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 08-20
March 2008

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

EXECUTIVE SUMMARY

Criminal organizations and individuals frequently use the telecommunication systems of the United States to further serious crimes, including terrorism, kidnapping, extortion, organized crime, drug trafficking, and public corruption. One of the most effective tools law enforcement agencies use to acquire evidence of these crimes is electronic surveillance techniques.[1] However, continuing advances in telecommunication technology have impaired and in some instances prevented law enforcement from conducting some types of authorized electronic surveillance.

With advances in telecommunication technologies and law enforcement's growing concern about the ability to conduct authorized electronic surveillance, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994. The purpose of CALEA was to enable law enforcement to conduct electronic surveillance despite the deployment of new technologies and wireless services that have altered the character of electronic surveillance. To facilitate CALEA implementation, Congress appropriated nearly $500 million to the Telecommunications Carrier Compliance Fund (TCCF). The Attorney General was designated to reimburse telecommunication carriers for the cost of modifying equipment, facilities, or services installed or deployed on or before January 1, 1995, to assist law enforcement authorities in carrying out its surveillance activities. In February 1995, the Attorney General delegated CALEA management to the Federal Bureau of Investigation (FBI).

---

* The full version of this report includes information that the FBI considered to be law enforcement sensitive or proprietary and confidential in nature, and therefore could not be publicly released. To create this public version of the report, the OIG: (1) redacted the portions of the full report that the FBI considered sensitive, and (2) indicated where those redactions were made.

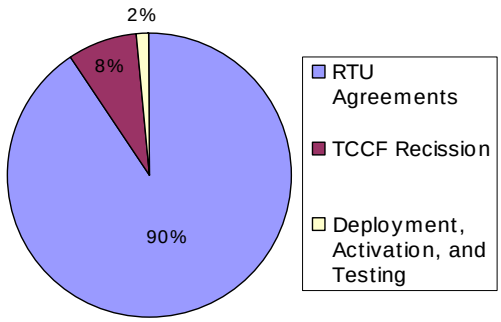
[1] Electronic surveillance consists of the acquisition of call-identifying information and the interception of communications content. Call-identifying information identifies the origin, direction, destination, or termination of a communication generated or received by a subject of surveillance, while content is the substance of a communication.

Background

Pursuant to CALEA, the Department of Justice (DOJ) Office of the Inspector General (OIG) is required to report to Congress biennially on the equipment, facilities, and services modified to comply with CALEA requirements.[2] In prior audits, we reported on FBI agreements that applied TCCF funds to pay manufacturers for software feature updates and associated licensing fees, referred to as Right-To-Use (RTU) agreements. These payments allowed carriers to obtain CALEA software solutions once the FBI reimbursed the manufacturer for development costs. As shown in the following table, over the past 10 years the FBI spent almost $452 million on these RTU licenses.

TCCF COST SUMMARY
(1997-2007)

Type of Cost	Amount ($)*
RTU Agreements	451.7
Carrier CALEA Solution Deployment, Activation, and Testing	7.5
2007 TCCF Rescissions	40.3
TOTAL	**$ 499.5**



Source: FBI
* Figures in millions, rounded to nearest $100,000

[2] Since 1998, the OIG has issued five audit reports on CALEA implementation activities. Appendix II presents a summary of these reports and their findings and recommendations.

Before finalizing various RTU software license agreements, the FBI prepared reports entitled *Determination and Findings Regarding the Implementation of CALEA* because it was unable to verify the reasonableness of the cost of the RTU software licenses through traditional means, such as actual cost data or price estimates. According to the FBI, manufacturers were unwilling to furnish adequate cost or price information despite repeated FBI attempts to obtain such information through extensive negotiations. As a result, prior OIG reports have not offered an opinion regarding the reasonableness of the nearly $452 million the FBI spent on RTU licensing costs.[3]

In addition to the RTU agreements, the FBI has spent nearly $7.5 million, including about $4.6 million during this audit period, to pay wire line carriers for deploying, activating, and testing CALEA solutions. By the end of the audit period, the FBI expended a total of $459 million primarily on RTU license agreements and carrier CALEA solution deployment and testing. In 2007, Congress rescinded over $40 million from the TCCF, which left only $5,037 remaining in the fund.[4]

Audit Approach

The objectives of the audit were to determine: (1) the type of equipment, facilities, and services brought into compliance with CALEA, and (2) whether payments during the most recent 2-year review period for CALEA-required modifications were reasonable and cost effective. Considering the 2007 TCCF rescissions, our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant.

Our review focused on TCCF-financed activity occurring between January 1, 2006, and December 31, 2007. During the audit, we interviewed officials at FBI Headquarters, the FBI CALEA Implementation Unit, various units of FBI's Finance Division, and selected telecommunication providers. We also reviewed CALEA annual reports, assessments, associated files, contracts, obligations, and payments for CALEA-implementation activities.

---

[3] Our March 2006 report found, in part, that the FBI negotiated substantially reduced costs for the RTU licenses at least when compared to the manufacturers' initial cost proposals for these licenses. See U.S. Department of Justice Office of the Inspector General, *The Implementation of the Communications Assistance for Law Enforcement Act*, Audit Report 06-13 (March 2006), 15.

[4] Pub. L. Nos. 110-5 (2007) and 110-161 (2007).

Results in Brief

Between January 2006 and December 2007, the FBI spent a total of $4.6 million in TCCF funds to implement CALEA provisions. Of this amount, the FBI paid $4.5 million to two carriers under formal agreements to deploy CALEA solutions on over [SENSITIVE INFORMATION REDACTED] network switches, while nearly $100,000 was paid to a carrier for testing various CALEA solutions on its telecommunication network.[5] We could not assess the reasonableness or cost effectiveness of TCCF expenditures paid during the audit period because the FBI based these costs on negotiated terms instead of independent cost data or competing price estimates derived from more than one carrier.

As of December 2007, the end of the audit period, only $5,037 remained in the TCCF. The FBI is working with DOJ to transfer remaining TCCF funds to the DOJ Working Capital Fund and close the TCCF account. As a result, the report makes no recommendations. The remaining sections of this Executive Summary describe in more detail our audit results.

TCCF Expenditures

During the 2-year period under review, the FBI had formal agreements with two carriers to deploy CALEA solutions. At a total cost of $4.5 million, carriers certified that they upgraded their networks to allow law enforcement agencies to receive CALEA compliant surveillance results. Although internal FBI communications stated that the $4.5 million compensated carriers only for reasonable CALEA deployment costs, the FBI did not provide any evidence based on independent cost data or competing price estimates to support this statement.[6] As a result, we could not determine the reasonableness or cost effectiveness of payments made to carriers that deployed CALEA solutions under these agreements.

The FBI also paid nearly $100,000 to a carrier to test various CALEA solutions. Our assessment of the reasonableness and cost effectiveness of

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

[6] Before one carrier deployment agreement was finalized, the FBI conducted an audit to assess the fairness and reasonableness of proposed carrier costs. Although the FBI audit found that certain proposed costs were reasonable, the FBI audit did not consider independent cost data or competing price estimates in making this determination. As a result, we could not use the results of the FBI audit in our analysis of whether carrier deployment costs paid under the agreement were reasonable or cost effective.

these payments found that the FBI based them on negotiated terms instead of independent cost data. However, the FBI has issued statements justifying the costs associated with various CALEA solutions because such solutions would result in long-term financial savings to law enforcement agencies.

Measuring and Enhancing CALEA's Impact on Electronic Surveillance

Over the past 2 years, the FBI has continued developing tools and implementing resources to help facilitate and measure CALEA compliance of telecommunication providers. We found that the FBI has hosted and attended forums and other types of meetings with law enforcement personnel, developed and updated its AskCALEA website, conducted and issued annual threat assessment surveys, and surveyed telecommunication providers regarding the status of CALEA solutions on their networks.[7]

The FBI participates as a member of the telecommunication industry electronic surveillance standard-setting groups.[8] However, FBI officials advised that because of the voting structure of these groups, which are industry dominated, the FBI has had limited ability to ensure that adequate CALEA solutions are available for newly developed communication standards. As a result, the FBI is concentrating its efforts on working with and testing packet-mode based telecommunication providers and manufacturers to develop and deploy adequate CALEA solutions.[9]

Conclusion

Of the nearly $4.6 million spent between January 2006 and December 2007, about $4.5 million was paid to two carriers to deploy CALEA-related solutions. The FBI also paid $96,878 to a carrier for testing CALEA solutions on its telecommunication network. We could not assess the reasonableness or cost effectiveness of these expenditures because the FBI did not base its costs on independent cost data or competing price estimates.

---

[7] AskCALEA is a website established by the FBI to assist law enforcement and carrier personnel with surveillance issues.

[8] Electronic surveillance standards provide the basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance.

[9] A telecommunication network based on packet-mode technology operates by routing and transferring data by means of packets of information.

Our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant. We found that the FBI has revamped its testing group and enhanced its resources to help measure and facilitate CALEA compliance. In addition, the FBI has implemented an extensive testing program to ensure carrier compliance and capability with regard to emerging technologies.

At the end of the audit period, only $5,037 remained in the TCCF. According to a DOJ finance official, the FBI is working with DOJ to transfer the remaining funds to the DOJ Working Capital Fund and close the TCCF.

We provided a draft of the report to the FBI for comment and review. Since the report made no recommendations, the FBI did not provide a response and we issued the report closed.

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

TABLE OF CONTENTS

INTRODUCTION

Law enforcement agencies use electronic surveillance techniques to acquire evidence for criminal and terrorism investigations. Traditionally, electronic surveillance involved using various techniques to intercept and obtain communication information and content. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) and portions of the Electronic Communications Privacy Act (ECPA) are the primary laws governing the use of electronic surveillance in criminal investigations.[10] Similar rules governing electronic surveillance conducted during foreign intelligence, counterintelligence, and terrorism investigations are found in the Foreign Intelligence Surveillance Act (FISA).[11]

The rapid pace of technological changes in the way people communicate has presented challenges to law enforcement agencies conducting electronic surveillance for criminal investigations. In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to ensure that the telecommunication industry would build surveillance solutions into the technologies they deploy that allow law enforcement agencies to continue to obtain electronic surveillance information. According to CALEA's assistance capability requirements, telecommunication carriers are to isolate, intercept, and deliver communication content and call identifying information to law enforcement pursuant to lawful authorization.[12]

CALEA Provisions and Responsibilities

CALEA assigned certain responsibilities to the Attorney General, the Federal Communications Commission (FCC), telecommunication carriers, equipment manufacturers (manufacturers), and the Department of Justice (DOJ) Office of the Inspector General (OIG). In February 1995, the Attorney

[10] Title III, as amended, contains the procedures law enforcement agencies must follow to obtain the necessary judicial authorization to conduct electronic surveillance, while ECPA, as amended, extends Title III coverage to the contents of electronic messages such as e-mail and to data transmissions from facsimiles and pagers.

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

[12] Call-identifying information is defined as dialed number information that identifies the origin, direction, destination, or termination of any communication generated or received by a subject of surveillance. Content is defined as the substance or meaning of a communication.

General delegated CALEA management to the Federal Bureau of Investigation (FBI). Table 1 outlines each entity with CALEA responsibilities.

TABLE 1: SUMMARY OF CALEA STATUTORY RESPONSIBILITIES

Entity	Responsibility
FBI	Ensures industry-wide implementation of the assistance capability requirements.
	Consults with state and local law enforcement agencies.
	Provides estimates to the telecommunication industry on the number of interceptions that government agencies may need to conduct.
	Establishes rules to facilitate carrier reimbursements.
	Allocates appropriated funds to carriers in a manner consistent with law enforcement priorities.
	Annually reports to Congress the amount of carrier payments during the preceding year and the projected payments for the current year.
FCC	Determines which entities are telecommunication carriers and may exempt any entity or category as a carrier by rulemaking and consulting with the FBI.
	Establishes technical standards for compliance with assistance capability requirements if industry associations fail to issue technical standards, or if a government agency or any other person believes that industry-adopted standards are deficient.[13]
	Reviews and grants or denies petitions for extensions.
Telecommunication Carriers and Other Service Providers[14]	Ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the CALEA assistance capability requirements.
Equipment Manufacturers	Make available all features or modifications necessary to meet assistance capability requirements, including consulting with carriers over current and planned equipment.
OIG[15]	Report to Congress biennially on the type of equipment, facilities, and services brought into compliance with CALEA and whether costs paid to each carrier for CALEA-required modifications were reasonable and cost effective.

Source: OIG Analysis of CALEA

Effective implementation of CALEA's provisions is dependant on the joint efforts of government agencies, service providers, and

[13] Electronic surveillance standards provide a basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance.

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

[15] See Appendix II for a summary of prior OIG audits.

telecommunications equipment manufacturers subject to the law's requirements.

The Telecommunications Carrier Compliance Fund

CALEA authorized the Attorney General to reimburse telecommunication carriers for modifications made to meet CALEA assistance capability requirements on their equipment, facilities, or services installed or deployed on or before January 1, 1995.[16] In 1996, Congress established the Telecommunications Carrier Compliance Fund (TCCF) and, over subsequent years, appropriated nearly $500 million for such reimbursements, as shown in Table 2 below.

TABLE 2: DEPOSITS TO THE TELECOMMUNICATIONS CARRIER COMPLIANCE FUND

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

Source: FBI

The Attorney General delegated the responsibilities of overseeing the TCCF and compensating carriers for CALEA compliance modifications to the FBI. To carry out these responsibilities, the FBI established a CALEA Implementation Unit (CIU) in its Operational Technology Division and an Offsite Contract Unit (OSCU) in its Finance Division.[17] The CIU worked with carriers, manufacturers, and other telecommunication industry representatives to develop and deploy CALEA-mandated solutions while the OSCU awarded and administered CALEA implementation agreements and audited proposed implementation costs.

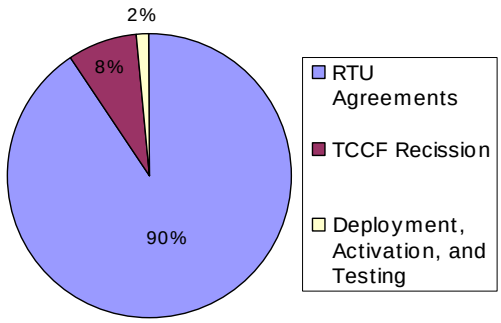
[16] 47 U.S.C. §1008

[17] The FBI's Operational Technology Division was formerly called the Investigative Technology Division, while the OSCU was formerly called the Telecommunications Contract and Audit Unit.

In prior OIG audits, we reported on FBI agreements that applied TCCF funds to pay manufacturers for software feature updates and associated licensing fees, referred to as Right-To-Use (RTU) agreements. These payments allowed carriers to obtain CALEA software solutions once the FBI reimbursed development costs to the manufacturer.[18] As shown in the Table 3, the FBI has spent about $451.7 million on these RTU licenses since 1997.

TABLE 3: TCCF COST SUMMARY (1997-2007)

Type of Cost	Amount ($)*
RTU Agreements[19]	451.7
Carrier CALEA Solution Deployment, Activation, and Testing	7.5
2007 TCCF Rescissions	40.3
TOTAL	**$ 499.5**



Source: FBI
* Figures in millions, rounded to nearest $100,000

In addition to the RTU agreements, the FBI spent approximately $7.5 million to reimburse wire line carriers for deployment, activation, and testing costs of solutions that allow carriers to comply with CALEA requirements, or CALEA solutions. In 2007, Congress rescinded over $40 million from the TCCF.[20] According to a DOJ finance official, the FBI is working with DOJ to transfer the $5,037 remaining in the TCCF to the DOJ's Working Capital Fund and subsequently close the TCCF account.

[18] Our March 2006 report found that the FBI was not provided the cost information necessary to determine the reasonableness of costs associated with RTU agreements. Therefore, the audit offered no opinion on the reasonableness or cost effectiveness of these expenses. See 2006 OIG CALEA Implementation Report, 16.

[19] Included in the $451.7 million figure is a late payment penalty of about $5,000, for which the FBI could provide no explanation.

[20] Pub. L. Nos. 110-5 (2007) and 110-161 (2007).

Audit Objectives and Scope

The objectives of the audit were to determine: (1) the type of equipment, facilities, and services brought into compliance with CALEA, and (2) whether payments during the most recent 2-year review period for CALEA-required modifications were reasonable and cost effective. In light of the TCCF rescissions that occurred in 2007, our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant.

Our review focused on TCCF-financed activity occurring between January 1, 2006, and December 31, 2007. During the audit, we interviewed officials at FBI Headquarters, the CIU, various FBI Finance Division units, and selected telecommunication providers. We reviewed CALEA annual reports, assessments, associated files, contracts, obligations, and payments for CALEA-implementation

AUDIT RESULTS

During the 2-year period ending in December 2007, the FBI spent $4.6 million in TCCF funds to implement CALEA provisions. Of this amount, the FBI paid about $4.5 million to two carriers to deploy CALEA-related solutions on over [SENSITIVE INFORMATION REDACTED] wire line networks switches. In addition, another carrier received $96,878 for costs incurred from testing software developed under 4 different agreements. We could not assess the reasonableness or cost effectiveness of these expenditures because the FBI did not base payments on independent cost data or competing price estimates. During this review period, the FBI revamped its CALEA testing team and implemented new resources to help measure and facilitate CALEA compliance capabilities of telecommunication providers and manufacturers.

TCCF Expenditures

Between January 2006 and December 2007, the FBI spent a total of $4.6 million in TCCF funds to implement CALEA. Table 4 presents a summary of TCCF payment activity during this period.

TABLE 4: TCCF EXPENDITURES 2006-2008

Cost	Amount ($)
Carrier Deployment Agreements	4,509,110
Carrier Testing	96,878
TOTAL	**$4,605,988**

Source: FBI and OIG analysis of FBI financial records

The following sections analyze the TCCF expenditures made during the audit period ending December 2007.

Carrier Deployment Agreements

The ability of law enforcement agencies to conduct authorized electronic surveillance anywhere within a telecommunication network is a central tenet of CALEA. According to internal FBI correspondence, if CALEA capabilities and dial-out solutions were not widely deployed, the ability of law enforcement to conduct surveillance would be, "limited to a few basic and costly surveillance functions." Therefore, after spending about

$452 million to pay manufacturers for costs of designing and developing CALEA software solutions under RTU licensing agreements, the FBI began assessing how best to deploy the developed technologies nationwide.

To maximize the benefits to law enforcement agencies, the FBI concentrated on activating CALEA software solutions on pre-1995 equipment used by the regional bell operating companies (RBOC). According to FBI documents, the RBOCs supported over 50 percent of all wire line switches in the United States.[21] To begin large-scale CALEA capability deployment, the FBI began negotiating reimbursement agreements with Verizon Communications, Inc. (Verizon); BellSouth Corporation (BellSouth); Qwest Communications International, Inc. (Qwest); and SBC Communications, Inc. (SBC) in 2004.[22]

We found that the FBI finalized agreements with two carriers – Verizon and BellSouth – and during our audit period paid a total of $4.5 million for costs associated with activating the RTU software CALEA features and dial-out solutions on over [SENSITIVE INFORMATION REDACTED] network switches.[23] In our previous CALEA audit report, we expressed concern over the FBI's plans to reimburse traditional wire line carriers the costs associated with deploying CALEA solutions on pre-1995 switches.[24] The report recommended that since CALEA implementation was delayed significantly and communication technologies had changed drastically since CALEA's enactment, the FBI should reexamine the benefits of activating CALEA software solutions on wire line systems. As discussed earlier in the report, however, Congress rescinded over $40 million from the TCCF in 2007. According to FBI's last annual CALEA report, the TCCF rescission effectively ended FBI plans to establish future reimbursement agreements with additional wire line carriers.[25]

---

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

[22] In 2005, SBC purchased AT&T and renamed itself AT&T. In 2006, the new AT&T acquired and merged with BellSouth.

[23] FBI officials added that discussions held with Qwest and SBC did not result in formalized reimbursement agreements. According to the FBI, Qwest and SBC deployed CALEA solutions on their networks without TCCF reimbursement.

[24] 2006 OIG CALEA Implementation Report, 51.

[25] Federal Bureau of Investigation, *Communications Assistance for Law Enforcement Act - Twelfth Annual Report to Congress* (2006), 13.

Verizon Contract

According to internal documents, the FBI had many discussions with Verizon officials about payments for deploying CALEA solutions developed under various RTU agreements. Since the FBI did not have an established history of reimbursing carriers for costs associated with implementing CALEA capabilities, the negotiations considered a series of cost proposals. To serve as a starting point for these negotiations, Verizon submitted a preliminary proposal detailing costs associated with activating CALEA solutions on its entire wire line network.

To determine the total reimbursable cost, Verizon first estimated the cost of: (1) upgrading equipment associated with its pre-1995 switches; and (2) deploying CALEA solutions based on security, training, management, and labor expenses to its entire wire line network. In communications with the FBI, Verizon first reported that it would cost about $[SENSITIVE INFORMATION REDACTED] to upgrade equipment and deploy CALEA solutions to its pre-1995 platforms. During subsequent negotiations with the carrier, the FBI identified certain proposed costs as unrecoverable under CALEA.[26] [SENSITIVE INFORMATION REDACTED]

In October 2004, the FBI Finance Division performed an audit of Verizon's reduced cost estimate for acceptability in negotiating a final contract price. The audit found that the $[SENSITIVE INFORMATION REDACTED] proposal appeared to be overstated and determined that the FBI should only pay Verizon for costs associated with: (1) training its personnel on new software; (2) implementing security system modifications; (3) testing upgraded software; and (4) direct costs of deploying CALEA software features, including dial-out enhancements, on three of its major platforms. As shown by Table 5, although the FBI audit did not take issue with the costs associated with activating network switches or security system development and training, the audit found that the FBI should not pay for other operating and support costs.

[26] Pursuant to CALEA, carriers can only recover costs directly associated with upgrading equipment deployed on or before January 1, 1995, 47 U.S.C. §1008(a) (2005).

TABLE 5: FBI ADJUSTMENTS TO CARRIER COST PROPOSAL

Cost Category	Revised Verizon Estimate ($)	FBI Audit Adjusted Figures ($)	Reason for Audit Adjustment
Security Administrative System development and training	898,290	898,290	n/a
Technical Operations Center testing, support, and maintenance	1,358,566	680,147	The FBI excluded costs: (1) associated with internal carrier testing of switches not subject to CALEA enhancements, and (2) reimbursable via surveillance fees charged by the carrier to law enforcement agencies.
Internal policies, instructions, and standards development	58,084	58,084	n/a
Third-party vendor costs	288,456	0	Verizon derived these costs from internal requirements it had with a third-party contractor. As a result, the FBI excluded these costs as they were considered to be outside of the scope of its CALEA compliance effort.
Planning and tracking switch activations	29,340	29,340	n/a
Switch equipment	351,710	0	The FBI excluded receiver and sender cards as capacity costs.
Switch activation	531,976	531,976	n/a
Memory for dial-out solution capability	733,170	733,170	n/a
TOTALS	**$4,249,592**	**$2,931,007**	

Source: FBI audit number P04-TL-004 and associated documentation.

Based on the audit results, the FBI formalized a contract to pay Verizon the costs associated with upgrading switches in November 2005. The contract stated that Verizon would be paid $[SENSITIVE INFORMATION REDACTED] for each switch activated with CALEA compliant software features.[27] As shown by Table 6, the agreement based the $[SENSITIVE

[27] According to the agreement, the FBI could reimburse a carrier for costs either via a cost reimbursement method or a firm-fixed price method. FBI officials indicated that they preferred the firm-fixed price method for this agreement because the carrier would only receive reimbursement once it certified that it had upgraded switches under the agreement. An FBI official also told us that the firm-fixed price method is more efficient than a cost reimbursement method because the firm-fixed price method does not require the FBI to perform additional financial reviews on incurred costs.

INFORMATION REDACTED] figure on the total cost Verizon would incur to upgrade its platforms, divided by the number of switches Verizon agreed to upgrade.

TABLE 6: VERIZON CONTRACT PAYMENT DETAILS

Final approved cost	$2,907,000
Number of switches to upgrade	1,140
Cost per certified upgraded switch	$2,550

Source: FBI-Verizon agreement dated November 3, 2005

To receive TCCF funds, the agreement called on Verizon to submit quarterly invoices to the FBI that: (1) listed the specific switches activated pursuant to the agreement; and (2) certified that all listed switches, "have been modified to provide all CALEA Assistance Capabilities required." Between April 2006 and January 2007, the FBI received [SENSITIVE INFORMATION REDACTED] invoices from Verizon certifying the upgrade of [SENSITIVE INFORMATION REDACTED] switches at a total cost of $2,901,900.[28]

BellSouth Agreement

The FBI also negotiated an agreement with BellSouth to reimburse costs associated with deploying CALEA solutions on its wire line network. According to officials at the OSCU, the FBI sought to have BellSouth deploy the same types of CALEA solutions to similar types of switch platforms as it had with Verizon.

In November 2005, the FBI formalized an agreement to pay BellSouth $1,607,210 to deploy CALEA software on [SENSITIVE INFORMATION REDACTED] network switches. According to these FBI officials, the agreed upon payment was: (1) based on performance terms negotiated during the Verizon negotiations; and (2) "in line with" the costs reimbursed under the Verizon contract on a per switch basis. Therefore, the FBI did not conduct an extensive series of negotiations with BellSouth, like it did with Verizon, before finalizing the BellSouth agreement. In April 2006, BellSouth certified that it had modified [SENSITIVE INFORMATION REDACTED] switches to provide CALEA assistance capabilities called for by the agreement and the following month invoiced the FBI $1,607,210.

[28] [SENSITIVE INFORMATION REDACTED] As a result, the FBI and Verizon agreed to adjust the agreement cost to $2,901,900.

Analysis and Assessment of Carrier Agreement Costs

We reviewed invoices sent by Verizon and BellSouth and found that each invoice: (1) individually listed the [SENSITIVE INFORMATION REDACTED] switches that either Verizon or BellSouth activated during the performance period of the agreements, and (2) included statements by the carriers certifying activation of CALEA compliant software on the individually identified switches. However, since the FBI did not conduct verification testing on the switches under either agreement, we spoke with carrier representatives to confirm the number of switches brought into compliance with TCCF funds. These officials told us that certifications provided to the FBI verifying the activation of CALEA software on the [SENSITIVE INFORMATION REDACTED] switches accurately reflected each carrier's activity under the agreement.

On a "per switch" basis, we calculated that the FBI paid Verizon $[SENSITIVE INFORMATION REDACTED] per switch, while BellSouth recovered an average of $[SENSITIVE INFORMATION REDACTED] per switch. FBI officials told us that the difference in rates was based on [SENSITIVE INFORMATION REDACTED]. We reviewed records of discussions held between the FBI and carriers to assess whether these costs were reasonable. We identified internal FBI communications authorizing payments that stated that the $4.5 million paid compensated carriers for only reasonable CALEA deployment costs. However, the FBI did not provide any evidence based on independent cost data or competing price estimates to support this statement.[29] Considering this and the variance in carrier size and equipment, we cannot determine whether the $4.5 million provided to the carriers was a reasonable cost to upgrade [SENSITIVE INFORMATION REDACTED] switches.

To determine the cost effectiveness, or impact, of the total $4.5 million the FBI paid Verizon and BellSouth to deploy their CALEA solutions, we asked carrier representatives how often they used the [SENSITIVE INFORMATION REDACTED] activated switches to capture surveillance results. Carrier representatives told us that they do not track surveillance intercepts by individual switch. As a result, we could not determine whether or how the carriers use their switches to conduct law enforcement surveillance intercepts.

[29] As stated previously, the FBI audited the proposed Verizon deployment costs to assess their fairness and reasonableness. The FBI audit found that certain proposed costs were fair and reasonable. However, the FBI audit did not consider independent cost data or competing price estimates. As a result, we could not use the results of the FBI audit in our determining of whether carrier deployment costs were reasonable or cost effective.

Carrier CALEA Solution Tests

During the audit period, the FBI paid a total of $96,878 for costs incurred by Qwest under four separate agreements finalized before January 2006. Three of the four agreements called on Qwest to test CALEA solutions developed by an equipment manufacturer, while another required Qwest to deploy and test surveillance capability solutions in anticipation of the 2002 Winter Olympic Games.

The FBI entered into three agreements with Nortel Networks Corporation (Nortel) to develop and include various CALEA solutions in its switch software. Under these agreements, Qwest worked with Nortel to test the developed capabilities and the FBI agreed to pay Qwest for planning, installing, deploying, testing, and retesting the solutions on its switches. At the conclusion of its dial-out testing, Qwest invoiced its costs under the agreements and received payments from the TCCF totaling $63,495.

In conjunction with the 2002 Winter Olympic Games, the FBI entered into an agreement with Qwest to ensure that 29 designated network switches in and around Salt Lake City, Utah, had the CALEA capabilities required for court-ordered electronic surveillance. The agreement also called on the FBI and Qwest to develop a technical plan that used a delivery network that carried court-ordered surveillance information from Qwest network switches to law enforcement agencies. In 2003, the FBI modified the agreement to allow Qwest to recover $33,383 in costs resulting from testing software on 29 designated switches.[30]

The FBI did not perform a formal technical review of the manufacturer agreements because Nortel did not provide cost data showing actual expenses incurred by developing CALEA solutions.[31] As a result, the FBI relied on various Determination of Findings it compiled to justify the reasonableness of CALEA solution costs. In one such document, the FBI's Operational Technology Division and the FBI's Finance Division stated that the telecommunication industry's reluctance to offer specific cost information stems from closely-guarded business practices. For example,

[30] In FY 2002, the FBI also paid Qwest $2.2 million from the TCCF for developing and implementing CALEA capabilities in the Salt Lake City area. See U.S. Department of Justice Office of the Inspector General, *The Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation*, Audit Report 04-19 (April 2004), 10.

[31] Although the FBI requested underlying developmental costs associated with various CALEA solutions from each manufacturer, manufacturers were unable or unwilling to provide such cost information to the FBI.

telecommunication industry non-disclosure agreements often restrict parties from publicly releasing pricing data. Nonetheless, the FBI concluded that costs associated with certain CALEA solutions would be reasonable since they would result in long-term financial savings to law enforcement agencies.

According to records provided by OSCU, the CIU specifically reviewed Qwest testing costs associated with the 2002 Winter Olympic Games. However, CIU's cost review did not consider independent cost data or competing price estimates. Therefore, we cannot offer an opinion on the reasonableness or cost effectiveness of the total $96,878 received by Qwest.

Measuring and Enhancing CALEA's Impact on Electronic Surveillance

In light of the $40 million in TCCF rescissions that occurred in 2007, our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant. Our audit found that, during the reporting period, the FBI has developed tools and resources to help facilitate and measure CALEA compliance. In addition, the FBI has hosted and attended forums and other types of meetings with law enforcement personnel, developed and updated the AskCALEA website, conducted and issued annual threat assessment surveys, and surveyed telecommunication providers regarding the status of CALEA solutions on their networks.[32]

To assist in its monitoring efforts, the FBI joined DOJ in its *Joint Petition for Expedited Rulemaking*, which asked the FCC to adopt a phase-in plan requiring carriers to provide information regarding their CALEA compliance status by certain dates.[33] In its *Second Report and Order*, the FCC declined DOJ's request but developed a form (Form 445) for certain service providers to use in reporting their extent of CALEA compliance to the FCC by the compliance deadline.[34] Using information provided to it by law enforcement and voluntarily reported by telecommunication providers, the

[32] AskCALEA is a website established and monitored by the FBI to assist law enforcement and carrier personnel with surveillance issues.

[33] In its *First Report and Order*, the FCC ruled that providers of Voice over Internet Protocol (VoIP) and broadband services must comply with CALEA. On May 12, 2006, the FCC issued its *Second Report and Order* and reaffirmed that providers of VoIP and broadband services must be CALEA compliant by May 14, 2007.

[34] FBI officials told us that they also received copies of Forms 445 submitted to the FCC by various telecommunication providers and used, in part, results reported on these forms to set testing priorities.

FBI has conducted CALEA solution tests with individual providers and trusted third parties. However, due to the rapid public emergence of packet-mode technology, such as Voice over Internet Protocol (VoIP) and broadband services, the FBI is focusing on establishing electronic surveillance solutions for these new and emerging technologies.[35]

Law Enforcement Forums and Working Groups

One of the ways the FBI has measured the impact of CALEA is through periodic meetings, including the FBI-sponsored Law Enforcement Technical Forum, the Law Enforcement Executive Forum, and various non-FBI sponsored law enforcement meetings. FBI officials stated that these meetings give law enforcement officials opportunities to discuss problems encountered while requesting or receiving electronic surveillance.

In addition, the FBI has established the Carrier Relations Working Group (CRWG) and the Electronic Surveillance Working Group (ESWG) to address law enforcement wiretap issues. Both working groups are comprised of members of the Law Enforcement Technical Forum. The CRWG works with providers and federal, state, and local law enforcement agencies to minimize the cost of electronic surveillance, while the ESWG focuses on assisting law enforcement surveillance efforts in the face of rapidly emerging telecommunication technologies.

Law Enforcement and Telecommunication Provider Surveys

The FBI prepares and issues Threat Assessment Survey Reports each year from responses received from National Technical Investigator Association meetings and various training sessions hosted by federal law enforcement agencies. As shown by Table 7, the 2005 and 2006 surveys detailed various areas affecting law enforcement's ability to conduct and receive electronic surveillance.

[35] A communication network based on packet-mode technology operates by routing and transferring data by means of addressed packets of information.

TABLE 7: SELECTED 2005 AND 2006 THREAT ASSESSMENT SURVEY RESULTS

Survey Response	2005 Survey	2006 Survey
Top emerging technologies	1. VoIP 2. Broadband 3. Prepaid Cell Phones	1. VoIP 2. Broadband 3. Prepaid Cell Phones
Attempted surveillance on VoIP communications? (Yes/No)	8% Yes	34% Yes
Attempted surveillance on broadband? (Yes/No)	Question not surveyed	35% Yes
Cost of surveillance has limited intercepts performed? (Yes/No)	68% Yes	65% Yes
Surveillance results are not provided in a usable format? (Agree/Disagree)	60% Agree	12% Agree
Have investigations been hindered by provider non-compliance with CALEA? (Yes/No)	22% Yes	41% Yes

Sources: 2005 and 2006 FBI Threat Assessment Reports

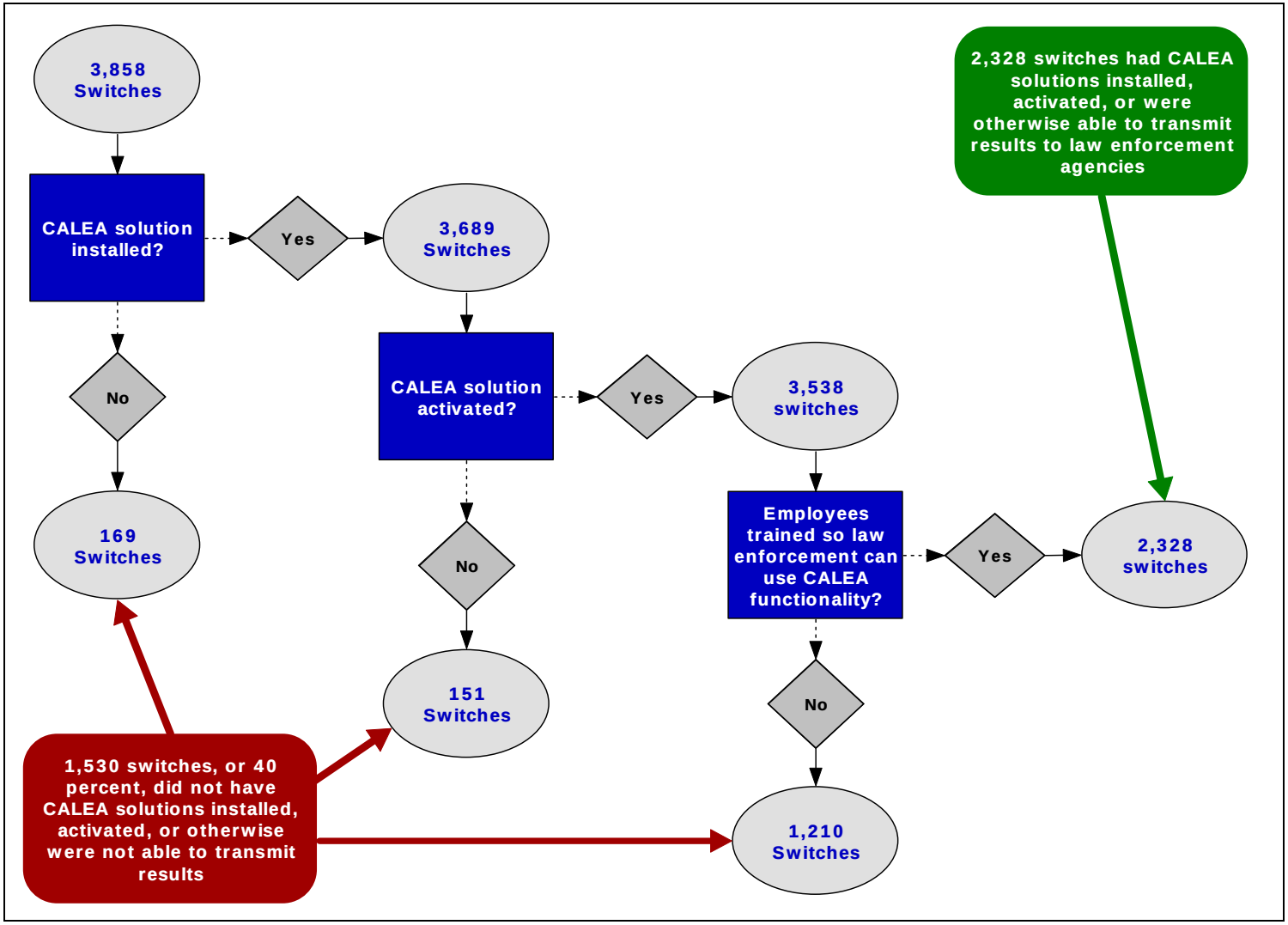
The 2005 and 2006 surveys showed that various law enforcement agencies perceive the same types of technology – [SENSITIVE INFORMATION REDACTED] – as the "hot items" most in need of CALEA solutions. The 2006 survey revealed a four-fold increase, [SENSITIVE INFORMATION REDACTED], in law enforcement agencies conducting electronic surveillance with a VoIP provider. While the 2006 survey responses demonstrated improvement in the way providers report surveillance results, [SENSITIVE INFORMATION REDACTED] of respondents stated that investigations continue to be hindered because telecommunication providers were not CALEA compliant. According to these responses, some of the problems stemmed from a lack of provider CALEA solutions. In the end, however, law enforcement representatives reported that their greatest concern regarding electronic surveillance remained its high cost.

In December 2005, the FBI conducted a survey of telecommunications providers to gauge their CALEA compliance status.[36] According to the FBI, 258 carriers responded to the survey and reported the CALEA solution status on a total of 3,858 switches.[37] As shown in Figure A, providers reported that 1,530 or nearly 40 percent of their switches could not be used to produce CALEA-compliant electronic surveillance results.

[36] The FBI conducted the survey in response to our 2004 OIG report recommendation that the FBI collect and maintain data on the number of carrier switches that are and are not CALEA-compliant.

[37] The FBI estimates that there are a total about 20,000 network switches in the United States. Total survey responses reported on the CALEA-compliance status of 3,858 network switches. Therefore, the survey reported on about 19 percent of the total estimated number of network switches in the United States.

FIGURE A: FBI TELECOMMUNICATION PROVIDER SURVEY RESULTS



Source: FBI

Figure A also shows that telecommunication providers indicated that they did not install manufacturer updates containing the software required to effectuate a CALEA-compliant wiretap on 169 switches. Considering the total switches that had CALEA software solutions installed, providers have not yet modified or adjusted their networks to activate the software on 151 switches. Meanwhile, of the 3,538 switches that have CALEA solutions both installed and activated, the survey reported that 1,210 switches are being administered by carrier personnel that have not been trained to use the intercept software or otherwise make CALEA functionality available to law enforcement.

AskCALEA Website and Help Desk

Considering the results of these surveys, we asked the FBI what it has done, in addition to the carrier deployment agreements, to help ensure deployment of CALEA solutions on provider networks. The FBI stated that since it can only work to enforce CALEA compliance when alerted to surveillance inadequacies by law enforcement, it has revamped its AskCALEA website to assist, in a user-friendly way, law enforcement officers and carrier personnel with surveillance issues. The website's AskCALEA Help Desk (Help Desk) maintains a law enforcement-restricted database that details various wiretap issues and CIU remedies, as shown in Figure B.

FIGURE B: SCREENSHOT OF ASKCALEA HELP DESK DATABASE

Action	Received Date	Platform	Organization	Description
FILE	12/27/2007	N/A	Montgomery County MD Police	Problems with CDC and CCC delivery
FILE	12/19/2007	N/A	Baltimore County Police	Having difficulty using the Cell Site database
FILE	12/14/2007	N/A	FBI - Omaha	Needed Contact in Sprint for provisioning a surveillance
FILE	11/30/2007	N/A	Kenner Louisiana Police	Wanted to know how to access the Law Enforcement Forum on AskCALEA
FILE	11/27/2007	N/A	Secret Service	Needed access to the Carrier Database on the Law Enforcement Forum
FILE	11/6/2007	N/A	Racine Police Department	Wanted help with AT&T subpoena compliance department
FILE	11/5/2007	DMS-MSC	Taylorsville, Utah Police	Needs number to investigate SMS storage policy

Source: FBI

User names and passwords provided by the Help Desk allow law enforcement personnel to search database fields to find a solution to their surveillance issue. If the inquiring law enforcement user has a new or previously undocumented surveillance problem, they can use the database to submit solution requests to the Help Desk. The CIU told us that it regularly monitors Help Desk activities and carefully reviews new requests in developing additional CALEA solutions.

Technology Standards Groups

The FBI also participates in several domestic and international technology standard-setting groups to: (1) encourage carriers to meet their CALEA responsibilities, and (2) promote effective liaison functions with the telecommunications industry. As a member of these groups, the FBI informs provider and manufacturer representatives about CALEA assistance capability requirements and responsibilities, especially concerning emerging technologies. Table 8 lists the various standard-setting groups with which the FBI participates.

TABLE 8: TECHNOLOGY STANDARD-SETTING GROUPS

United States	International
American Association of Paging Carriers	International Softswitch Consortium
Telecommunication Industry Association	European Telecommunications Standards Institute
Alliance for Telecommunications Industry Solutions	
American Mobile Telecommunications Association	Third Generation Partnership Project

Source: FBI

Participants in these standard-setting groups have a vote in the decision-making process when developing new technological standards. Since the FBI has only one vote within each group, FBI officials told us that manufacturers, engineers, and private industry representatives can easily overrule their attempts to advocate guidelines that ensure newly established standards comply with CALEA prior to public release.

Developing and Testing CALEA Solutions

As a result of the FBI's inability under CALEA to dictate specific standards in these standard-setting groups, the FBI told us that some new technologies lack adequate CALEA solutions. As a result, the FBI is concentrating its efforts on working with and testing VoIP, broadband, and other packet-mode based communication providers to develop and deploy CALEA solutions for their unique technologies. To perform CALEA solution tests more efficiently, the CIU has reorganized its in-house Solutions Verification Team (Solutions Team). During the reorganization, the Solutions Team hired additional engineers and acquired new equipment that automated testing tasks. According to CIU officials, the reorganization, staff hires, and equipment purchases have allowed the CIU to conduct many more CALEA solution tests per year.

Test Subject Selection

CALEA does not require telecommunication providers, vendors, or trusted third parties to work with the FBI to ensure their networks and systems provide compliant surveillance results. Nevertheless, FBI officials told us that they have reached out to various companies that have indicated a willingness to cooperate and work with its CIU to perform CALEA solution testing. To determine which companies are willing to work with them, FBI officials maintain a list of potentially cooperative test subjects that include companies that responded to FBI or FCC surveys or contacted the AskCALEA Help Desk for wiretap assistance. In addition, officials with the Solutions Team told us they considered other variables, as shown in Table 9, when deciding whether to approach, schedule, and test the CALEA capabilities of a certain provider or vendor.

TABLE 9: ELEMENTS CONSIDERED FOR SOLUTIONS VERIFICATION TESTING

1. Test Subject footprint. Regarding providers, the FBI looks at whether the provider services a large number of subscribers. For manufacturers, the FBI focuses on whether a large number of providers use the equipment.
2. Solution availability. According to the CIU, resources are focused on technological standards where it is feasible to use a developed CALEA solution or develop a new CALEA solution.
3. Known vulnerabilities. CIU officials told us that they prioritize work with providers or manufacturers to solve CALEA compliance issues that: (1) they are aware of from their work with the standard-setting groups, and (2) have reportedly affected prior or current lawful electronic surveillance.
4. Test Subject availability. In light of the FCC's reluctance to mandate that carriers report on CALEA compliance activity, the FBI has to rely on providers or manufacturers that want or are otherwise willing to work with the FBI to develop or implement CALEA solutions.

Source: OIG analysis of Solutions Team documents

Once the FBI selects a test subject, the Solutions Team begins developing a test plan. In developing the plan, the Solutions Team reviews the technology standard against the tested feature specifications while identifying the particular surveillance need identified by law enforcement. Once drafted, the Solutions Team sends the test plan to the provider or manufacturer and once the test plan is agreed upon, the Solutions Team begins the test.

Solutions Team Test Results

From 2005 to 2007, the Solutions Team tested CALEA capabilities at 12 different providers that used emerging technologies. According to test results, the Solutions Team uncovered deficiencies in various proposed CALEA solutions. We obtained and analyzed CALEA solution problems revealed by the Solutions Team tests. Of the 50 deficiencies reviewed, we found that their impact on law enforcement could be categorized in four

different ways: (1) incomplete surveillance data; (2) inaccurate surveillance data; (3) unusable surveillance data; and (4) other miscellaneous impacts, as shown in Table 10.

TABLE 10: SUMMARY OF SOLUTIONS TEAM TESTING RESULTS

Type of Issue	Test A	Test B	Test C	Test D
Incomplete Data	10	5	7	4
Inaccurate Data	2	2	1	3
Unusable Data	2	0	1	5
Other Miscellaneous Issues	3	0	2	3
TOTAL	**17**	**7**	**11**	**15**

Source: FBI

Incomplete Surveillance Data. The CALEA solution weaknesses that had the most detrimental impact to law enforcement were those that caused incomplete surveillance data. As identified during our analysis, incomplete surveillance was caused by a variety of different issues with the CALEA solutions. For example, one test revealed that the implemented CALEA solution was not intercepting all communications, and therefore surveillance results did not contain complete information. Another test found that the solution required that the subject's modem and computer be active before the intercept could begin. In such cases, equipment needed to be active on the subject's end before the FBI could initiate a court-ordered intercept.

Inaccurate or Unusable Surveillance Data. The tests also identified CALEA solutions that could result in inaccurate or unusable information. For example, in one tested case law enforcement agencies reported receiving different data on the same target. Another test revealed that a CALEA solution resulted in hard-to-read surveillance reports.

At the conclusion of a test, the Solutions Team compiles a list of issues and sends the list to the company test subject. The company test subject and the Solutions Team then work to develop solutions to the identified problems. Once these solutions are developed, the CIU compiles a Quick Reference Guide describing the issue and its solution. These guides are posted to the AskCALEA website to assist law enforcement personnel conducting electronic surveillance in a given telecommunication environment. During our audit, we found that the FBI has developed several Quick Reference Guides that are posted to the AskCALEA website.

Conclusion

Of the nearly $4.6 million spent between January 2006 and December 2007, about $4.5 million was paid to two carriers to deploy CALEA-related solutions. The FBI also paid $96,878 to a carrier for testing CALEA solutions on its telecommunication network. We could not assess the reasonableness or cost effectiveness of these expenditures because the FBI did not base its costs on independent cost data or competing price estimates.

Our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant. We found that the FBI has revamped its testing group and enhanced its resources to help measure and facilitate CALEA compliance. In addition, the FBI has implemented an extensive testing program to ensure carrier compliance and capability with regard to emerging technologies.

At the end of the audit period, only $5,037 remained in the TCCF. According to a DOJ finance official, the FBI is working with DOJ to transfer the remaining funds to the DOJ Working Capital Fund and close the TCCF. Since the OIG is tracking residual TCCF funds by a recommendation made in a prior OIG report, this report makes no additional recommendations and is issued closed.[38]

We provided a draft of the report to the FBI for comment and review. Since the report made no recommendations, the FBI did not offer a response.

[38] 2006 OIG CALEA Implementation Report, 51 and 72.

STATEMENT ON INTERNAL CONTROLS

In planning and performing the audit of the Federal Bureau of Investigation's (FBI) Implementation of the Communications Assistance for Law Enforcement Act (CALEA), we considered aspects of the FBI's internal controls for determining our auditing procedures. A review of internal controls within the FBI was not done to provide an assurance on the propriety or adequacy of FBI internal controls as a whole.

Due to prior Office of the Inspector General recommendations regarding CALEA implementation, the FBI has implemented or updated certain procedures and internal controls. Due to these changes, including the lack of remaining funds in the Telecommunications Carrier Compliance Fund, our review did not reveal internal control weaknesses. As a result, the report makes no recommendation regarding the internal control environment within the FBI's CALEA implementation program. Since we are not expressing an opinion on the FBI's internal controls as a whole, we include this statement solely for the FBI to consider in managing its CALEA program.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We conducted this audit of the Federal Bureau of Investigation's (FBI) Implementation of the Communications Assistance for Law Enforcement Act (CALEA) in accordance with the *Government Auditing Standards*. Since compliance with laws and regulations applicable to the FBI's CALEA program is the responsibility of FBI managers, we reviewed management processes and records to obtain a reasonable assurance concerning the FBI's compliance with relevant portions of CALEA (47 U.S.C. § 1001 et. seq.), that in our judgment, would have a material effect on FBI operations if not complied with. Our audit identified no areas where the FBI did not comply with CALEA (47 U.S.C. § 1001 et. seq.).

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of the audit were to determine the type of equipment, facilities, and services brought into compliance with CALEA and whether payments during the most recent 2-year review period for CALEA-required modifications were reasonable and cost effective. In light of the TCCF rescissions that occurred in 2007, our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

This audit covered FBI CALEA-related compliance actions and TCCF payments from January 1, 2006 through December 31, 2007. We conducted fieldwork and interviewed officials at FBI Headquarters and at other FBI facilities described in the report, and selected telecommunication providers. In certain cases, we relied on computer-generated data that documented TCCF expenditure history and FBI negotiations with telecommunication carriers. To assess the reasonableness and cost effectiveness of payments made from the TCCF, we required actual cost data or competing price estimates, which the FBI did not provide. As a result, we did not offer an opinion on the reasonableness or cost effectiveness of these costs.

We reviewed CALEA annual reports, records, program plans, assessments, and associated files maintained by the FBI to obtain an overall understanding of the FBI's CALEA implementation initiative. We also reviewed supporting documentation related to all contracts, obligations, and payments for CALEA implementation activities, including documentation pertaining to carrier payment negotiations, since the last report. Since our prior audit recommended that funds remaining in the TCCF be put to a better use, we also obtained and analyzed documents pertaining to the TCCF rescissions that occurred in 2007.

APPENDIX II

PRIOR OIG AUDIT REPORTS

The OIG issued five previous audit reports on CALEA implementation and the TCCF payments under 47 U.S.C. §1001 et. seq. In March 1998, the OIG reported that the FBI and the telecommunications industry disagreed over what capabilities had to be provided for a carrier to be CALEA compliant and eligible for TCCF reimbursement.[39] At that time, the carriers had not modified any equipment pursuant to CALEA, and the FBI had made no payments to carriers.

In March 2000, the OIG reported that the FBI began negotiations with carrier and manufacturer representatives to determine the most appropriate way to arrange for carriers to meet the capability requirements.[40] The FBI also entered into RTU license agreements with a vendor (Nortel) and certain carriers to permit carriers who were using specified Nortel equipment, the use of the CALEA software solutions developed by Nortel. The FBI negotiated a price of $101.8 million for carrier purchase of these RTU software licenses, with payments made to Nortel on behalf of all carriers who used the Nortel equipment specified in the agreement.

The OIG reported in March 2002 that the FBI had paid or obligated about $400 million for carrier purchases of RTU software licenses.[41] 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 since each major carrier would require an additional $100 million in funding, capability solutions could only be deployed in about 25 percent of the switches prioritized by the FBI.

In April 2004, the OIG reported that deployment of CALEA technical solutions remained delayed and the FBI did not collect and maintain data on

[39] Department of Justice Office of the Inspector General, *Implementation of the Communications Assistance For Law Enforcement Act*, Audit Report 98-13 (March 1998).

[40] Department of Justice Office of the Inspector General, *Implementation of the Communications Assistance For Law Enforcement Act*, Audit Report 00-10 (March 2000).

[41] Department of Justice Office of the Inspector General, *Implementation of the Communications Assistance For Law Enforcement Act by the Federal Bureau of Investigation*, Audit Report 02-14 (March 2002).

carrier equipment that was CALEA-compliant.[42] Instead, the FBI estimated that carriers had activated CALEA solution software on approximately 50 percent of pre-January 1, 1995 and 90 percent of post-January 1, 1995 wireless equipment, and only 10 to 20 percent of wire line equipment. FBI personnel advised that some law enforcement agencies could not conduct proper surveillance on non-CALEA-compliant equipment, but the FBI could not demonstrate evidence of adverse impacts. The OIG concluded it was critical for the FBI to collect data on carrier compliance and the impact to law enforcement of non-compliance to determine the extent to which electronic surveillance is compromised.

Except for a one-time payment of $2.2 million, the 2004 report found that the FBI had not made any payments from TCCF funds for carriers to activate of CALEA-compliant software.[43] Furthermore, cost estimates from the FBI suggested that the current funding level of $500 million for CALEA was insufficient to activate necessary switches. In December 2003, the FBI estimated that about $204 million in additional funds might be required; however, because cost estimates for CALEA implementation varied widely, and technological change continued to occur at a rapid pace, the OIG questioned the accuracy of the FBI's estimates or whether CALEA's implementation cost could be determined with any amount of specificity.

Our most recent report, issued in March 2006, documented that the $450 million the FBI expended on RTU software licenses did not guarantee that CALEA compliant software would be operable or cover carriers' activation costs.[44] At the time of publication, the FBI was negotiating reimbursement agreements with 4 wire line carriers regarding deploying CALEA solutions on pre-1995 equipment. The 2006 report also found that CALEA has provided law enforcement agencies with beneficial electronic surveillance features, but these benefits generally have not been realized on wire line systems. However, the report revealed that the effects of delayed implementation on wire lines were mitigated by the limited number of wiretaps performed on wire lines (only 12 percent of the total as of 2005). Moreover, the report found that the growing popularity of Internet telephony and emerging technologies have undercut the usefulness of wiretaps conducted on traditional communication networks.

---

[42] 2004 OIG CALEA Implementation Report.

[43] 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 was derived from FBI Counterterrorism funds and $2.2 million came from CALEA funding.

[44] 2006 OIG CALEA Implementation Report.

APPENDIX III

ACRONYMS

Acronym	Description
BellSouth	BellSouth Corporation
CALEA	Communications Assistance for Law Enforcement Act
CIU	CALEA Implementation Unit
CRWG	Carrier Relations Working Group
DOJ	Department of Justice
ECPA	Electronic Communications Privacy Act
ESWG	Electronic Surveillance Working Group
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FISA	Foreign Intelligence Surveillance Act
Form 445	FCC Request for carrier status on CALEA compliance
Help Desk	AskCALEA Help Desk
Manufacturers	Equipment Manufacturers
Nortel	Nortel Networks Corporation
OSCU	Offsite Contract Unit
OIG	Office of the Inspector General
Qwest	Qwest Communications International, Inc.
RBOC	Regional Bell Operating Carriers
RTU	Right-To-Use
Solutions Team	Solutions Verification Team
Title III	Title III of the Omnibus Crime Control and Safe Streets Act of 1968
TCCF	Telecommunications Carrier Compliance Fund
Verizon	Verizon Communications, Inc.
VoIP	Voice over Internet Protocol