, in the coming months, reach out to more law enforcement agencies using the same source material cited in the OIG Draft Report (i.e., National Law Enforcement Administrators Directory); its Internet website, www.AskCALEA.net; and other sources.

3. Methodology Assessing Impact of Non-Compliance with CALEA

OIG Recommendation: *Improve the methodology used to gather accurate and current data regarding the adverse impact on criminal investigations arising from carriers' inability to provide CALEA-compliant wiretaps or access to call-identifying information. This can be accomplished by soliciting detailed information on adverse responses to the Threat Assessment Survey, and through the CALEA helpdesk.*

The FBI believes the FBI's Threat Assessment Survey and CALEA Helpdesk are effective data collection tools that have been used in the past to gather data and will continue to be used for that purpose. The FBI regularly examines its survey forms and questions to ensure the most effective collection of data and is currently revising the Threat Assessment Survey to allow for the collection of specific data regarding the adverse impact from carriers' non-compliance with CALEA. In response to this recommendation, the FBI will re-assess its current Threat Assessment Survey in recognition of the need to collect more detailed information for adverse responses. The FBI will also correlate Threat Assessment Survey and Helpdesk information to provide a more comprehensive view of the technological impacts affecting law enforcement.

However, as the Draft Report acknowledged, there are a number of factors that limit the FBI's ability to collect valuable information from law enforcement regarding impacts on investigations. However, despite these limiting factors, the FBI will continue its efforts to improve the methods it uses to collect this valuable information.

4. Remaining TCCF Funding

OIG Recommendation: *Reexamine the benefits of activating CALEA solutions on wireline systems prior to the expenditure of the remaining $45 million in CALEA funding.*

The FBI agrees with this recommendation and will continue to periodically (e.g., bi-annually) assess its prioritization of funds associated the CALEA (i.e., the Telecommunications Carrier Compliance Fund [TCCF]) and strive to make the best use of available funds. The FBI has already utilized approximately 90 percent ($450 million of the available $499.5 million) of the funds appropriated to reimburse the telecommunications industry for technical solutions (i.e., RTU software licenses, dial-out delivery mechanisms, and deployment of solutions for two large carriers). The FBI's considerations with respect to the funds already expended and plans for future expenditures include:

- The recognition that the effectiveness of RTU software licenses, dial-out solutions, and deployment agreements are cumulative. The FBI will assess the benefit of pursuing reimbursement agreements to deploy technical solutions with wireline carriers which would maximize the effectiveness of the funds already expended.
- The FBI will assess the benefit to Federal, State, and local law enforcement of lowering wireline delivery costs while simultaneously decreasing the amount of time needed to provision an intercept by deploying the dial-out solution. As stated in the Draft Report, delivery methods of the industry greatly influence the costs of electronic surveillance to law enforcement. Reimbursing the deployment of dial-out solutions will greatly reduce those costs.
- The total amount of TCCF funds expended on two large wireline carriers for deployment of technical solutions (i.e., software activation) was $4.5 million. If the FBI pursues these solutions it expects to negotiate similar agreements with the remaining two large carriers and estimates that entering into software activation agreements with these carriers would make about 90 percent of the wireline switches CALEA-compliant.
- CALEA itself limits reimbursement to equipment, facilities, and services deployed on or before January 1, 1995. For equipment, facilities, and services deployed after January 1, 1995, a carrier must petition the FCC for a determination of whether compliance with the assistance capability requirements is reasonably achievable. To date, no such determination has been made by the FCC.

In the event petitions are filed before the FCC and determinations are made so that reimbursement may be made to telecommunications carrier for any additional, reasonable costs of making compliance with CALEA's assistance capability requirements, the FBI will assess the effectiveness of utilizing available funds for those purposes.

5. Training of State and Local Law Enforcement

OIG Recommendation: *Provide training for state and local law enforcement agents and technical personnel on how to conduct CALEA intercepts. In conjunction with this recommendation, the FBI should pursue legal clarification of Attorney General Order 1945-95 from the DOJ.*

The FBI agrees with this recommendation. The FBI's Operational [Investigative] Technology Division (OTD) routinely provides training to federal, state, and local law enforcement agents and technical personnel – it has a Unit specifically dedicated to the training of the FBI's technical agents as well as those of state and local law enforcement. Training includes CALEA intercepts and ad-hoc solutions developed by the FBI. The FBI conducted numerous training sessions in 2005, educating members of the federal, state, and local law enforcement community. Additionally, OTD makes available the results of its testing program to members of the law enforcement community and periodically makes available to the law enforcement community information on: new and converging technologies; the rapid introduction of new products and services; the expanding numbers of service providers; and global third party application providers - to facilitate better understanding of emerging technologies and their impact on law enforcement.

In prior years the FBI provided training to its Law Enforcement Technical Forum (LETF) membership through meetings. This training was funded with FBI resources dedicated to the implementation of CALEA. However, due to a lack of funding the FBI can no longer afford to provide as much training as in the past. The FBI believes training of federal, state, and local law enforcement can be more effectively addressed through a Congressionally mandated and funded Lawful Access Policy Office – an office with the specific responsibility to address electronic surveillance matters on behalf of the entire law enforcement community. In the absence of such a mandate and associated funding, the FBI will continue its policy of providing overarching support to the training and intercept needs of law enforcement to the extent its resources allow.

The FBI will, in conjunction with this recommendation, pursue legal clarification of Attorney General Order 1945-95 from the DOJ to permit the FBI to loan electronic surveillance equipment to state and local law enforcement agencies while ensuring appropriate safeguards exist to minimize the risk of disclosing sensitive intercept techniques.

6. Law Enforcement / Industry Liaison

OIG Recommendation: *Improve liaison between law enforcement officials and carrier and manufacturer representatives by providing a forum to address electronic surveillance issues. This would enhance carrier customer service and law enforcement officials' technical knowledge.*

The FBI agrees with this recommendation in that the FBI can facilitate liaison between law enforcement officials and carrier and manufacturer representatives by providing a forum to address electronic surveillance issues. However, as stated in the Draft Report, over the last decade, various forums have been held regarding the CALEA required capabilities such as telecommunications industry-sponsored legal summits, the FBI-sponsored Service Specific Document Summits, and conferences and summits held by various organizations (industry and privacy groups). These meetings have historically

allowed participants to express their views – often contentious and contradictory to each other. However, more recently there appears to be a willingness in some segments of industry to work more cooperatively with law enforcement. The FBI will re-examine its duties and capabilities within the scope of CALEA to assist in improving law enforcement's liaison with the industry.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

We provided a draft audit report to the FBI for review and comment. The response from the FBI is incorporated as Appendix XI of this final report. As part of its response to the draft report, the FBI suggested edits that we considered, and where appropriate, incorporated into the final report. The following contains our analysis of the FBI's response to the 6 recommendations.

Recommendation Number:

1. **Resolved.** This recommendation will remain resolved while the FBI coordinates with DOJ to determine the legality of FBI-sponsored testing of CALEA solutions. This recommendation can be closed when the FBI coordinates with DOJ and the telecommunications industry (as appropriate) to determine the legality and feasibility of FBI-sponsored development and testing of manufacturers' CALEA solutions prior to their dissemination to carriers.

2. **Resolved.** According to the FBI, in the coming months it will reach out to more law enforcement agencies using the National Law Enforcement Administrators Directory, its Internet website, and other sources. This recommendation can be closed when the FBI provides documentation of having reached out to more law enforcement agencies.

3. **Resolved.** In response to this recommendation, the FBI will assess its current Threat Assessment Survey in recognition of the need to collect more detailed information for adverse responses. The FBI will also correlate Threat Assessment Survey and Helpdesk information to provide a more comprehensive view of the technological impacts affecting law enforcement. This recommendation can be closed when the FBI provides us its revised survey, its procedures for correlating Threat Assessment Survey and Helpdesk information to obtain a more comprehensive view of the technological impacts affecting law enforcement, and more comprehensive information on adverse responses.

4. **Resolved.** The FBI agreed to reexamine the benefits of spending the funds remaining in the Telecommunications Carrier Compliance Fund (TCCF). This recommendation can be closed when we receive the FBI's analysis of the costs and benefits of future TCCF expenditures.

5. **Resolved.** The FBI agreed with the recommendation. In prior years, the FBI provided training to it Law Enforcement Technical Forum membership through meetings. This training was funded with FBI resources dedicated to the implementation of CALEA. However, the FBI stated that due to a lack of funding it can no longer afford to provide as much training as in the past. The FBI said it believes training of federal, state, and local law enforcement can be more effectively addressed through a Congressionally mandated and funded Lawful Access Policy Office – an office with the specific responsibility to address electronic surveillance matters on behalf of the entire law enforcement community. In the absence of such a mandate and associated funding, the FBI said it will continue its policy of providing overarching support to the training and intercept needs of law enforcement to the extent its resources allow. This recommendation will remain resolved while the FBI seeks adequate authority and appropriate funding to provide training for state and local law enforcement agents and technical personnel on how to conduct CALEA intercepts. In addition, the FBI will, in conjunction with the recommendation, pursue legal clarification of Attorney General Order 1945-95 from the DOJ to permit the FBI to loan electronic surveillance equipment to state and local law enforcement agencies while ensuring appropriate safeguards exist to minimize exist to minimize the risk of disclosing sensitive intercept techniques. This recommendation can be closed when the FBI either provides training for state and local law enforcement agents and technical personnel on conducting CALEA intercepts, or provides an alternative corrective action that will help state and local law enforcement agents and technical personnel in performing CALEA intercepts.

6. **Resolved.** The FBI agreed with this recommendation, and will examine its duties and capabilities within the scope of CALEA to assist in improving law enforcement's liaison with the telecommunications industry. This recommendation can be closed when the FBI develops and implements a plan for improving law enforcement's liaison with the telecommunications industry.