



IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT BY THE FEDERAL BUREAU OF INVESTIGATION

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 04-19
April 2004

**IMPLEMENTATION OF THE
COMMUNICATIONS ASSISTANCE FOR
LAW ENFORCEMENT ACT
BY THE FEDERAL BUREAU OF INVESTIGATION***

EXECUTIVE SUMMARY

Criminal organizations and individuals frequently use the telecommunications systems of the United States in the furtherance of serious violent crimes, including terrorism, kidnapping, extortion, organized crime, drug trafficking, and corruption. One of the most effective tools law enforcement uses to investigate these crimes is court-authorized electronic surveillance. According to Federal Bureau of Investigation (FBI) personnel, however, continuing advances in telecommunications technology have impaired and in some instances prevented telecommunication carriers (carriers) from assisting law enforcement to conduct authorized electronic surveillance.

Electronic surveillance is provided for in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986, which extended authorized lawful electronic surveillance to communications transmitted via wireless technology. In October 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) because of concerns that advances in telecommunications technology, such as cellular telephones and features such as call forwarding and multiparty calls, could limit the effectiveness of lawful electronic surveillance, especially at the state and local level. Law enforcement agencies at the state and local level often do not have the same level of resources or technical ability to conduct electronic surveillance as do federal law enforcement agencies. Because of this, CALEA required that carriers deploy electronic surveillance standards to ensure that technological advances in the telecommunications industry (industry) would not compromise the ability of law enforcement agencies to engage in lawful electronic surveillance.

* BECAUSE THIS REPORT CONTAINED PROPRIETARY/COMMERCIAL INFORMATION, WE REDACTED (WHITED OUT) THAT INFORMATION FROM THE VERSION OF THE REPORT THAT IS BEING PUBLICLY RELEASED. WHERE SUCH INFORMATION WAS REDACTED IS NOTED IN THE REPORT.

Proprietary/Commercial Information Redacted

CALEA provides that the Attorney General can reimburse telecommunications carriers for modifications to equipment, facilities, or services installed or deployed on or before January 1, 1995, to meet CALEA capability requirements.¹ Essentially, the capability requirements of CALEA require carriers to be able to isolate, intercept, and deliver communication content and call identifying information to law enforcement pursuant to lawful government order. The carriers are responsible for such modifications to equipment, facilities, and services installed or deployed after January 1, 1995.² To date, funding for CALEA implementation has totaled \$499.5 million.

Audit Results

CALEA requires biannual audit reporting on the equipment, facilities, and services that have been modified to comply with CALEA requirements; whether FBI payments to the carriers were reasonable and cost effective; and projections of future costs for such modifications.³ Consistent with these congressionally mandated audit objectives, we assessed CALEA's implementation to date. Our audit found the following:

- After more than nine years and nearly \$450 million in payments or obligations, deployment of CALEA technical solutions for electronic surveillance remains significantly delayed. The FBI does not collect and maintain data on carrier equipment that is CALEA compliant. Nevertheless, FBI personnel estimate that CALEA compliant software has been activated on approximately 50 percent of pre-January 1, 1995, and 90 percent of post-January 1, 1995, wireless equipment. Most troubling, according to FBI estimates, CALEA compliant software has been activated on only 10 to 20 percent of wireline equipment. FBI personnel advised that law enforcement agencies were unable to properly conduct electronic surveillance on equipment for which the CALEA-compliant software has not been activated. However, the FBI was unable to demonstrate the extent to which lawful electronic surveillance has been adversely impacted by the lack of CALEA

¹ CALEA vests authority for its implementation with the Attorney General. The Attorney General delegated this authority to the FBI pursuant to 28 CFR section 0.85(o).

² The carriers may request reimbursement for these modifications provided that the FCC has ruled that such modifications are not reasonably achievable.

³ The General Accounting Office performed the first biannual audit in 1996. The DOJ Office of the Inspector General (OIG) performed the audits in 1998, 2000, and 2002.

Proprietary/Commercial Information Redacted

implementation. We concluded that it was critical that the FBI collect data on carrier compliance and the impact of non-compliance on state and local law enforcement to determine the extent to which lawful electronic surveillance is being compromised.

- The FBI has made approximately \$450 million in payments and obligations to equipment manufacturers for Right-To-Use (RTU) licenses. A RTU software license allows a carrier to activate the software once the manufacturer has been reimbursed for its development costs. Except for a one-time payment of \$2.2 million, the FBI has not yet made any payments from CALEA funds to telecommunications carriers for activation of CALEA-compliant software discussed below.⁴ The FBI believed that first negotiating RTU licenses with manufacturers would ultimately lessen the cost for telecommunications carriers. Whether or not this is true will be determined as the FBI negotiates agreements with carriers to activate the software obtained under the RTU agreements.
- Cost estimates from the FBI suggest that the current funding level of \$500 million for CALEA is insufficient. In December 2003, the FBI estimated that about \$204 million in additional funds might be required. Estimates on the cost of CALEA implementation have varied widely, however, and technological change continues to occur at a rapid pace. For these reasons, we are skeptical of the accuracy of the FBI's estimates or whether CALEA's implementation cost can be determined with any specificity.

We found a variety of factors that have seriously complicated CALEA implementation, including: (1) delays in establishing electronic surveillance standards together with Federal Communications Commission (FCC) extensions, (2) contested cost recovery regulations, (3) carrier cost estimates that were viewed as exorbitant by the FBI, and (4) negotiating RTU licenses with equipment manufacturers. We describe each of these factors in turn.

⁴ 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.

Factors Complicating CALEA Implementation

Electronic Surveillance Standards

Electronic surveillance standards provide the basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting lawful electronic surveillance. Development of the initial electronic surveillance standards and obtaining agreement by all parties on their content has been a lengthy process. It was not until April 2002, nearly 8 years after CALEA was passed, that the FCC finally mandated electronic surveillance technical standards for wireline local exchange service, cellular, and broadband personal communications services. However, technical standards for other services such as packet-mode are still in the development stage.⁵

In June 1996, approximately two years after the enactment of CALEA, the Department of Justice (DOJ) issued the Electronic Surveillance Interface Document (ESI). The ESI set forth law enforcement surveillance capabilities, which were developed in consultation with law enforcement agency and industry representatives. In December 1997, the industry published Interim Standard J-STD-025 (known as the J-Standard) to meet the electronic surveillance capability requirements of CALEA. The J-Standard incorporated many of the standards set forth in the ESI but excluded several electronic surveillance capabilities deemed necessary to law enforcement. As a result DOJ filed a deficiency petition with the FCC in March 1998 because the J-Standard did not meet all the capabilities that law enforcement was seeking.

In September 1998, the FCC granted an extension to carriers of CALEA deadline for complying with CALEA capability requirements for equipment installed or deployed after January 1, 1995, from October 28, 1998, to June 30, 2000. This extension was granted on the basis that there was no technology currently available to permit carriers to deploy the minimum industry developed J-Standard capability standards.

⁵ Packet-mode is the digitalization of telecommunication transmissions so that a carrier can use its entire system to transmit a communication instead of dedicating a specific portion of the system for the transmission duration as with a conventional transmission. Packet-mode is more efficient and less costly because each digitized communication packet can travel the most direct system path.

Proprietary/Commercial Information Redacted

In August 1999, the FCC ruled that carriers must comply with additional requirements (punchlist) sought by the government and not included in the J-Standard. The FCC gave carriers until September 2001 to comply. The FCC also mandated that carriers provide the capability to intercept packet-mode communications by September 30, 2001. The industry appealed the FCC decision to United States Court of Appeals, District of Columbia Circuit. On August 21, 2000, the Court of Appeals ruled that each capability standard is required by CALEA, but remanded four of the challenged capabilities to the FCC for further proceedings (99-1442). In an April 11, 2002, Order on Remand, the FCC found that all of the punchlist requirements are required under CALEA and must be provided by wireline, cellular, and broadband telecommunications carriers by June 30, 2002. The FCC has continued to provide extensions of time for carriers with respect to post January 1, 1995 equipment. Also the FBI has not yet agreed to any carrier cost proposal to deploy the CALEA capability requirements on pre-January 1, 1995 equipment because the FBI considered the carriers cost estimates to be exorbitant as we describe below.

Cost Recovery Regulations

In March 1997, the FBI published the final cost recovery regulations (28 CFR Part 100), which set forth the procedures for carriers to follow in order to receive reimbursement for costs incurred in deploying their CALEA solution on their pre-1995 equipment. A CALEA solution is the standards that carriers adopt to be able to comply with law enforcement requests to conduct lawful electronic surveillance. Carriers will incur costs to deploy their CALEA solutions through activation of the software provided by manufacturers under the RTU agreements. The Cost Recovery Regulations became effective on April 21, 1997. Industry representatives filed a lawsuit in April 1998 in U.S. District Court for the District of Columbia (Court) challenging the definition of "installed or deployed" as the term applied to the January 1, 1995, cutoff for reimbursements to carriers. DOJ filed a motion to dismiss, and in August 2000 the Court ruled in favor of DOJ (98-2010).

Carrier Cost Proposals

According to the FBI, a primary reason for the delay in implementing CALEA have been exorbitant cost estimates by carriers. The FBI provided us with examples of several carrier proposals for deployment of their electronic surveillance capabilities. These included proposals from General Telephone and Electric (GTE), SBC Communications (SBC), and Verizon. As detailed

Proprietary/Commercial Information Redacted

below, the cost proposals for these three carriers alone exceeded the \$500 million authorized by Congress for CALEA implementation.

- GTE submitted its proposal in February 1999 prior to the RTU agreements and prior to its becoming part of Verizon. GTE estimated that the cost of deploying their CALEA solution throughout its entire network could exceed [Proprietary Information Redacted].
- SBC and Verizon cost estimates were submitted after the RTU agreements had been consummated and reflected the cost savings resulting from these agreements. The SBC cost proposal submitted in September 2000 showed an estimate of [Proprietary Information Redacted] for deployment of their CALEA solution.
- The FBI provided us with two examples of cost proposals submitted by Verizon. The first, submitted in June 2001, showed a cost estimate of [Proprietary Information Redacted] to deploy their CALEA solution throughout its network. The second proposal submitted by Verizon in July 2002 showed the total cost estimate to be [Proprietary Information Redacted].

The FBI recently received a proposal from a major telecommunications carrier to deploy its electronic surveillance solution on specified carrier priority equipment. FBI personnel were optimistic that an agreement could be negotiated with this carrier, and that this will lead to the deployment of a CALEA solution throughout a significant portion of this carrier's network. The FBI is hopeful that if agreement is achieved with this carrier, the possibility of negotiating reasonably priced agreements with other carriers will be increased.

Right to Use Licenses

A RTU software license allows a carrier to activate the software once the manufacturer is reimbursed for its development costs. The FBI entered into several RTU licensing agreements with manufacturers and carriers and has paid or obligated to manufacturers, primarily Nortel and Lucent, approximately \$450 million to permit carriers to obtain RTU software

licenses at no charge.⁶

These agreements were negotiated between February 1998 and April 2003. According to the FBI, it believed that negotiating RTU licenses with manufacturers for the use of their software would be a major advantage for the carriers and that nationwide software buyouts (FBI purchase of RTU licenses for all carriers that use a given manufacturers equipment) would be more cost effective than reimbursing individual carriers for the cost of this software. Under the RTU agreements, the manufacturers developed and made available the software with the necessary features for electronic surveillance needed in order for carriers to deploy their CALEA solutions.

In negotiating RTU agreements, the FBI General Counsel opined in February 1999 that "the proposed [RTU licensing] arrangement is a reasonable attempt to minimize the costs to the federal government because it reduces the potential for manufacturers to collect substantial profit from carriers who will in turn seek reimbursement from the federal government."⁷

Current and Future Issues

In addition to the past delays described above, we found several current and future issues that will likely have a direct impact on whether CALEA can be fully implemented. These are: (1) the sufficiency of current funding, (2) emerging technologies for which electronic surveillance standards are inadequate or not yet developed, and (3) legislative changes that are necessary to fully implement CALEA.

⁶ The manufacturers and the approximate amounts paid or obligated under RTU agreements were: Lucent (\$189 million), Nortel (\$113 million), Siemens (\$60 million) Motorola (\$55 million), and AG Communications (\$30 million).

⁷ In June 1999, the FBI prepared a Determination and Findings Regarding the Implementation of CALEA prior to entering into any RTU software license agreements. The FBI prepared this document because it was unable to determine the reasonableness of the cost of the RTU software licenses through traditional means, such as cost or price analysis. This was because the manufacturers were unwilling to furnish adequate cost or price information to the FBI in spite of repeated attempts by the FBI to obtain such information. As a result, the information given to us by the FBI was insufficient for use to determine the reasonableness of these costs. Accordingly, we were not able to offer an opinion on the reasonableness of the cost paid for the RTU software licenses.

Proprietary/Commercial Information Redacted

Future Funding Needs

As of the end of our audit fieldwork approximately \$50 million in unobligated funds remained for deployment of carrier electronic surveillance solutions and other FBI funding priorities such as wireless geo-location and trunk surveillance, which are described below.

	<u>Status of Funding</u>	
Appropriations		\$456,976,876
Funds from other sources ⁸		42,580,270
Total Received [a]		<u>\$499,557,146</u>
Less:		
Payments [b]		\$441,367,124
Obligations [c]		<u>8,664,775</u>
Unobligated Funds [a] less [b + c]		<u>\$ 49,525,247</u>

According to the FBI, cost estimates for obtaining CALEA compliance have varied widely. Prior to enactment of CALEA, industry estimated that CALEA compliance would cost from \$3 to \$5 billion. The FBI estimated the cost to be between \$500 million and \$1 billion. From 1998 to 1999, the industry estimates were reduced to \$1.3 billion. According to the FBI, manufacturers initially requested \$734 million for RTU software licenses in the early stages of negotiation with the FBI. Negotiations between the FBI and industry representatives reduced the final price to \$450 million.

In December 2003, the FBI estimated that an additional \$204 million would be necessary to complete deployment of CALEA solutions on carrier equipment in high priority areas and to conduct other current FBI priorities such as wireless geo-location and trunk surveillance which are described below. For a variety of reasons, we are skeptical as to whether CALEA's implementation cost can be determined with any degree of specificity. These reasons include wide variances in past budget estimates, the continued slow pace of CALEA implementation, and rapid technological changes in the telecommunications field. We agree, however, that it is unlikely that CALEA can be implemented with the \$49.5 million that remains unobligated from current funding.

⁸ The sources of these other funds were the DOJ working capital fund - \$40 million; U.S. Customs Service - \$1,580,270; and U.S. Postal Inspection Service - \$1 million.

Proprietary/Commercial Information Redacted

Emerging Technologies

The FBI is concerned that the emergence of new technologies without the development of concomitant CALEA standards will lessen law enforcement's ability to conduct authorized electronic surveillance. The new technologies include:

- Packet-mode (digitalized transmissions) communications that can be used via conventional telecommunications systems or the internet.
- Internet-based telecommunications services, which use packet-mode communication.
- Nontraditional wireless services, such as personal digital assistants.
- Internet hotspots, such as cyber cafes, that provide anonymity with multiple access points.
- Walkie-talkie networks, such as Verizon's push-to-talk.
- Third party calls using calling cards and toll free numbers.

In addition, the slow pace of CALEA's implementation increases the likelihood that additional technologies will continue to emerge that could impact law enforcement's ability to conduct authorized electronic surveillance.

Legislative Issues

DOJ is currently considering whether to propose to Congress changes to CALEA. Currently, CALEA does not apply to "information services," which include Internet Service Providers. However, vendors are now offering phone service over the internet. Some modification of the information services exemption may be necessary in order to ensure that Voice-over-Internet-Protocol services are subject to CALEA requests.

Other CALEA amendments DOJ is considering include: modifying the Attorney General's role with regard to electronic surveillance standard setting, limiting the FCC's authority to grant extensions to carriers for implementing CALEA, granting the FCC enforcement power to compel carriers to comply with CALEA, and amending the mechanism by which carriers may be reimbursed for deploying electronic surveillance standards.

Proprietary/Commercial Information Redacted

Although we discuss these legislative issues in greater detail in this report, it is not our intent to endorse any specific legislative change. The FBI, in consultation with DOJ and the administration, must fully evaluate each issue before recommending any legislative changes.

OIG Recommendations

In addition to assessing the status of CALEA implementation and assessing its cost effectiveness, our report contains three recommendations to the FBI to improve CALEA implementation:

- Collect and maintain data on the carrier equipment that is and is not CALEA compliant.
- Periodically survey state and local law enforcement to determine the extent to which delay in the implementation of CALEA is adversely impacting law enforcement's ability to conduct lawful electronic surveillance.
- Submit to Congress CALEA legislative changes necessary to ensure that lawful electronic surveillance is achieved expeditiously in the face of rapid technological change.

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	1
BACKGROUND	1
MAJOR PROVISIONS OF CALEA.....	2
FINDINGS AND RECOMMENDATIONS.....	6
DEPLOYMENT OF CALEA SOLUTIONS HAS BEEN SIGNIFICANTLY DELAYED	6
Causes for Delay in Deployment.....	7
FBI Efforts to Implement CALEA.....	11
Current Issues Affecting the Implementation of CALEA.....	17
Conclusion	23
Recommendations.....	24
APPENDIX I - CHRONOLOGY OF CALEA IMPLEMENTATION	
ACTIVITIES SINCE THE FY 1996 GAO REPORT	26
APPENDIX II - FCC ACTIONS ON PETITIONS.....	33
APPENDIX III - OBJECTIVES AND METHODOLOGY	34
APPENDIX IV – FBI RESPONSE	35
APPENDIX V - OIG, AUDIT DIVISION ANALYSIS AND SUMMARY	
OF ACTIONS NECESSARY TO CLOSE THE REPORT.....	37

INTRODUCTION

Background

Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in October 1994 and authorized \$500 million to reimburse telecommunications carriers (carriers) for certain eligible costs associated with implementing CALEA capability and capacity⁹ requirements to facilitate law enforcement's electronic surveillance.¹⁰ CALEA states

a . . . carrier shall ensure that its equipment, facilities and services that provide . . . a customer . . . the ability to originate, terminate, or direct communications are capable of expeditiously isolating and enabling the government, pursuant to court order . . . to intercept electronic communications . . .

In passing CALEA, Congress was concerned that advances in telecommunications technology, such as cellular telephones and features such as call forwarding and multiparty calls, could limit the effectiveness of lawful electronic surveillance. CALEA required that carriers deploy electronic surveillance standards to ensure that technological advances in the telecommunications industry (industry) would not compromise the ability of law enforcement agencies to engage in lawful electronic surveillance.

Congress assigned overall responsibility for implementing CALEA to the Attorney General, and the Attorney General delegated this responsibility to the FBI. To carry out these responsibilities, the FBI established a CALEA Implementation Unit (CIU) in its Investigative Technology Division and the Telecommunications Contract and Audit Unit (TCAU) in its Finance Division.

The CIU was responsible for development of CALEA-mandated requirements in concert with other federal, state, and local law enforcement agency and industry representatives. Once the requirements were developed, the CIU worked with these representatives to develop and deploy necessary methods and products to implement these requirements.

⁹ Capability refers to the ability to meet the electronic surveillance requirements provided in Section 103 of CALEA. Capacity refers to the ability to meet the simultaneous electronic surveillance intercepts provided in Section 104 of CALEA.

¹⁰ Electronic surveillance is the interception of communications and collection of call identifying information via carrier systems pursuant to lawful government authorization in the investigation of criminal activity.

Proprietary/Commercial Information Redacted

The TCAU was primarily responsible for awarding and administering all agreements involving the implementation of CALEA. The TCAU consisted of a contract group and a contract audit group. The contract group drafted and promulgated the cost recovery regulations, executed RTU agreements, and obligated and disbursed funds pursuant to the RTU agreements. The contract audit group assisted in the development of independent government cost estimates for the RTU agreements and provided audit support for the implementation of CALEA.

Major Provisions of CALEA

CALEA does not change or expand the government's electronic surveillance authority. Rather, CALEA seeks to ensure that carriers will have the necessary technical capability and sufficient capacity to assist law enforcement in conducting electronic surveillance pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986, which extended authorized lawful electronic surveillance to communications transmitted via wireless technology. The following are salient provisions in CALEA:

- Pursuant to CALEA, the Attorney General may reimburse the carriers for modifications to equipment, facilities, or services installed or deployed on or before January 1, 1995, to meet the capability requirements. If the Attorney General does not make such reimbursement, a given carrier is deemed in compliance with CALEA for such equipment unless the equipment has been replaced, significantly upgraded, or otherwise undergoes major modification. The carriers are responsible for such CALEA compliant modifications to equipment, facilities, and services installed or deployed after January 1, 1995.
- CALEA gives certain responsibilities and authority to the Federal Communications Commission (FCC) under sections 102, 105, 107, and 109. Under section 102, the FCC has the authority to identify telecommunications services, not specifically identified in the law, that are subject to the requirements of CALEA. Section 105 of CALEA states that the FCC shall prescribe regulations to ensure that carriers conduct electronic surveillance only pursuant to a court order or other lawful authorization with the affirmative intervention of a carrier employee.

Proprietary/Commercial Information Redacted

- CALEA provides for three kinds of FCC relief from the capability requirements of CALEA under sections 107 and 109: Deficiency petitions under section 107(b), compliance extensions under section 107(c) and reasonably achievable petitions under section 109(b). The FCC may grant relief under section 107(b) if industry electronic surveillance standards are deemed deficient or nonexistent. Also, the FCC may grant compliance extensions to carriers under section 107(c) if carrier compliance is deemed not to be reasonably achievable through the application of currently available technology. Finally, the FCC may grant relief under section 109(b) if carrier compliance with electronic surveillance standards is deemed too costly or technically complex or both with regard to equipment installed or deployed after January 1, 1995. Carriers may request reimbursement for these modifications provided that the FCC has ruled that such modifications are not otherwise reasonably achievable under section 109(b) of CALEA. According to FBI personnel, the FCC has not granted any relief to carriers under section 109(b) of CALEA.
- CALEA provided that telecommunications equipment manufacturers (manufacturers) cooperate with carriers in order to ensure that carriers were able to comply with CALEA on a timely basis. CALEA provided that manufacturers shall make available to carriers features and modifications, timely and at a reasonable charge, as necessary to allow the carriers to comply with CALEA requirements.
- When enacting CALEA, Congress recognized that standards for interception of electronic surveillance needed to be developed. Therefore, to develop such standards, CALEA provides for consultation among: DOJ; federal, state and local law enforcement agencies; industry standard-setting organizations; and state utility commissions.

Past DOJ OIG Reports

The Department of Justice (DOJ) Office of the Inspector General (OIG) is required by CALEA to report to Congress biannually on the equipment, facilities and services that have been modified to comply with CALEA capability and capacity requirements; whether FBI payments to carriers for such modifications were reasonable and cost effective; and projections of future costs for such modifications to meet CALEA capability requirements. We have issued three previous reports on CALEA:

Proprietary/Commercial Information Redacted

- In March 1998, we reported that the FBI and the industry disagreed over what capabilities had to be provided by the industry to be CALEA compliant and eligible for reimbursement (see OIG report number 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, we 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 capability requirements (see report number 00-10). The FBI determined that right-to-use (RTU) licenses for the use of the manufacturers' software would be a major cost for the carriers.¹¹ We also 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 software developed by Nortel. At the time, CALEA only permitted reimbursement of carrier costs. For this reason carriers were included as parties to these agreements. Under these agreements payments were made to Nortel on behalf of all carriers who used the Nortel equipment specified in the agreement. Pursuant to these agreements, the FBI negotiated a price of \$101.8 million for carrier purchase of Nortel's RTU software licenses.

According to the FBI, the manufacturers would not provide the FBI with adequate cost or pricing data. As a result, the FBI was unable to determine the reasonableness of the cost of the RTU software licenses through traditional means, such as cost and price analysis. Therefore, the FBI prepared a Determination and Findings Regarding the Implementation of the Communications Assistance for Law Enforcement Act (D&F) dated June 2, 1999, prior to entering into these agreements. The D&F set forth the FBI's rationale for entering into these agreements without adequate cost or pricing data. Nevertheless, the information given to us by the FBI at that time did not provide us with an adequate basis to determine the reasonableness of these costs. Accordingly, in the

¹¹ A RTU software license allows a carrier to activate the software once the manufacturer has been reimbursed for its development costs. However, having an RTU license does not guarantee that a carrier will activate the software.

Proprietary/Commercial Information Redacted

March 2000 report, we were unable to offer an opinion on the reasonableness of the cost incurred for the RTU software licenses.

We also reported in the March 2000 report that the FBI's Office of General Counsel had issued a legal opinion stating that the RTU license agreements were legal within the framework of CALEA. The legal opinion stated that such agreements were:

[A] reasonable attempt to minimize the costs to the federal government because it reduces the potential for manufacturers to collect substantial profit from carriers who will in turn seek reimbursement from the federal government.

- In March 2002, we 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 number 02-14). The FBI concluded that RTU license agreements were the most cost effective vehicles to reimburse the carriers for the use of the manufacturers' software. The FBI prepared D&Fs to support this approach because the manufacturers would not provide the FBI with adequate cost or pricing data. Thus, the information given to us by the FBI did not provide a basis to determine the reasonableness of the cost incurred for the RTU software licenses. Accordingly, we again were unable to offer an opinion on the reasonableness of these costs.

We 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 locations prioritized by the FBI. The FBI had identified carrier equipment locations with high electronic surveillance activity and determined these to be priority locations for the deployment on the electronic surveillance standards.

FINDINGS AND RECOMMENDATIONS

Deployment of CALEA Solutions Has Been Significantly Delayed

Implementation of CALEA solutions remains delayed after more than nine years since CALEA's enactment.¹² Despite payments and obligations of approximately \$450 million for manufacturers to assist carriers in implementing the requirements of CALEA, the FBI has not entered into any agreements with carriers to deploy electronic surveillance solutions at priority locations as defined in footnote 17. The main reasons for the delay in implementation are that carriers: (1) have stalled the implementation of CALEA by challenging or failing to develop electronic surveillance standards that address all law enforcement needs; (2) challenged the FBI's carrier cost recovery regulations; and (3) did not provide the FBI with reasonable deployment cost estimates. In addition, the first negotiation with a manufacturer to develop a software solution that will provide carriers with RTU licenses to use manufacturer-developed electronic surveillance features, began in 1998, and the FBI reports that only now are negotiations with manufacturers being completed.

In addition, the FCC has granted the carriers extensions for compliance with CALEA that have delayed implementation by nearly four years which has adversely impacted the FBI's ability to implement CALEA for the benefit of law enforcement. As a result, the FBI estimated that electronic surveillance standards have been deployed on only 10 to 20 percent of carrier wireline equipment, and 50 percent of pre-1995 and 90 percent of post-1995 wireless equipment. However, the FBI was unable to provide us with data showing the extent to which state and local law enforcement has been unable to conduct electronic surveillance as a result of these delays.

¹² A CALEA solution is the standards that carriers adopt to be able to comply with law enforcement requests to conduct lawful electronic surveillance.

Proprietary/Commercial Information Redacted

We discuss the causes of these delays in detail below. Also we discuss below the two major efforts undertaken by the FBI to implement CALEA: the RTU agreements, and the flexible deployment program. Finally, we discuss issues that CALEA implementation is still facing: emerging technologies, legal issues, and future funding needs.

Causes for Delay in Deployment

Electronic Surveillance Standard Setting and FCC Actions

In June 1996, DOJ issued the Electronic Surveillance Interface (ESI) Document. The ESI sets forth the law enforcement surveillance capabilities, which were developed in consultation with law enforcement and industry representatives. In December 1997, the industry published Interim Standard J-STD-025 (J-Standard) to meet the electronic surveillance capability requirements of CALEA. The J-Standard incorporated many of the standards set forth in the ESI but excluded several electronic surveillance capabilities deemed necessary to law enforcement. As a result, DOJ filed a deficiency petition with the FCC in March 1998 because the J-Standard did not meet an additional nine capabilities (punch-list) that law enforcement was seeking.¹³ The punchlist included the following capability requirements for carriers:

1. Provide the content of subject-initiated conference calls supported by the subject's service (including the call content of parties on hold).
2. Identify the active parties of a multiparty 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.

¹³ See Appendix II for a listing of FCC actions relating to petitions.

Proprietary/Commercial Information Redacted

6. Provide digits dialed by a 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 a law enforcement agency via electronic continuity check tone if the facility used for delivery of call content has failed or lost continuity.
9. Notify a law enforcement agency if the subject modifies his subscribed features.

In September 1998, the FCC granted an extension to carriers of CALEA deadline for complying with CALEA capability requirements. 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 on the basis that there was no technology currently available to permit carriers to deploy the minimum industry-developed J-Standard capability standards. In its order, the FCC noted that, pursuant to CALEA, carriers are deemed to be CALEA-compliant with respect to equipment installed or deployed on or before January 1, 1995, unless the Attorney General agrees to reimburse carriers for all reasonable costs necessary to bring such equipment into compliance.

In August 1999, the FCC ruled that carriers must comply with six of the additional punch-list requirements sought by the government and not included in J-Standard (items 1 through 6 on page 7). The FCC gave carriers until September 2001 to comply with these additional capability standards. The FCC also mandated that carriers provide the capability to intercept packet-mode communications by September 30, 2001.¹⁴ The industry appealed the FCC decision to the United States Court of Appeals, District of Columbia Circuit. On August 21, 2000, the Court of Appeals ruled that each capability standard is required by CALEA, but remanded four of the challenged capabilities (items 2, 3, 4 and 6) to the FCC for further proceedings (99-1442). In an April 11, 2002, Order on Remand, the FCC found that all of the punchlist requirements are required under CALEA and

¹⁴ Packet-mode is the digitalization of telecommunication transmissions so that a carrier can use its entire system to transmit a communication instead of dedicating a specific portion of the system for the transmission duration as with a conventional transmission. Packet-mode is more efficient and less costly because each digitized communication packet can travel the most direct system path.

Proprietary/Commercial Information Redacted

must be provided by wireline, cellular, and broadband telecommunications carriers by June 30, 2002.

Cost Recovery Regulations

In March 1997, the FBI published the final cost recovery regulations (28 CFR Part 100), which set forth the procedures for carriers to follow to receive reimbursement for costs incurred in deploying their CALEA solutions on their pre-1995 equipment. A CALEA solution is the methodologies that carriers adopt to be able to comply with law enforcement requests to conduct lawful electronic surveillance. Carriers will incur costs to deploy their CALEA solutions through activation of the software provided by manufacturers under the RTU agreements. The Cost Recovery Regulations became effective on April 21, 1997. Industry representatives filed a lawsuit in April 1998 in U.S. District Court of the District of Columbia (Court) challenging the definition of "installed or deployed" as the term applied to the January 1, 1995, cutoff for reimbursements to carriers. DOJ filed a motion to dismiss, and in August 2000 the Court ruled in favor of DOJ (98-2010).

On October 5, 2001, the FBI published a Supplemental Notice of Proposed Rulemaking, 66 Fed. Reg. 50931 (2001). The notice addressed the implementation of CALEA Section 109 regarding the definitions of "replaced" and "significantly upgraded or otherwise undergoes major modification." The FBI published on July 2, 2003, an information collection request 68 Fed. Reg. 39597 (2003) to the Office of Management and Budget for review and approval of the Cost Recovery Regulations in accordance with the Paperwork Reduction Act of 1995. The proposed information collection was published to obtain comments from the public and affected agencies. On October 16, 2003, the FBI published 68 Fed. Reg. 59638 (2003), a 30-day notice of information collection reply comment period regarding the Cost Recovery Regulations.

Carrier Cost Proposals

The FBI implemented an approach to reimbursement that allowed carriers to receive at no charge CALEA electronic surveillance software. The FBI determined that RTU licenses for the use of the manufacturers' software would be a major cost for the carriers and that nationwide software buyouts would be more cost effective than reimbursing individual carriers for the cost of this software (FBI purchase of RTU licenses for all carriers that use a given manufacturer's equipment). Under these RTU agreements, the

Proprietary/Commercial Information Redacted

manufacturers developed and made available to carriers the software with the necessary features for electronic surveillance that carriers require in order to deploy their CALEA solutions. 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.

In the past, carriers have submitted cost estimates to the FBI for deployment of CALEA solutions. Deployment involves activation by the carriers of the software solutions previously developed by manufacturers. The FBI has not yet entered into any agreements with carriers because FBI personnel believed that carrier cost estimates for activation were unreasonable. The only exception to this was an agreement with Qwest, dated February 28, 2002, to implement its electronic surveillance solution in the Salt Lake City area before the Winter Olympics held in February 2002.¹⁵

FBI personnel provided us with several carrier proposals for deployment of their electronic surveillance solutions as examples of what FBI personnel considered to be exorbitant cost estimates to deploy CALEA solutions. These included submissions by GTE, SBC, and Verizon. The three examples provided by the FBI contained cost estimates that together exceeded the total funds authorized by Congress for CALEA implementation. GTE submitted its proposal in February 1999 before the RTU agreements and before merging with Verizon. GTE estimated that the cost of deploying a CALEA solution throughout its entire network could exceed [Proprietary Information Redacted]. SBC and Verizon submitted cost estimates after the RTU agreements had been consummated and reflected the cost savings resulting from these agreements. The SBC cost proposal, submitted in September 2000, showed an estimate of [Proprietary Information Redacted] for deployment of a CALEA solution. The FBI provided us with two cost proposals submitted by Verizon. The first, submitted in June 2001, showed a cost estimate of [Proprietary Information Redacted] to deploy a CALEA solution throughout its network. The revised proposal submitted by Verizon in July 2002 showed the total cost estimate to be [Proprietary Information Redacted].

¹⁵ The agreement between the FBI and Qwest was in response to the September 11, 2001 (9/11) terrorist attacks. Qwest was reimbursed \$6.2 million under the agreement. Of this amount, \$4 million was paid from the FBI's counterterrorism fund that was established in response to the 9/11 terrorist attacks. The remaining funds - \$2.2 million - were from FBI funds.

Proprietary/Commercial Information Redacted

The FBI recently received a proposal from a major telecommunications carrier to deploy its electronic surveillance solution on specified carrier priority equipment. FBI personnel were optimistic that an agreement could be negotiated with this carrier, and that this will lead to the deployment of a CALEA solution throughout a significant portion of this carrier's network. The FBI is hopeful that if agreement is achieved with this carrier, the possibility of negotiating reasonably priced agreements with other carriers will be increased.

FBI Efforts to Implement CALEA

Results of Right-To-Use Software License Agreements

As previously reported in an OIG audit of CALEA, the FBI implemented an approach to reimbursement that allowed carriers to receive CALEA electronic surveillance software at no charge through RTU agreements (see OIG audit report numbers 00-10 and 02-14). Under RTU agreements, the manufacturers developed and made available the software with the necessary features for electronic surveillance in order for carriers to deploy their CALEA solutions. As of November 2003, the FBI had paid or obligated approximately \$450 million, primarily for the purchase of the RTU software licenses from various manufacturers. The following major manufacturers have participated in RTUs: Nortel, Lucent, Motorola, Siemens, and AG Communications. In addition, the first negotiation with a manufacturer to develop a software solution, which provides the carriers with RTU licenses to use manufacturer developed electronic surveillance features, began in 1998 and the FBI reports that only now are negotiations with manufacturers essentially complete.

The FBI initiated the first agreement with Nortel in 1998. In our previous reports, we stated that the FBI was unable to determine the reasonableness of these agreements because the manufacturers refused to provide adequate cost and pricing data. Nevertheless, the FBI determined that the costs were reasonable through a Determination and Finding (D&F). We were unable to offer an opinion on the reasonableness of these costs without the supporting data. In defense of this approach, the FBI's general counsel opined that: "the . . . [RTU licensing] arrangement is a reasonable attempt to minimize the costs to the federal government because it reduces the potential for manufacturers to collect substantial profit from carriers who will in turn seek reimbursement from the federal government."

Proprietary/Commercial Information Redacted

In this audit, to determine the result of the RTU agreements, we requested FBI personnel to provide us with data showing the extent to which CALEA compliant software was resident on carrier equipment. The FBI obtained the requested information from two sources. According to the data provided to us by the FBI, as reported in the industry's "Local Exchange Routing Guide" and by carriers under the FBI's Flexible Deployment Initiative described below, CALEA compliant software is now resident on carrier equipment switches as set forth in the two tables below, and that these results were because of the RTU agreements that the FBI had negotiated.¹⁶

RTU Software Resident on Carrier Wireline Equipment

	Wireline Equipment Switches					
	Pre-1995			Post-1995		
	Priority ¹⁷	Non-Priority ¹⁸	Total	Priority	Non-Priority	Total
Total number of Switches	5,232	6,510	11,742	1,270	1,665	2,935
Number with Resident Software	2,810	1,809	4,619	788	720	1,508
Percentage with Resident Software	54%	28%	39%	62%	43%	51%

Source: FBI

RTU Software Resident on Carrier Wireless Equipment

	Wireless Equipment Switches					
	Pre-1995			Post-1995		
	Priority	Non-Priority	Total	Priority	Non-Priority	Total
Total number of Switches	317	0	317	1,799	0	1,799
Number with Resident Software	270	0	270	1,530	0	1,530
Percentage with Resident Software	85%		85%	85%		85%

Source: FBI

¹⁶ A switch is a computer that directs electronic communication on a carrier system and controls the services and features available to customers.

¹⁷ Priority equipment is at locations with high historical intercept activity.

¹⁸ Non-priority equipment is at locations with low historical intercept activity.

Proprietary/Commercial Information Redacted

However, CALEA compliant software features must be activated by the carrier to effect compliance with CALEA requirements. The FBI did not have specific data from the carriers to determine the number of carrier equipment switches on which CALEA features have been activated, but the FBI has requested this information from the carriers. FBI personnel advised us that Verizon has recently agreed to begin providing such information to the FBI. FBI officials provided us with their best estimate of activated carrier switches based on ongoing interaction with industry representatives. They estimated that only 10 to 20 percent of the wireline resident software had been activated and approximately 50 and 90 percent of the pre- and post-1995 wireless resident software, respectively, had been activated. We were told by the FBI that law enforcement agencies may not be able to conduct electronic surveillance on equipment that lacks activated software. We requested that the FBI demonstrate the extent to which law enforcement agencies have been unable to conduct adequate electronic surveillance as a result. However, the FBI was unable to provide us with such information. In our judgment, collection and maintenance of this data is critical for the FBI to determine the degree to which CALEA has been implemented and the extent to which lawful electronic surveillance has been adversely impacted due to delay in carrier deployment.

In order to determine if lawful electronic surveillance had been adversely affected due to the lack of activation of CALEA compliant software, we reviewed reported nationwide domestic intercept activity from passage of CALEA to the present. In this review, we examined intercept activity trends at the federal, state, and local levels since CALEA was enacted. The following table shows the extent and cost of reported intercept activity for federal, state, and local law enforcement agencies. This data was taken from the "Report of the Director of the Administrative Office of the United States Courts (AOUSC) on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications" (Wiretap Report) dated April 2003.¹⁹ The Wiretap Report did not include counterterrorism investigation intercepts regulated by the Foreign Intelligence Surveillance Act of 1978. In addition, the Wiretap Report only showed so-called "full content" intercept activity, which does not include

¹⁹ This report is required under the Omnibus Crime Control and Safe Streets Act of 1968.

Proprietary/Commercial Information Redacted

“pen register” or “trap and trace” intercepts that only collect call-identifying data such as dialed phone numbers.²⁰

Post-CALEA Intercept Activity

Description	1995	1996	1997	1998	1999	2000	2001	2002
Intercepts Authorized	1,058	1,150	1,186	1,331	1,350	1,190	1,491	1,359
Intercepts Installed	1,024	1,035	1,094	1,245	1,277	1,139	1,405	1,273
Average Cost	\$56,454	\$61,436	\$61,176	\$57,669	\$57,511	\$54,829	\$48,198	\$54,586

Source: AOUSC Wiretap Report

As shown above, there has been a minimal but steady growth in the number of intercepts authorized and installed since 1995, with some drop off in 2000 and 2002. The Wiretap Report stated that more than 75 percent of 2002 electronic intercept locations were portable devices with no fixed location (e.g., cellular phones). As noted above, FBI officials believe that 50 to 90 percent of wireless equipment was CALEA compliant. Unfortunately, according to FBI personnel, law enforcement agencies are not required to report on electronic intercepts that are not conducted because costs are prohibitive or because the carrier equipment is not CALEA compliant. Therefore, we are unable to determine the full impact on law enforcement of the delay in implementing CALEA.

The FBI also entered into several additional RTU license agreements subsequent to the issuance of our March 2002 report. These agreements were made to reimburse the carriers for the purchase of RTU Enhanced Dial-Out software licenses from Siemens, Lucent, and Nortel (manufacturers) for \$19.8 million, \$19.6 million, and \$10.7 million, respectively. The FBI determined that RTU license agreements were the most cost effective vehicles to reimburse the carriers for the use of the manufacturers' software. The FBI prepared D&Fs to support this approach because it was unable to obtain adequate cost or price data. However, the information given to us by the FBI did not provide a basis to determine the reasonableness of the cost incurred for the RTU software licenses. Accordingly, we offer no opinion on the reasonableness of these costs.

²⁰ Full-content intercept activity includes call content as well as call-identifying information.

Proprietary/Commercial Information Redacted

In the Attorney General's Ninth Annual Report to Congress on CALEA (October 29, 2003), the FBI reported that these manufacturers were making available to carriers dial-out software.²¹ According to the report, dial-out is an efficient and effective way for law enforcement agencies to conduct authorized electronic surveillance because it uses existing telephone lines and does not require a time delay for carriers to establish additional lines and facilities. As a result, the cost to both carriers and law enforcement agencies should be significantly reduced according to the Report. The effects of these agreements are not reflected in the tables above, which show the extent to which RTU software is resident on carrier equipment.

Flexible Deployment

The FBI offered carriers three flexible deployment initiatives that the FBI said were designed to provide cost savings and operational flexibility to carriers to ensure that deployment of CALEA electronic surveillance solution would occur. The carriers have the option under CALEA to petition the FCC to permit deployment of their capability solutions after the FCC-mandated deadlines. The FBI stated that it would support such petitions before the FCC for those carriers who have approved flexible deployment plans. After the FBI and a carrier agreed on a CALEA deployment schedule, the FBI acknowledged the agreed-upon deployment timeline in a letter of support of the carrier's FCC petition.

The first flexible deployment initiative was offered in January 2000. Carriers were invited to voluntarily provide the FBI certain information regarding their telecommunications systems and a timeline for activating CALEA software provided under the RTU licensing agreements or otherwise deploy a CALEA solution. The flexible deployment initiative also provided carriers with the opportunity to petition the FCC for an extension of time from the June 30, 2000, compliance date established by the FCC. The major carriers petitioned the FCC and were granted an extension to June 2002, which the FBI supported.

The FBI offered a second flexible deployment initiative in August 2001, for carriers with packet-mode communications equipment switches. This initiative was similar in scope and intent to the first flexible deployment

²¹ CALEA requires the Attorney General to provide Congress with an annual report on the amounts paid to carriers, the projected amounts to be paid in the current fiscal year, and the equipment, facilities, or services for which the amounts were paid or are projected to be paid.

Proprietary/Commercial Information Redacted

initiative. However, the FBI discontinued this initiative because of the scarcity of technical standards for packet-mode systems.

The FBI initiated a third flexible deployment initiative to permit carriers to complete deployment of their electronic surveillance solutions within normal business cycles in order to minimize carrier costs. In the Attorney General's Ninth Annual Report to Congress on CALEA (October 29, 2003), the FBI stated that the FCC had provided extensions to the industry for compliance with CALEA capability requirements to June 2000, and again to June 2002. Pursuant to the third flexible deployment initiative, the major carriers submitted petitions to the FCC in response to the FCC Public Notice (Public Notice), dated September 28, 2001, to extend the June 30, 2002, FCC-mandated CALEA compliance date. On April 28, 2003, the FBI advised Verizon, BellSouth Telecommunications, and SBC that the FBI would not support their petitions to the FCC because of the refusal by these carriers to accommodate law enforcement's high priority electronic surveillance needs.

In this review, we requested from the FBI evidence of these carriers' refusals to accommodate law enforcement's high priority electronic surveillance needs. FBI personnel advised us that a group of federal, state, and local law enforcement officials called the Law Enforcement Technical Forum (LETf) meets regularly to discuss technical matters relating to the implementation of CALEA. FBI personnel stated that the minutes of meetings of the LETf contained comments from state and local law enforcement representatives indicating that law enforcement faced significant problems because carriers had not yet completed deployment of their electronic surveillance solutions. However, our review of these minutes revealed no significant references to such problems. We asked FBI personnel about this, and we were told that such comments had been made at the forum meetings but evidently had not been recorded to the official minutes.

At the time of our audit, FBI representatives stated that the FCC had not ruled on the carriers' petitions. However, on page 6 of an FCC Public Notice dated September 28, 2001, the FCC stated: "Upon the filing with the Commission of a petition or supplement in accordance with the requirements set forth in this *Public Notice*, the carrier will be deemed to have received a preliminary extension for the period requested in its filing, but not to exceed the two-year limit provided by Section 107(c)(3)(B) . . . ". Therefore, this suggests that the FCC endorsed the major carriers' petitions to extend the June 30, 2002, compliance date. The FBI stated that FCC's granting of repeated extensions to carriers of CALEA compliance date is adversely

Proprietary/Commercial Information Redacted

affecting law enforcement's ability to carry out authorized electronic surveillance. Yet, CALEA provides that the FCC should consider the extensions in consultation with the Attorney General. Until recently, as noted above, the FBI did not object to the extensions.

Current Issues Affecting the Implementation of CALEA

Current issues affecting the implementation of CALEA include future funding needs, emerging technologies for which electronic surveillance standards are inadequate or not yet developed, and legislative changes to facilitate CALEA implementation.

Future Funding Needs

Approximately \$50 million in unobligated CALEA funds remain for implementation of carrier technical solutions and other FBI funding priorities as described below. Following is the total CALEA funding received and paid, and the remaining obligated and unobligated funds.

Appropriations	\$456,976,876
Funds from other sources ²²	42,580,270
Total Received [a]	<u>\$499,557,146</u>
Less:	
Payments [b]	\$441,367,124
Obligations [c]	<u>\$ 8,664,775</u>
Unobligated Funds: [a] less [b + c]	<u>\$ 49,525,247</u>

According to Congress' July 1995 Office of Technology Assessment report, entitled "Electronic Surveillance in a Digital Age," the costs of CALEA legislation and who should bear those costs were highly controversial issues. The \$500 million authorized for CALEA implementation was a compromise among widely ranging cost estimates from industry and law enforcement. Both industry's and law enforcement's cost estimates for modifying carrier equipment and deploying electronic surveillance technology were based on assumptions that were generally not backed by formal engineering cost analysis.

²² The sources of these funds were the DOJ working capital fund - \$40 million; U.S. Customs Service - \$1,580,270; and U.S. Postal Inspection Service - \$1 million.

Proprietary/Commercial Information Redacted

Cost estimates for obtaining CALEA compliance have varied widely. Prior to the enactment of CALEA, industry estimated that CALEA compliance would cost from \$3 to \$5 billion, while the FBI Director estimated the cost to be between \$500 million and \$1 billion. In 1998 and 1999, industry estimates totaled \$1.3 billion. Manufacturers initially requested \$734 million for the RTU software licenses, and negotiations between the FBI and industry representatives reduced the final price to about \$447 million. In December 2003, the FBI estimated that an additional \$204 million would be necessary to complete deployment of CALEA solutions on carrier equipment in high priority areas and to conduct other essential activities described below.

Regarding deployment of the carriers' capability and capacity technical solutions, the FBI's Office of General Counsel issued a legal opinion, dated September 1, 2000, which stated in part:

[E]ntering into these [RTU software license] agreements does not guarantee that CALEA-compliant solutions will be operable and available for use by law enforcement. These agreements only ensure that right-to-use licenses for CALEA software will be made available to carriers at no additional charge . . . Additional monies will need to be authorized and appropriated by Congress to deploy the solutions fully. Although how much it will cost to install or deploy the solutions by carriers remains uncertain . . .

The FBI estimated that approximately \$254 million will be needed to develop geo-location and trunk surveillance, implement capability requirements on the highest priority switches, and obtain one additional RTU dial-out agreement. The funds will also be used for potential CALEA section 109(b) petitions, the Nextel upstream solution, and other exigent circumstances.²³ However, the FBI can use approximately \$50 million of unobligated funds, resulting in about \$204 million in new funds needed, according to its estimates.

For a variety of reasons, we are skeptical as to whether CALEA's implementation cost can be determined with any degree of specificity.

²³ Wireless geo-location is a CALEA feature enhancement that would provide law enforcement personnel with subject geographic locator information that is maintained by telecommunications equipment. Trunk surveillance would assist law enforcement personnel in surveillance of calls initiated through network-based features such as 800 numbers, calling cards, and voice mail.

Proprietary/Commercial Information Redacted

These reasons include wide variances in past budget estimates, the continued slow pace of CALEA implementation, and rapid technological changes in the telecommunications field. We agree, however, that it is highly unlikely that CALEA can be implemented with the \$49.5 million that remains unobligated from current funding.

The FBI had not estimated the costs to meet CALEA capacity requirements. Capacity refers to the ability of a carrier to conduct more than one intercept simultaneously. In this regard, according to the FBI report entitled, Status of Reimbursement for Capability and Capacity:

The precise delineation of the modifications needed and the costs, which must be incurred to attain capacity for simultaneous intercepts, has not been established because the variety of technical solutions inhibits a single interpretation.

The FBI hopes that evolving technologies will significantly reduce capacity costs. For example, the dial-out technology described above should permit the reduction of carrier capacity costs because electronic surveillance will be conducted over existing phone lines rather than carriers having to charge law enforcement for additional dedicated lines for such purposes.

Emerging Telecommunications Technologies

New technologies will continue to evolve that will require development of additional electronic surveillance standards. Some of these technologies are:

- Internet-based telecommunication services and packet-mode communication, which can be used via the internet or conventional telecommunication systems;
- Nontraditional wireless services, such as personal digital assistants (PDA);
- Internet hotspots, such as internet cafes that provide wi-fi or hard wired access points to one service;
- Walkie-talkie networks, such as Verizon's push-to-talk;²⁴ and

²⁴ FBI personnel advised us that Motorola developed a CALEA solution that Nextel uses for its walkie-talkie network.

Proprietary/Commercial Information Redacted

- Third party calls using calling cards and toll free numbers for access.

At the time CALEA legislation was introduced, the FBI Director characterized the proposed legislation as necessary "to maintain technological capabilities commensurate with the existing statutory authority, that is, to prevent advanced telecommunications technology from repealing *de facto* . . . authority already conferred by Congress."

The FBI is working with various industry standard-setting bodies to develop electronic surveillance standards for new technologies. However, carriers may be reluctant to adopt such standards because of the cost or technological complexity. Therefore, we believe that the legal changes addressed below will, if recommended by DOJ and adopted by Congress, also assist the FBI in meeting the challenges of rapid technological change in the telecommunications field.

Legislative Issues

In addition to future funding needs and emerging telecommunications technologies, there are also a number of legislative issues to consider in fully implementing CALEA. Although we discuss the legislative issues in this section, it is not our intent to endorse any specific legislative change. The FBI, in consultation with DOJ and the administration, must fully evaluate each issue before recommending any legislative changes.

Information Services Exemption

Currently, CALEA does not apply to "information services". However, vendors are currently offering phone service over the internet. Some modification of the information services exemption may be necessary in order to ensure that Voice-over-Internet-Protocol (VoIP) services are subject to law enforcement requests for lawful electronic surveillance.

The FBI provided one example of the controversy surrounding VoIP carriers. In 2003, the Minnesota Public Utility Commission (MPUC) ruled that Vonage Holdings, Inc. (Vonage), a VoIP carrier, was a telephone service provider under Minnesota state law. As a result, Vonage was subject to certain state regulations, such as those governing 911 emergency calling services. Vonage petitioned both the Minnesota District Court for injunctive

Proprietary/Commercial Information Redacted

relief and the FCC for preemption of all state regulation on the grounds that Vonage is an information service provider.

The Minnesota District Court ruled in favor of Vonage. The Minnesota Attorney General filed a petition on behalf of the MPUC, which was pending at the time of our review. The FCC sought comment on Vonage's petition and the FBI filed comments stating that Vonage did not qualify for relief because its VoIP service is a telecommunications service, not an information service.

FBI personnel stated that the regulatory counsel for Vonage advised the FBI that CALEA definition of "telecommunications carrier" is flexible enough to permit the imposition of CALEA responsibilities on vendors that are not telecommunications carriers under Title II of the Communications Act of 1934.

The FCC issued a notice of proposed rule making, dated February 14, 2002, that would classify wireline broadband internet access and cable modem internet access services as information services. The DOJ filed comments opposing such classifications that it believes will thwart the purpose of CALEA. The FCC had yet to rule on these issues at the time of our review.

Potentially, VoIP services could be a dominant method of telephonic communication in a few years. As the technology evolves, people will be able to make phone calls over the internet using their PDAs. Carriers may be forced to offer such services quickly because their costs should be significantly reduced through the use of packet-mode technology versus conventional communications technology.

Technical Standards Setting

CALEA provides that the Attorney General consult with organizations setting industry standards and others to ensure the efficient and industry-wide implementation of CALEA capability requirements. Modifying the Attorney General's role with regard to electronic surveillance standard setting could make CALEA standard setting more accountable, efficient, and controllable and alleviate the current litigious atmosphere.

Proprietary/Commercial Information Redacted

Cost Recovery

Currently, CALEA states that the Attorney General may reimburse the carriers for modifications to equipment, facilities, or services installed or deployed on or before January 1, 1995, to meet the capability requirements. If the Attorney General does not make such reimbursement, the carriers are deemed in compliance with CALEA for such equipment. The carriers are responsible for such modifications to equipment, facilities, and services installed or deployed after January 1, 1995. However, the carriers may request reimbursement for these modifications provided that the FCC has ruled that such modifications are not otherwise reasonably achievable because of being too costly, technically complex, or both. Amending the mechanism by which carriers are reimbursed for deploying electronic surveillance standards may also alleviate the non-cooperative atmosphere.

Extension Authority

As noted above, Section 107 of CALEA provides authority to the FCC, after consultation with the FBI, to grant extensions of time to carriers to comply with CALEA capability standards with respect to their post-1995 equipment, facilities, and services. An extension may be granted for a maximum of two years if the FCC determines that compliance with CALEA capability requirements is not reasonably achievable using current technology or technology is deficient or nonexistent. The FCC has granted several extensions of time to carriers in the past that we reported on previously. However, CALEA is silent on the number of extensions the FCC may grant carriers under section 107.

Enforcement

Section 108 provides for court issuance of enforcement orders under section 2522 of title 18, United States Code. Enforcement orders may be issued by a court (1) that approved an electronic surveillance order with which a carrier failed to comply, or (2) upon application by the Attorney General in a civil action to obtain an order to direct a carrier, manufacturer, or provider of telecommunications support services to comply with CALEA. 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. A court issuing such an enforcement order must allow a reasonable time period for compliance and may impose a

Proprietary/Commercial Information Redacted

civil penalty not to exceed \$10,000 per day for each day of violation of such enforcement order

However, CALEA imposes strict limitations on enforcement orders having to do with capacity, reasonable achievability, and modifications to pre-January 1, 1995, equipment. First, a carrier may not be compelled to comply with court ordered electronic surveillance if the carrier lacks sufficient capacity and the government has not agreed to pay for such capacity. Second, a carrier may not be forced to modify post-January 1, 1995, equipment if the FCC has ruled under section 109(b) of CALEA that such modifications will be too costly or technically complex. Finally, a carrier may not be compelled to modify pre-January 1, 1995, equipment unless the government agrees to pay for such modifications provided that such equipment has not been replaced or significantly upgraded.

In our judgment, CALEA does not give additional powers to the FCC. However, FBI personnel advised us that the Communication Act of 1934 provides the FCC with enforcement powers sufficient to compel carriers to comply with CALEA requirements but, for whatever reason, the FCC has not used such powers. According to FBI personnel, the FCC has very strong enforcement powers over carriers in other areas such as local number portability and enhanced 911.

DOJ petitioned the FCC in March 2004, to attempt to resolve some outstanding issues with regard to some of the legal considerations and technology changes impacting CALEA implementation identified above. These included but were not limited to: identification of services considered to be packet-mode, establishment of a timeline and criteria for carrier compliance with packet-mode standards and standards covering future technology, a ruling that would assist in identification of future services and entities that are subject to CALEA, establishment of procedures for enforcement action against carriers that do not comply with CALEA, and permission for carriers to recover CALEA implementation costs from their customers. If the FCC does what is requested in the DOJ petition, we believe that it would facilitate the implementation of CALEA.

Conclusion

More than nine years since enactment, CALEA has not been fully implemented. Among the causes for this delay are deficient and contested electronic surveillance standards, contested cost recovery regulations,

Proprietary/Commercial Information Redacted

lengthy negotiations with industry representatives regarding the price for the RTU licenses, and carrier cost proposals deemed unreasonable by the FBI. The FBI has made available to carriers electronic surveillance software developed by manufacturers, but the FBI does not know the extent to which carriers have implemented the electronic surveillance solutions utilizing this software. However, FBI personnel estimate that only 10 to 20 percent of the wireline equipment switches are CALEA compliant. Additionally, FBI personnel estimate that only one-half of the pre-January 1, 1995, carrier wireless switches are CALEA compliant.

Our review of nationwide electronic surveillance intercepts indicates that intercept activity at the federal, state, and local level appears to be increasing. But no statistics are kept on intercepts that were not conducted because they were deemed too costly or because carrier equipment was not compliant with CALEA requirements. The FBI was unable to state what effect the delay in CALEA implementation has had on law enforcement's ability to conduct electronic surveillance.

The FBI is concerned that the continual and rapid change in telecommunications technology without concomitant electronic surveillance solutions will adversely impact the ability of law enforcement to conduct electronic surveillance. There are a number of legislative issues that the FBI and DOJ need to evaluate that may assist the FBI in implementing CALEA in the face of rapid technological change.

The FBI has paid or obligated about \$50 million during the current reporting period for carrier purchases of the RTU enhanced dial-out software licenses. The FBI determined that RTU license agreements were the most cost effective vehicles to reimburse the carriers for the use of the manufacturers' software. The FBI prepared D&Fs to support this approach because it was unable to obtain adequate cost or price data. However, the information given to us by the FBI did not provide a basis to determine the reasonableness of the cost incurred for the RTU software licenses. Accordingly, we offer no opinion on the reasonableness of these costs.

Recommendations

We recommend that the FBI:

1. Collect and maintain data on the number of carrier switches that are and are not CALEA compliant.

Proprietary/Commercial Information Redacted

2. Periodically survey state and local law enforcement to determine the extent to which delay in the implementation of CALEA is adversely impacting law enforcement's ability to conduct lawful electronic surveillance.
3. Submit to Congress CALEA legislative changes necessary to ensure that lawful electronic surveillance is achieved expeditiously in the face of rapid technological change.

APPENDIX I

**CHRONOLOGY OF CALEA IMPLEMENTATION ACTIVITIES
SINCE THE FY 1996 GAO REPORT**

June 1996 - Capability Requirements Issued

Law enforcement surveillance capabilities were developed in consultation with other law enforcement agency and industry representatives. These capabilities were issued in a document entitled, Electronic Surveillance Interface (ESI) Document on June 24, 1996.²⁵

October 1996 - Telecommunications Carrier Compliance Fund Established

The Congress established the Telecommunications Carrier Compliance Trust Fund (TCCF) and authorized agencies with law enforcement responsibilities to deposit unobligated balances into the TCCF to assist in the funding of CALEA implementation efforts, subject to Congressional reprogramming requirements.

The Congress appropriated \$60 million as start-up funds to begin CALEA implementation and deposited these funds in the TCCF. The Attorney General also transferred \$40 million of DOJ working capital funds to the TCCF. Additionally, the U.S. Postal and Customs Services made contributions to the TCCF of \$1 million and \$1.6 million, respectively, for a total of \$102.6 million available for CALEA implementation.

March 1997 - Implementation Plan Submitted

The FBI submitted an implementation plan to Congress on March 3, 1997. The implementation plan included: (1) law enforcement requirements for electronic surveillance, (2) a prioritized list of carrier equipment to be modified to meet law enforcement requirements for electronic surveillance; (3) capacity requirements; and (4) a projected reimbursement plan. The FBI estimated that carrier reimbursements would amount to \$100 million a year for 5 years beginning in FY 1997.

March 1997 - Final Cost Recovery Regulations Published

The FBI published final cost recovery regulations (28 CFR Part 100) setting forth the procedures for carriers to follow in order to receive reimbursement under CALEA. The cost recovery regulations state the:

²⁵ 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 punch-list capabilities.

Proprietary/Commercial Information Redacted

(1) criteria for determining allowable and unallowable costs, (2) requirements carriers must meet in their submission of cost estimates and requests for payments for the disbursements of funds, and (3) audit requirements for CALEA implementation effort. The FBI also developed requisite audit programs and procedures to audit carrier proposals and agreements.

July 1997 - FCC Petition Filed

The Cellular Telecommunications Industry Association (CTIA) filed a petition with the FCC to establish electronic surveillance technical standards to implement Section 103 of CALEA because: “. . . the standards process is deadlocked, due . . . to unreasonable demands by law enforcement for more surveillance features than either CALEA or the wiretap laws allow.” In its petition the CTIA characterized the ESI as a de facto standard even though CALEA expressly prohibits law enforcement from requiring any specific design of systems or features or the adoption of any particular technology to meet CALEA. The FCC did not rule on the CTIA petition.

January 1998 - Implementation Report Submitted

The FBI reported to Congress on January 26, 1998, in response to a Conference Committee Report (H. Rpt. 105-405) that directed the DOJ to submit to the Committees on Appropriations a report that included: (1) cost estimates for development and deployment of the proposed CALEA solution, (2) a timeline for development and deployment of the solution, and (3) two signed cooperative agreements with appropriate carriers.

According to the implementation report, manufacturers reviewed the punch-list requirements and none stated that these requirements were impossible to meet. However, several of the manufacturers stated that some of the requirements would be extremely difficult to meet. The implementation report included no cost estimates for development and deployment of a CALEA solution. Only one manufacturer permitted the FBI to disclose pricing data in the implementation report.

The implementation report provided a timeline that showed manufacturers' best estimates for deployment of solutions to permit carriers to satisfy law enforcement requirements to intercept electronic communications. Only one manufacturer expected to have a CALEA compliant solution by the October 25, 1998, deadline. Based on manufacturer timelines disclosed in the implementation report, the FBI expected that the carriers would not be able to meet the October 25, 1998,

Proprietary/Commercial Information Redacted

deadline. According to the implementation report, the FBI had not entered into any cooperative agreements with carriers at that time.

February 1998 - DOJ Position on the Capability Requirements Established

The DOJ advised that 9 of the 11 punch-list capabilities contained in the ESI were clearly within the scope of CALEA. The DOJ was willing to compromise on one punch-list capability and acknowledged that one other punch-list capability, although it would enhance the effectiveness of electronic surveillance, was not required by CALEA. The DOJ stated that the carriers' interim standard was deficient in that it failed to address the nine punch-list capabilities within the scope of CALEA.

The carrier associations responded and disagreed that CALEA required carriers to provide the punch-list capabilities. The carrier associations urged the DOJ to accept the industry developed interim standard capability standards.

March 1998 - Final Notice of Capacity Requirements Published

The FBI published in the Federal Register the Final Notice of Capacity Requirements, which superceded notices published on October 16, 1995 and January 14, 1997. The carriers had 180 days to provide the FBI with a statement of equipment that does not meet the capacity requirements. The FBI would consider reimbursing carriers for modifications to equipment to meet the capacity requirements.

March 1998 – FBI Petitioned the Federal Communications Commission

On March 27, 1998, the FBI filed with the FCC a petition entitled Joint Petition for Expedited Rulemaking Regarding Technical Requirements and Standards, to compel carriers to adopt the government's CALEA capability requirements. This initiated a series of telecommunication industry and government FCC filings to assist the FCC in its decision-making.

September 1998 – FCC Issued Memorandum Opinion and Order

On September 11, 1998, the FCC granted an extension of the deadline (October 28, 1998) for complying with CALEA capability requirements and ruled that carriers must be compliant with the industry assistance capabilities by June 30, 2000.

December 1998 – Attorney General's Fourth Annual Report to Congress

On December 10, 1998, the Attorney General issued the fourth annual report to Congress on the implementation of CALEA.

Proprietary/Commercial Information Redacted

August 1999 – FCC Issued Second Report and Order

On August 31, 1999, the FCC concluded that the language and legislative history of CALEA provide sufficient guidance as to what the term “telecommunications carrier” means. The FCC also issued guidance for carriers seeking relief under CALEA reasonably achievable standard from CALEA assistance capability requirements for equipment, facilities, or service deployed after January 1, 1995.

August 1999 – FCC Issued Third Report and Order

On August 31, 1999 the FCC ruled that by September 30, 2001, carriers had to be compliant with six additional assistance capabilities sought by the government but not included in the industry assistance capabilities.

September 1999 – FBI Entered into Agreement with Nortel and Ameritech

On September 10, 1999, the FBI, Ameritech, and Nortel entered into an agreement through which the FBI agreed to reimburse Ameritech for its purchase of CALEA software RTU license from Nortel for its wireline systems. This agreement further stipulated that the FBI would commit \$101.8 million for CALEA software RTU license for all carriers in the United States that used Nortel’s equipment installed on or before January 1, 1995.

December 1999 – FBI Entered into Agreement with Nortel and AirTouch

On December 29, 1999, the FBI, Nortel, and AirTouch entered into an agreement through which the FBI agreed to reimburse AirTouch, and all other carriers in the United States, for its purchase of CALEA software RTU license from Nortel for its wireless system installed on or before January 1, 1995. The funds would come from the \$101.8 million that was committed pursuant to the FBI’s agreement with Nortel and Ameritech.

January 2000 – The Attorney General’s Fifth Annual Report

On January 3, 2000, the Attorney General issued to the Congress the fifth annual report on the implementation of CALEA.

January 2000 – The Flexible Deployment Guide was published

The FBI published the Flexible Deployment Guide in January 2000. The Guide requested carriers to submit certain information to the FBI and explained under what circumstances the FBI might support a carrier’s request to the FCC for an extension of the FCC-mandated deadlines.

Proprietary/Commercial Information Redacted

March 2000 – The FBI Agreement with Lucent and Bell Atlantic

On March 31, 2000, the FBI entered into an agreement with Lucent and Bell Atlantic to reimburse Bell Atlantic and certain other carriers \$170 million for their purchase of the RTU software licenses from Lucent.

June 2000 – The FBI Agreement with AG Communication Systems and GTE Communications Systems

On June 30, 2000, the FBI entered into an agreement with AG Communications Systems and GTE Communications Systems to reimburse GTE Communications Systems \$25 million for its purchase of the RTU software license for the GTE telephone operating companies from AG Communications Systems.

September 2000 – The FBI Agreement with Nortel, Motorola, and Nextel

On September 29, 2000, the FBI entered into an agreement with Nortel, Motorola, and Nextel to reimburse Nextel and certain other carriers \$17.9 million for their purchase of the RTU software licenses from Nortel.

October 2000 – The FBI Agreement with Siemens and Loretto

On October 2, 2000, the FBI entered into an agreement with Siemens and Loretto Telephone Company to reimburse Loretto \$20 million for its purchase of the RTU software license from Siemens.

January 2001 – The Attorney General's Sixth Annual Report

On January 9, 2001, the Attorney General issued to the Congress the sixth annual report on the implementation of CALEA.

March 2001 – The FBI Agreement with Motorola and Nextel

On March 28, 2001, the FBI, Motorola, and Nextel entered into an agreement through which the FBI agreed to reimburse Nextel and certain other carriers \$25 million for their purchase of the RTU software licenses from Motorola.

March 2001 – The FBI Agreement with Motorola

On March 29, 2001, the FBI entered into a National Availability Commitment with Motorola to reimburse carriers who use certain Motorola equipment switches \$30 million for their purchase of the RTU software licenses from Motorola.

Proprietary/Commercial Information Redacted

August 2001 – The Flexible Deployment Assistance Guide Second Edition for Packet-Mode Communications was published (Second Guide)

The Guide requested carriers to submit certain information to the FBI and explained under what circumstances the FBI might support a carrier's request to the FCC for an extension of the FCC-mandated deadlines.

September 2001 – The FBI Agreement with Siemens and Farmers

On September 25, 2001, the FBI entered into an agreement with Siemens and Farmers Telephone Company (Farmers) to reimburse Farmers and certain other carriers \$20 million for their purchase of the RTU software licenses from Siemens.

December 2001 – The Attorney General's Seventh Annual Report

On December 13, 2001, the Attorney General issued to the Congress the seventh annual report on the implementation of CALEA.

February 2002 – The FBI Agreement with Qwest

On February 28, 2002, the FBI entered into an agreement with Qwest to reimburse Qwest for its costs for deployment of its CALEA solution in the Salt Lake City area for the 2002 Winter Olympics.

May 2002 – The 3rd Flexible Deployment Guide was published

The FBI published the 3rd Flexible Deployment Guide in May 2002. The Guide requested carriers to submit certain information to the FBI and explained under what circumstances the FBI might support a carrier's request to the FCC for an extension of the FCC-mandated deadlines.

September 2002 – The FBI Agreement with Nortel and Qwest

On September 25, 2002, the FBI entered into an agreement with Nortel and Qwest to reimburse Qwest and certain other carriers \$4.2 million for their purchase of the RTU Enhanced Dial-Out software licenses from Nortel.

September 2002 – The FBI Agreement with Lucent and TDS

On September 30, 2002, the FBI entered into an agreement with Lucent and TDS to reimburse TDS \$19.4 million for its purchase of the RTU Enhanced Dial-Out software license from Lucent.

November 2002 – The FBI Agreement with Siemens and TDS

On November 15, 2002, the FBI entered into an agreement with Siemens and TDS to reimburse TDS \$15 million for its purchase of the RTU Enhanced Dial-Out software licenses from Siemens.

Proprietary/Commercial Information Redacted

April 2003 – The FBI Agreement with Nortel and Qwest

On April 4, 2003, the FBI entered into an agreement with Nortel and Qwest to reimburse Qwest \$6 million for its purchase of the RTU Enhanced Dial-Out software license from Nortel.

April 2003 – The FBI Agreement with Siemens and Loretto

On April 24, 2003, the FBI entered into an agreement with Siemens and Loretto Telephone Company to reimburse Loretto \$4.8 million for its purchase of the RTU Enhanced Dial-Out software license from Siemens.

May 2003 – The Attorney General's Eighth Annual Report

On May 16, 2003, the Attorney General issued to the Congress the eighth annual report on the implementation of CALEA.

October 2003 – The Attorney General's Ninth Annual Report

On October 29, 2003, the Attorney General issued to the Congress the ninth annual report on the implementation of CALEA.

APPENDIX II

FCC ACTIONS ON PETITIONS

- The DOJ filed a deficiency petition with the FCC in March 1998 because the J-Standard did not meet the additional nine punch-list capabilities that law enforcement was seeking. In September 1998, the FCC granted an extension to carriers of CALEA deadline for complying with CALEA capability requirements. For equipment installed or deployed after January 1, 1995, the FCC extended the deadline from October 28, 1998, to June 30, 2000.
- In August 1999, the FCC ruled that carriers must comply with six of the additional punch-list requirements sought by the government and not included in J-Standard. The FCC gave carriers until September 2001 to comply with these additional capability standards. The FCC also mandated that carriers provide the capability to intercept packet-mode communications by September 30, 2001.
- The major carriers petitioned the FCC for an extension of complying with CALEA and were granted an extension to June 2002, which the FBI supported pursuant to the FBI's approval of their flexible deployment plans.
- The major carriers submitted petitions to the FCC in response to the FCC Public Notice dated September 28, 2001 to extend the June 30, 2002, FCC-mandated CALEA compliance date. On April 28, 2003, the FBI advised Verizon, BellSouth Telecommunications, and SBC that the FBI would not support their petitions to the FCC because of the refusal by these carriers to accommodate law enforcement's high priority electronic surveillance needs. At the time of our audit, FBI representatives stated that the FCC had not ruled on these petitions.
- The FCC issued a notice of proposed rule making, dated February 14, 2002 that would classify wireline broadband internet access and cable modem internet access services as information services. The DOJ filed comments opposing such classifications that it believes will thwart the purpose of CALEA. The FCC had yet to rule on these issues at the time of our review.

APPENDIX III

OBJECTIVES AND METHODOLOGY

CALEA required the Comptroller General to report to Congress on the implementation of CALEA biannually beginning April 1, 1996. CALEA was subsequently amended to give the DOJ OIG this reporting responsibility.

We performed the audit in accordance with the Government Auditing Standards issued by the Comptroller General of the United States. Our audit covered CALEA enactment through December 2003. The DOJ OIG is required by CALEA, as amended, to report to Congress biannually on the equipment, facilities, and services that have been modified to comply with CALEA capability and capacity requirements; whether FBI payments to carriers for such modifications were reasonable and cost effective; and projections of future costs for such modifications to meet CALEA capability requirements. In this regard, carriers had made no modifications and the FBI had made no payments to carriers for modifications with the exception of an agreement with Qwest to deploy its CALEA solution in the Salt Lake City area for the Winter Olympics.

Our procedures were designed to determine the status of CALEA implementation activities. We reviewed the FBI progress of implementing CALEA since our last report. We also undertook a review of CALEA implementation since the enactment of CALEA to ascertain the major impediments to the full implementation of CALEA.

APPENDIX IV

FEDERAL BUREAU OF INVESTIGATION RESPONSE



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 26, 2004

Mr. Domenic A. Zazzaro
Regional Audit Manager
Washington Regional Audit Office
Office of the Inspector General
United States Department of Justice
Suite 3400
1300 North 17th Street
Arlington, Virginia 22209

Dear Mr. Zazzaro:

Reference is made to your memorandum dated March 18, 2004, concerning the FBI's response to recommendations set forth in the Department of Justice (DOJ), Office of the Inspector General (OIG) audit report entitled, "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation." This memorandum requested the FBI provide a written response to the recommendations set forth in the subject audit report and conduct a classification and sensitivity review. Specifically, you requested that the FBI response provide information concerning specific actions completed or alternative corrective actions proposed on the recommendations.

Attached is the FBI's written response and the result of the sensitivity and classification review. Please note that the format of the enclosed document identifies the DOJ OIG draft audit report recommendation followed by the response of FBI executive management.

The recommendation responses set forth in the attached were coordinated through the FBI's Inspection Division. Please contact Chris Boehringer of the Inspection Division should you have any questions. Mr. Boehringer can be reached at (202) 324-6801.

Sincerely yours,

A handwritten signature in black ink, appearing to read "J.C. McCraw".

Steven C. McCraw
Assistant Director
Inspection Division

FBI RESPONSE TO OIG RECOMMENDATIONS

OIG Recommendation #1: Collect and maintain data on the carrier equipment that is and is not CALEA compliant.

FBI Response: As a condition of reimbursement contracts with carriers for their deployment of technical solutions, the FBI requires periodic updates of progress. This information will allow the FBI to better recognize the level of compliant carrier equipment. Additionally, the FBI has already requested, as part of its Petition for Expedited Rulemaking, very specific benchmarks and deadlines to be adopted by the FCC. Information collected as a result of the FBI's recommended "phase-in plan" will allow it to know with great specificity the level of industry's compliance.

OIG Recommendation #2: Periodically survey state and local law enforcement to determine the extent to which delay in the implementation of CALEA is adversely impacting law enforcement's ability to conduct lawful electronic surveillance.

FBI Response: The FBI conducts an annual "Threat Assessment Survey" of law enforcement agencies throughout the country to gauge the impact that new and emerging technologies are having on law enforcement's ability to conduct lawful electronic surveillance. The FBI will augment its survey to include the recommendation of the Audit Report and assess the extent to which delay in the implementation of CALEA is impacting electronic surveillance.

OIG Recommendation #3: Submit to Congress CALEA legislative changes necessary to ensure that lawful electronic surveillance is achieved expeditiously in the face of rapid technological change.

FBI Response: The FBI is currently preparing a legislative recommendation. After completing internal review and approval, the FBI will gain consensus with DOJ and the Administration. The FBI will further brief the appropriate members of Congress to highlight the need for legislative remedy. The FBI estimates it can accomplish this action in the current calendar year.

APPENDIX V

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

Recommendation Number:

1. **Resolved.** In order to close this recommendation, please document the final management action taken to remedy the recommendation.
2. **Resolved.** Same as recommendation 1.
3. **Resolved.** Same as recommendation 1.