Communications Assistance for Law Enforcement Act (CALEA)

CALEA Implementation Section Federal Bureau of Investigation

Introduction

Electronic surveillance is one of the most valuable tools in law enforcement's crime fighting arsenal. In many instances, criminal activity has been either thwarted, or, if crimes have been committed, the criminals have been apprehended as a result of lawfully-authorized electronic surveillance.

The use of lawfully-authorized electronic surveillance continues to increase in importance to law enforcement as telecommunications systems become cornerstones of everyday life. Dependence on telecommunications for business and personal use has increased dramatically, computers and data services have become increasingly important to consumers, and the nation has become enthralled with mobile communications.

Three primary techniques of lawfully-authorized electronic surveillance are available to law enforcement: pen registers, trap and trace devices, and content interceptions. Pen registers and trap and trace devices, which account for the vast majority of lawfully-authorized surveillance attempts, record/decode various types of dialing and signaling information utilized in processing and routing the communication, such as the signals that identify the numbers dialed (i.e., outgoing) or the originating (i.e., incoming) number of a telephone communication. A third and more comprehensive form of lawfully- authorized electronic surveillance includes not only the acquisition of call- identifying, or dialed number information, but also the interception of communications content.

Although lawfully-authorized electronic surveillance is crucial to effective law enforcement, it is used sparingly. This is particularly true with respect to the interception of communications content. The federal government, District of Columbia, Virgin Islands, and forty-five states allow the use of this technique, but only in the investigation of felony offenses, such as kidnapping, extortion, murder, illegal drug trafficking, organized crime, terrorism, and national security matters, and only when other investigative techniques, either can not provide the needed information or would be too dangerous.

Legal Origins of Electronic Surveillance

Passage of the Communications Assistance for Law Enforcement Act (CALEA) 1994 Pub. L. No. 103-414, 108 Stat. 4279, was not without precedent; it was a logical and necessary development of the nation's electronic surveillance laws.

The modern legal framework for electronic surveillance arises out of the Supreme Court's landmark decision in *Katz v. United States,* 389 U.S. 347 (1967). Prior to *Katz*, the Supreme Court had regarded wiretapping as outside the scope of the Fourth Amendment's restrictions on unreasonable searches and seizures. *See Olmstead v. United States,* 277 U.S. 438 (1928). In *Katz*, however, the Supreme Court reversed its prior position and held for the first time that Fourth Amendment protections do apply to government interception of telephone conversations.

A year after the *Katz* decision, and after a failed attempt to address wiretapping through amendments to the Communications Act of 1934, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968. Section 605 of the Communications Act of 1934 was amended to provide that "no person not being authorized by the sender shall intercept any communication and divulge or publish [its] existence, contents . . . or meaning." By 1968, the provisions of the Act dealing with wiretapping had become so muddled by inconsistent interpretations of federal and state courts that Congress intervened. *See* Pub. L. No. 90-351, 82 Stat. 212.

Title III of the Omnibus Act created the foundation for communications privacy and electronic surveillance law. The Omnibus Act not only established a judicial process by which law enforcement officials could obtain lawful authorization to conduct electronic surveillance, but also prohibited the use of electronic surveillance by private individuals. A subsequent amendment to Title III also required telecommunications carriers to "furnish [law enforcement] . . . all information, facilities, and technical assistance necessary to accomplish [an] interception." 18 U.S.C. § 2518[4].

In response to continued advances in telecommunications technology, Congress expanded the protections of Title III by enacting the Electronic Communications Privacy Act (ECPA) 1986 Pub. L. No. 99-508, 100 Stat. 1848. Among the ECPA amendments to Title III were requirements that: (1) interceptions be conducted unobtrusively and with a minimum of interference with the services of the person whose communications are being intercepted; and (2) the interception be conducted in such a way as to minimize access to communications not otherwise authorized to be intercepted. ECPA also expanded electronic surveillance authority to include telecommunications technologies and services such as electronic mail, cellular telephones, and paging devices.

Following the enactment of ECPA, advancements in telecommunications technology continued to challenge and, in some cases, thwart law enforcement's electronic surveillance capability. What was once a simple matter of attaching wires to terminal posts now either required expert assistance from telecommunications service providers or was impossible altogether.

Although Title III required telecommunications carriers to provide "any assistance necessary to accomplish an electronic interception," 18.U.S.C. § 2518[4], the question of whether telecommunications carriers had an obligation to design their networks such that they did not impede a lawfully- authorized interception had not been decided.

In October 1994, at the request of the nation's law enforcement community, Congress responded to this dilemma by enacting CALEA, which clarified the scope of a carrier's duty in effecting lawfully-authorized electronic surveillance.

Communications Assistance for Law Enforcement Act

Although telecommunications carriers have been required, since 1970, to cooperate with law enforcement personnel in conducting lawfully-authorized electronic surveillance, CALEA for the first time requires telecommunications carriers to modify the design of their equipment, facilities, and services to ensure that lawfully-authorized electronic surveillance can actually be performed. CALEA also imposes certain responsibilities on the Attorney General of the United States, the Federal Communications Commission (FCC), telecommunications equipment manufacturers, and telecommunications support services providers. A brief description of the roles and responsibilities of each is provided below.

A. Attorney General of the United States

Congress assigned the Attorney General of the United States a key role in the implementation of CALEA, the most important being that of chief integrator and spokesperson for the law enforcement community. The responsibilities of the Attorney General include, but are not limited to:

* Consulting with industry associations, standard-setting organizations, representatives of users, and state utility commissions to facilitate implementation of the assistance capability requirements;

Providing telecommunications carriers, telecommunications industry associations, and standard-setting organizations with an estimate of the number of interceptions, pen registers, and trap and trace devices that government agencies may conduct;

* Establishing regulations to facilitate timely and cost-efficient reimbursement to telecommunications carriers as authorized under CALEA;

* Allocating funds appropriated for reimbursement in a manner consistent with law enforcement priorities; and

Reporting to Congress, annually, the total amount of payments made to telecommunications carriers during the preceding year, and the projected expenditures for the current year.

B. Federal Bureau of Investigation

On February 24, 1995, the Attorney General delegated management and administrative responsibilities for CALEA to the Federal Bureau of Investigation (FBI) 28 C.F.R. § 0.85 (1995). The FBI, in turn, created the CALEA Implementation Section (CIS), which works with the telecommunications industry and the law enforcement community to facilitate effective and industry-wide implementation of CALEA.

C. Federal Communications Commission

Consistent with the FCC's duty to regulate the use of wire and radio communications, Congress assigned specific CALEA responsibilities to the FCC. These include, but are not limited to:

Determining which entities should be considered telecommunications carriers for purposes of CALEA;

Establishing systems security and integrity regulations for carrier administration of interceptions;

Establishing technical requirements or standards for compliance with the assistance capability requirements of CALEA if industry associations or standard-setting organizations fail to issue technical requirements, or if a government agency or any other person believes that industry-adopted standards are deficient;

Reviewing reasonably achievable petitions regarding compliance with the assistance capability requirements; and

Reviewing petitions for extension of the capability compliance date.

CALEA also amends the Communications Act of 1934 to provide that the FCC "shall prescribe such rules as are necessary to implement [CALEA]" 47 U.S.C. § 229.

D. Telecommunications Carriers

Telecommunications carriers must ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the following assistance capability requirements:

Expeditious isolation and interception of communications content;

Expeditious isolation and access to call-identifying information;

Delivery of communications content and call-identifying information; and

Unobtrusive interception and access to call-identifying information and protection of the privacy and security of communications not authorized to be intercepted.

E. Equipment Manufacturers and Support Service Providers

Congress also recognized that without the assistance of manufacturers of telecommunications equipment and support service providers, carriers would be unable to comply with CALEA. To that end, it imposed an affirmative duty on manufacturers of telecommunications equipment and support service providers to make available all features or modifications necessary to meet the assistance capability requirements of CALEA.

Legal Provisions of CALEA

The CALEA statute consists of the following main sections:

A. Section 102

Section 102 defines key terms and phrases, such as call-identifying information, information services, and telecommunications carrier. Of the terms defined in section 102, telecommunications carrier required further clarification by the FCC. Specifically, the FCC addressed whether certain telecommunications carriers are subject to CALEA's assistance capability requirements.

CALEA requires that all telecommunications carriers' equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of meeting specific assistance capability requirements. The Act defines such carriers as:

1. person[s] or entit[ies] engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

2. includes-

a. person[s] or entit[ies] engaged in providing commercial mobile service (as defined in 47 U.S.C.§ 332(d)); or

b. person[s] or entit[ies] engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title; but

3. does not include-

a. persons or entities insofar as they are engaged in providing information services; and

b. any class or category of telecommunications carriers that the FCC exempts by rule after consultation with the Attorney General.

On August 31, 1999, the FCC released a Report and Order clarifying which entities and services are subject to the assistance capability requirements of CALEA. The following list provides illustrative examples of the *types* of entities determined by the FCC to be telecommunications carriers for purposes of CALEA:

* All entities previously classified as common carriers;

* Cable operators and electric or other utilities to the extent that they offer telecommunications services for hire to the public;

* Commercial mobile radio service (CMRS) providers, including industrial and business radio services licensees, specialized mobile radio (SMR) providers, 220 megahertz (MHZZ) service licensees, to the extent that such services consist of interconnected services offered to the public;

* Resellers, to the extent that they actually own facilities; and

* Entities that provide calling features, such as call forwarding, call waiting, three-way calling, and speed dialing.

Private mobile radio service (PMRS) operators and pay telephone providers were excluded from the list of carriers subject to CALEA. However, if a PMRS operator uses its facilities to offer interconnected service for profit to the public, or to a substantial portion of the public, that service qualifies as CMRS, and is therefore subject to CALEA.

The FCC also clarified that where facilities are used solely to provide an information service (IS), whether offered by an exclusive-IS provider or by a common carrier that has established a dedicated IS system apart from its telecommunications system, such facilities *are not* subject to CALEA. These include messaging and on-line services such as Prodigy and America OnlLine. By contrast, facilities used to provide both telecommunications and information services (i.e., joint-use facilities) are subject to CALEA in order to ensure law enforcement's ability to access the telecommunications services portion of joint-use facilities.

B. Section 103

Section 103 of CALEA establishes four assistance capability requirements that telecommunications carriers are required to meet in connection with services or facilities, that provide customers the ability to originate, terminate, or direct communications. They are:

1. Interception of Communications Content

Telecommunications carriers must ensure that they are capable of expeditiously isolating, and enabling the government to intercept pursuant to appropriate legal authorization, all wire and electronic communications to or from a particular subscriber within that carrier's network.

2. Access to Call-identifying Information

Telecommunications carriers must ensure that they are capable of expeditiously isolating, and enabling the government to access pursuant to appropriate legal authorization, all call-identifying information reasonably available to the carrier. Such information, however, if acquired solely through pen registers or trap and trace devices, does not include information that may disclose the physical location of the subscriber, except to the extent that location can be determined by the telephone number.

Section 102 of CALEA defines call-identifying information as ". . . dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."

3. Delivery of Communications Content and Call-identifying Information

Telecommunications carriers must ensure that they are capable of delivering intercepted communications and call-identifying information to a location specified by the government, other than the carrier's premises. The information must be made available to the government in a format that can be transmitted over communications channels and either translated or converted into useable form.

4. Protection of Privacy and Security of Communications

Telecommunications carriers must ensure that they are capable of conducting interceptions and providing access to call-identifying information unobtrusively. Carriers must also protect the privacy and security of communications and call-identifying information not authorized to be intercepted, as well as information about the government's interception of call content and access to call-identifying information. The requirement that interceptions be conducted in a manner that will minimize the interception of unauthorized communications was intended to avoid improper intrusion on rights of privacy.

C. Section 104

Section 104 of CALEA requires the Attorney General to provide notice of the actual and maximum "number of communications interceptions, pen registers, and trap and trace devices . . . that the Attorney General estimates" government agencies may "conduct and use simultaneously." Section 104 also requires that the Attorney General publish in the *Federal Register* the capacity notices "after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment." In addition, section 104 mandates that the Attorney General publish capacity notices after notice and comment.

Section 104 consists of five subsections:

1. Notice of Actual and Maximum Capacity

The FBI began the process of implementing section 104 by publishing on October 16, 1995, the Initial Notice of Capacity in the *Federal Register*. Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Rreg. 53, 643 (Oct. 16, 1995). (to be codified at 28 C.F.R. pt. 100) On January 14, 1997, the Second Notice of Capacity was published. Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 620 Fed. Rreg. 190253, 643 (Jan. 14, 1997). A Final Notice of Capacity was published on March 12, 1998. Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 630 Fed. Reg. 53, 643 (Mar. 12, 1998).

The Final Notice of Capacity adopted capacity requirements for telecommunications services that law enforcement viewed as its highest priorities in implementing lawfully-authorized electronic surveillance: wireline local exchange service, cellular service, and broadband PCS. Capacity requirements for wireline local exchange service providers are based on the geographic boundaries of a county, whereas the capacity requirements for cellular and broadband PCS providers is based on established market service areas as defined by licenses granted by the FCC.

The Final Notice of Capacity provided that telecommunications services other than wireline local exchange service, cellular, and broadband PCS would be addressed in future notices of capacity. As a continuation of the capacity process, the FBI issued a Notice of Inquiry, which gave interested parties an opportunity to provide input to the FBI as it develops law enforcement's capacity requirements for services other than wirelinewireline local exchange, cellular, and broadband PCS. A Further Notice of Inquiry was published to narrow the scope of the second phase to capacity requirements for paging, mobile satellite services, and specialized and enhanced specialized mobile radio.

2. Compliance

Subsection (b) of section 104 addresses carrier compliance with published capacity notices. It requires that telecommunications carriers ensure, within three years after publication of the notices or within four years of enactment, whichever is greater, that their systems are equipped with sufficient "actual" capacity and capable of "expeditiously" expanding to accommodate any necessary increases. Based on the publication date of the Final Notice of Capacity, telecommunications carriers hadve until March 12, 2001, to comply with the requirements. Because capacity requirements for telecommunications carriers other

than wirelinewireline local exchange, cellular, and broadband PCS have not been published, a compliance date has not been established.

3. Notice of Increased Maximum Capacity Requirements

Section 104(c) states that notices of increased maximum capacity are to be published in the *Federal Register* by the Attorney General. Similar to the actual and maximum capacity requirements, carriers have three years after the notice has been published to comply with the requirements. However, the Attorney General may specify a longer compliance period.

4. Carrier Statements

Within 180 days after the publication of the Final Notice of Capacity, section 104(d) requires that a telecommunications carrier submit a statement identifying all systems or services incapable of meeting the published capacity requirements. Telecommunications carriers had until September 8, 1998, to submit their carrier statement. The information obtained from the carrier statements will be used, in conjunction with law enforcement priorities and other factors, to determine which carriers may be eligible for capacity-related reimbursement.

5. Reimbursement

Section 104(e) provides a capacity "safe harbor" for telecommunications carriers who meet the following requirements. First, the carrier must have submitted a carrier statement pursuant to section 104(d). The Attorney General may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for costs directly associated with modifications to attain the capacity requirements, and the cost must be reasonable under section 109(e).

D. Section 105

Section 105 of CALEA seeks to ensure systems security and integrity by requiring that a "telecommunications carrier ensure any interceptions of communications or access to call-identifying information . . . can be activated only in accordance with a court order or other lawful authorization and . . . in accordance with the regulations prescribed by the Commission." 47 U.S.C. CALEA§ 1004.105 short cite 12.12.9

On March 15, 1999, the FCC published a Report and Order, which promulgated systems security and integrity regulations that carriers must follow to comply with section 105 of CALEA. Implementation of the Communications Assistance for Law Enforcement Act, 64 Fed. Reg. 14,83451; 462 (Mar. 295 1999). (codified at 47 C.F.R. pt. 64) Specifically, the FCC addressed policies and procedures for employee supervision and control, record keeping requirements, the submission and review of carrier policies and procedures, and penalties for violation of carrier policies and Commission rules.

E. Section 106

Section 106 requires that telecommunications carriers consult with equipment manufacturers and support services providers to ensure that their equipment, facilities, or services comply with CALEA's assistance capability requirements. Congress, by including section 106, recognized that manufacturers and support service providers play a critical role in the conduct of lawful electronic surveillance, and without their assistance, carriers would be unable to comply.

Accordingly, manufacturers and support service providers are required to make available all features or modifications necessary to meet CALEA's assistance capability requirements. In return, manufacturers and support services providers are to be paid a reasonable fee by carriers in accordance with normally

accepted business practices. Manufacturers or support service providers that fail to provide customers with necessary modifications may be subject to civil penalties under section 108 of CALEA.

F. Section 107

Section 107 of CALEA grants safe harbor to equipment manufacturers, telecommunications carriers, and support service providers that are in compliance with publicly available technical requirements or standards adopted by an industry association, standard-setting organization, or the FCC. Compliance with industry standards is voluntary; a carrier may, at its discretion, adopt other solutions for complying with the assistance capability requirements of section 103.

Section 107 also requires that the Attorney General consult with appropriate industry representatives and standards-setting organizations in developing CALEA requirements or technical standards. However, CALEA prohibits law enforcement from requiring that telecommunications carriers adopt a *specific* design or system configuration.

If industry associations or standard-setting organizations fail to adopt a technical standard, or if a government agency or any other person believes that industry-adopted standards are deficient as a means of meeting the assistance capability requirements of section 103, that party may petition the FCC to establish technical requirements or standards by rule. However, the FCC cannot make standards determinations or confer safe harbor if a deficiency petition has not been properly presented. Technical standards or requirements established by the FCC must:

* Meet the assistance capability requirements of section 103 by cost- effective methods;

* Protect the privacy and security of communications not authorized to be intercepted;

* Minimize the cost of such compliance on residential ratepayers;

* Serve the policy of the United States to encourage the provision of new technologies and services to the public; and

* Provide a reasonable time and conditions for compliance with the transition to any new standard, including defining the obligations of telecommunications carriers during the transition period.

1. Development of an Industry Standard

In early 1995, an ad hoc group, sponsored by the Telecommunications Industry Association (TIA) Subcommittee TR45.2, began working to develop an industry standard that would satisfy the assistance capability requirements of CALEA for wire linewireline local exchange, cellular, and broadband PCS services. This effort included participation by industry and law enforcement.

A proposed industry standard was released for ballot in February, 1997. On December 5, 1997, TIA and Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), announced the adoption and joint publication of an official interim industry technical standard, J-STD-025.

J-STD-025 defines the services and features necessary to support lawfully authorized electronic surveillance and the interfaces used to deliver intercepted communications and call-identifying information to law enforcement. Although the interim technical standard was received favorably by industry, it was met with disfavor by both law enforcement and privacy organizations. Law enforcement argued that the interim standard was under- inclusive and failed to satisfy CALEA requirements because it did not include nine specific capabilities. The following table contains brief descriptions of these nine capabilities.

Name	Description
Content of subject-initiated conference calls	Capability that would enable law enforcement to access the content of conference calls supported by the subject's service.
Party Hold, Party Join, Party Drop	Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a multi-leg call, whether a party is on hold, has joined, or has been dropped from the call.
Access to subject-initiated dialing and signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook and other feature keys).
In-band and out- of-band signaling (Notification Message)	A message would be sent to law enforcement when a subject's *service* sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or busy.
Timing to associate call data to content	Information necessary to correlate call identifying information with the call content of a communications interception.
Post-cut-through dialed digits (dialed digit extraction)	Extraction and delivery on a call data channel of call-routing digits dialed by a subject after the initial call setup is completed.
Surveillance Status Message	Message that would provide the verification that an interception is still functioning on the appropriate subject.
Continuity check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed or lost continuity.
Feature Status Message	Message that would provide affirmative notification of any change in a subject's subscribed-to features.

By contrast, privacy organizations, such as the Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), and American Civil Liberties Union (ACLU), argued that the interim technical standard was over-inclusive because it included access to information that identified the location of an intercept subject and failed to protect the privacy of packet-switched communications. CDT also argued that the additional capabilities sought by law enforcement were not required under CALEA and would further render the industry standard deficient.

By April 1998, the FCC had received four official petitions requesting that it establish, by rule, technical requirements and standards for CALEA compliance. The FCC responded, launching what would become a protracted debate, by issuing a public notice and soliciting comments on the petitions.

On August 31, 1999, the FCC issued a Third Report and Order, adopting technical requirements for wirelinewireline local exchange, cellular, and broadband PCS services. Communications Assistance for Law Enforcement Act 64 Fed. Reg. 51, 710 (Sept. 24Aug. 31, 1999). (codified at 47 C.F.R. pts. 22, 24, 64 In remanding the interim standard to the TR45.2 subcommittee for modification, the FCC ruled that telecommunications carriers will be required to implement all of the capabilities included in J-STD-025 (the interim technical standard), plus six of nine missing capabilities requested by law enforcement. The subcommittee was allowed seven months, or until March 30, 2000, to complete necessary changes to J-STD-025, in accordance with the FCC ruling. The six missing capabilities determined by the FCC to be

required by CALEA include: content of subject-initiated conference calls; party-hold, party-join, and party-drop messages; access to subject initiated dialing and signaling; in band and out-of-band signaling; timing; and post-cut-through dialed digits. The FCC further ruled that while CALEA did not require carriers to provide the remaining three missing capabilities, carriers may offer the capabilities to law enforcement at their discretion.

The FCC did not modify the technical requirements of J-STD-025 for packet-mode communications. Instead, it permits packet-mode data to be delivered to law enforcement in accordance with the interim technical standard, pending further study of packet-mode communications by the telecommunications industry.

On November 16, 1999, members of the telecommunications industry filed suit in the United States Court of Appeals challenging certain elements of the FCC's Third Report and Order. *United States Telecom Ass'n v. F.C.C.*, 227 F.3d 450 (D.C. Cir. 2000). On August 15, 2000, the United States Court of Appeals rendered a decision regarding the FCC's Third Report and Order. The Court vacated a portion of the FCC's order, and remanded the following capabilities to be reassessed by the FCC on the grounds that the FCC did not adequately substantiate its conclusions: (1) party-hold, party-join, and party-drop messages; (2) access to subject initiated dialing and signaling; (3) in-band and out-of-band signaling; and (4) post-cut-through dialed digits. The Court upheld the FCC's conclusions regarding location information and packet-mode communications.

2. Compliance Extensions

Section 107 also authorizes the FCC to extend the date for compliance with the assistance capability requirements of section 103. In a Memorandum Opinion and Order, released on September 11, 1998 (CC docket No.97-213, FCC 98-233), the FCC exercised this authority by extending the deadline for compliance from October 25, 1998, to June 30, 2000. Communications Assistance for Law Enforcement Act, 63 Fed.Reg. 63, 639 (Sept. 11, 1998) (codified at 47 C.F.R. pt. 64)

The FCC, in its Third Report and Order, established a separate compliance deadline for implementation of the six missing capabilities. WirelineWireline local exchange, cellular, and broadband PCS carriers will be required to make the six punch list capabilities available to law enforcement by September 30, 2001.

G. Section 108

Section 108 establishes conditions for the issuance of an enforcement order directing a carrier, a provider of support services, or a manufacturer of telecommunications equipment to comply with CALEA, including compliance requirements and limitations on the scope of an enforcement order.

1. Issuance of an Enforcement Order

Section 108(a) establishes conditions for which a court may issue an enforcement order under 18 U.S.C. § 2522. First, a court must find that alternative technologies, capabilities, or facilities are not reasonably available to law enforcement, and that compliance is or would have been reasonably achievable had timely action been taken by a carrier, a provider of support services, or a manufacturer. A court may impose a civil penalty of up to $10,000 per day against a carrier, a provider of support services, or a manufacturer for each day in violation.

2. Compliance with an Enforcement Order

Under section 108(b), a court shall specify a reasonable time period for compliance considering the good faith efforts of the violating entity to comply, the effect upon the entity's ability to continue to conduct business, the entity's degree of culpability, and other matters as justice may require.

3. Limitations of an Enforcement Order Directing a Carrier

Section 108(c), imposes three limitations on the scope of an enforcement order. First, an enforcement order may not require a carrier to comply with a surveillance request that requires the use of capacity for which the Attorney General has not agreed to reimburse the carrier. Second, an enforcement order may not require a carrier to comply with a capability requirement that the FCC has determined is not "reasonably achievable," unless the Attorney General has agreed to reimburse the carrier for necessary modifications. Third, no enforcement order can require a carrier to modify its equipment, facilities, or services, installed before January 1, 1995, unless the Attorney General has agreed to pay all reasonable costs of the modification or there has been a significant upgrade.

H. Section 109

Section 109 establishes reimbursement guidelines for two categories of equipment, facilities, and services:

1. Equipment, Facilities, and Services Installed or Deployed on or Before January 1, 1995

Under section 109(a), the Attorney General is authorized to pay all reasonable costs directly associated with modifications to equipment, facilities, and services installed or deployed on or before January 1, 1995, to achieve the assistance capability requirements of section 103.

If the Attorney General elects not to reimburse a carrier for modifications, such equipment, facilities, and services are deemed to be in compliance with CALEA and are not subject to enforcement under section 108. If, however, the carrier subsequently replaces, significantly upgrades, or modifies the equipment, the grant of compliance will be rescinded, and the carrier required to comply with provisions governing equipment, facilities, and services installed or deployed after January 1, 1995.

2. Equipment, Facilities, and Services Installed or Deployed after January 1, 1995

The Attorney General is authorized to reimburse telecommunications carriers for modifications to equipment, facilities, and services installed or deployed after January 1, 1995, only if the FCC determines that compliance is not "reasonably achievable." Whether compliance is "reasonably achievable" depends on a number of factors spelled out in section 109(b), including whether compliance would "impose significant difficulty or expense on the carrier or on . . . users of the carrier's systems."

If the FCC determines that compliance is not reasonably achievable, the Attorney General may either reimburse the carrier for all costs in excess of what the FCC finds to be reasonable or consider the carrier to be in compliance with the assistance capability requirements of section 103.

3. Cost Recovery Regulations

Section 109 also requires that the Attorney General, after notice and comment, establish regulations to facilitate carrier reimbursement as authorized under CALEA, including reimbursement under 18 U.S.C. § 2518(4), 18 U.S.C. § 3124, and 50 U.S.C. § 1802 (the Foreign Intelligence Surveillance Act). The Attorney General satisfied this obligation with the publication of the CALEA Cost Recovery Regulations on March 20, 1997. Implementation of Section 109 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 13, 307 (March 20, 1997) (codified at 28 C.F.R. Part§ 100). The published rules establish standard recovery procedures for carriers seeking reimbursement under section 109.

4. Nationwide Right-to-Use Licenses

The FBI has implemented a reimbursement strategy that allows telecommunications carriers to receive CALEA software at no charge for certain high priority switching platforms. Under nationwide right-to-use (RTU) license agreements, the FBI pays for the development of CALEA software solutions for high priority switching platforms. This allows telecommunications carriers to receive CALEA software at a nominal charge for equipment, facilities, or services installed or deployed now and in the future.

I. Section 110

When CALEA was enacted into law in 1994, Congress *authorized* $500 million to be appropriated to reimburse the telecommunications industry for certain eligible costs associated with modifications to their networks. This dollar amount was authorized to remain available until expended. CALEA was subsequently amended by The Omnibus Consolidated Appropriations Act of 1997, which created the Telecommunications Carrier Compliance Fund (TCCF) and appropriated $60 million in initial CALEA funding. The purpose of the TCCF is to facilitate the disbursement of funds available for CALEA implementation. Additionally, the Act authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF, subject to applicable Congressional reprogramming requirements.

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

TELECOMMUNICATIONS CARRIER COMPLIANCE FUND ACTIVITY	
Activity	**Amount**
FY 1997 Direct Appropriations	$60,000,000
FY 1997 Department of Justice Working Capital Fund	$40,000,000
FY 1997 United States Postal Inspection Service Transfer	$1,000,000
FY 1997 United States Customs Service Transfer	$1,580,270
FY 2000 Direct Appropriations	$15,000,000
FY 2000 Supplemental Appropriations	$181,000,000
FY 2001 Direct Appropriations	$200,977,000
TOTAL DEPOSITS	$499,557,270

J.Section 111

Section 111 establishes the effective date for compliance with provisions of Section 103 and 105. These deadlines have since been revised by the FCC to accommodate industry promulgation of a technical standard and the development of technical solutions.

K. Section 112

Section 112 ensures that both congressional and public oversight of CALEA is maintained by requiring the submission of reports by the Attorney General. This section also specifies reporting requirements for the Comptroller General that includes describing the type of equipment, facilities, and services that have been brought into compliance and reflecting the cost effectiveness of the payments made by the Attorney General.

Further Information

As stated previously, the CALEA Implementation Section (CIS) of the FBI has been delegated implementation responsibilities and represents the interests of the law enforcement community in matters pertaining to CALEA. CIS has established a website, www.askcalea.net, in order to disseminate implementation details and provide an avenue for requesting additional information.

ABOUT THE AUTHOR

CALEA Implementation Section (CIS) was established in 1995 in response to the delegation of implementation responsibilities to the Federal Bureau of Investigation (FBI) by the Attorney General. CIS spearheads CALEA implementation efforts by fulfilling the responsibilities assigned to the Attorney General through consultation with the telecommunications industry and privacy advocates. CIS represents the interests of the entire law enforcement community before Congress, other government agencies involved in the implementation of CALEA, and the telecommunications industry. CIS is headed by Section Chief, Supervisory Special Agent Michael P. Clifford, a 21 year veteran of the FBI. CIS maintains a website, www.askCALEA.net, where more information is available and specific questions can be submitted regarding CALEA implementation activities.