CIS' CALEA Website - www.AskCALEA.net

CIS has developed an Internet Website in order to foster a more productive information-sharing portal. The Website offers recent CALEA implementation updates as well as the following:

- The current status of Congressional appropriations and CALEA reimbursement funds,
- Implementation documents issued by CIS and the Federal Communications Commission,
- A description of the CIS organization and implementation programs underway at CIS, and
- Legislation granting Law Enforcement the authority to conduct electronic surveillance.

Visitors to the Website can also ask questions of the CIS staff and subscribe to the AskCALEA News e-mail newsletter. Members of the law enforcement community can join a secure on-line forum.

Come visit us at www.AskCALEA.net

How to contact CIS

CALEA Implementation Section
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151-0450
800-551-0336
www.AskCALEA.net

U.S. Department of Justice
Federal Bureau of Investigation

Communications Assistance for Law Enforcement Act (CALEA)

CALEA Implementation Section
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151-0450
800-551-0336
www.AskCALEA.net

Introduction

The purpose of this *Communications Assistance for Law Enforcement Act (CALEA)* guide is to provide a brief summary of the importance of lawfully-authorized electronic surveillance to the law enforcement community and describe some of the electronic surveillance techniques in use today. In addition, this guide provides a historical perspective as to the need for CALEA and describes the efforts of the CALEA Implementation Section (CIS) to fulfill the legislative responsibilities of the Attorney General.

Importance of Electronic Surveillance

Electronic surveillance is one of the most valuable tools in law enforcement's crime fighting arsenal. In many instances, criminal activity has either been thwarted, or if crimes have been committed, the criminals have been apprehended as a result of lawfully-authorized electronic surveillance. Electronic surveillance is strictly and carefully regulated by federal statute. Courts only authorize interceptions after an exhaustive demonstration of need by law enforcement.

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.

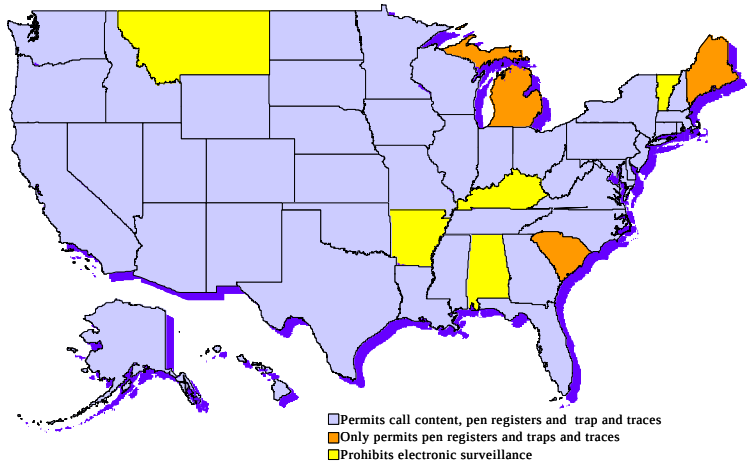
Types of Electronic Surveillance

Three primary techniques of lawfully-authorized electronic surveillance are available to law enforcement: pen registers, trap and trace devices, and content interceptions. The first two, pen registers and trap and trace devices, which account for the vast majority of lawfully-authorized electronic surveillances, 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. The 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 electronic surveillance is crucial to effective law enforcement, it is used sparingly. The federal government, District of Columbia, Guam, Puerto Rico, Virgin Islands, and 42 states allow its use, but only in the investigation of felony offenses, such as kidnaping, 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.

In addition to the 42 states that allow the three forms of electronic surveillance discussed above, three states (Maine, Michigan, and South Carolina) permit the use of pen registers and trap and trace devices for the surveillance of call-identifying information. The five remaining states (Alabama, Arkansas, Kentucky, Montana, and Vermont) do not permit any of the three forms of electronic surveillance discussed above. However, federal law enforcement agencies have the authority to conduct electronic surveillance throughout the entire country.



What Is CALEA?

> The purpose of [CALEA] is to preserve the Government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.
>
> To [e]nsure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability to: (1) isolate expeditiously the content of targeted communications transmitted by the carrier within the carrier's service area; (2) isolate expeditiously information identifying the origin and destination of targeted communications; (3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications.
>
> *H. Rep. No. 103-827, 103d Cong., 2d Sess. 9 (1994).*

Why Was CALEA Passed?

Passage of the Communications Assistance for Law Enforcement Act was a logical and necessary development of our Nation's electronic surveillance laws — originating in the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III formed the foundation

for communications privacy and law enforcement's electronic surveillance authority. In response to continued advances in telecommunications technology, Congress passed the Electronic Communications Privacy Act (ECPA) of 1986, which confirmed law enforcement's electronic surveillance authority to include emerging technologies and services such as electronic mail, cellular telephones, and paging devices.

Following enactment of the 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 requires expert assistance from telecommunications service providers. Examples of technological changes that impeded law enforcement's efforts to conduct lawfully-authorized electronic surveillance include:

- New, switch-based features and services (e.g., call forwarding, call transfer, one number service, follow-me service),
- Conversion from analog to digital transmission modes between the subscriber and carrier,
- Cellular, Personal Communications Services (PCS), and other non-wireline technologies that do not allow law enforcement access through a local loop.

Although Title III required telecommunications carriers to provide "any assistance necessary to accomplish an electronic interception," the question of whether companies had an obligation to *design* their networks such that they did not impede a lawfully authorized interception had not been decided.

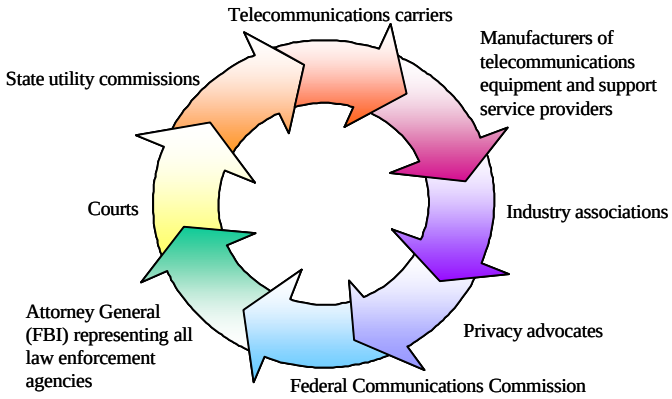
In October 1994, at the request of the nation's law enforcement community, Congress responded to this dilemma by enacting CALEA, which clarifies the scope of a carrier's duty in effecting court-approved electronic surveillance.

CALEA At A Glance - Implementation Developments

Section		CIS	Industry	FCC	Other
102	Definitions	• Provided input to the FCC	• Provided input to the FCC	• **Second Report &Order** - Definition of a telecommunications carrier	
104	Notices of Capacity Requirements	• **Final Notice of Capacity** for local exchange services, cellular, and broadband PCS • Notice of Inquiry and **Further Notice of Inquiry** for other technologies	• Provided input to the CIS • Submitted carrier statements • Challenged Final Notice of Capacity in Court		• Industry associations challenged the Final Notice of Capacity in Court
105	Systems Security and Integrity (SS&I)	• Provided input to the FCC	• Provided input to the FCC	• **Memorandum Opinion and Order** outlining carriers' SS&I responsibilities	
106	Cooperation of Equipment Manufacturers and Providers of Telecommunications Support Services	• Consulted with individual manufacturers and providers of support services in their development of solution(s)	• Solution developed by switch manufacturers and peripheral equipment providers		
107	Technical Requirements and Standards; Extension of Compliance Date	• Consulted with the industry in the development of J-STD-025 • Filed deficiency petition with FCC • Provided input to the FCC • Adopted **Flexible Deployment** Initiative	• **J-STD-025** for local exchange, cellular and broadband PCS • Requested extension of 10/25/98 compliance date	• **Third Report & Order** determining required capabilities • Granted extension of 10/25/98 date until 6/30/00 • Granting additional extensions in conjunction with Flexible Deployment	• Privacy Groups filed petition of deficiency with FCC
109	Payment of Costs of Telecommunications Carriers to Comply with Capability Requirements	• **Cost Recovery Regulations** with definition of "installed or deployed" • Reimbursed industry for a number of technical solutions	• Provided input to the CIS • Challenged Cost Recovery Rules in Court		• Industry associations challenged the Final Notice of Capacity in Court
110	Authorization of Appropriations				• To date, Congress has appropriated $499 million
112	Reports	• Submitted six **Annual Reports to Congress**			

Implementation of CALEA

The implementation of CALEA requires the active participation and cooperation of a variety of parties. In addition to the law enforcement community, there are a significant number of stakeholders and influential players that need to work together to ensure that the introduction of sophisticated telecommunications technologies into the nation's networks does not erode law enforcement's ability to conduct lawfully-authorized electronic surveillance. Telecommunications carriers; manufacturers of telecommunications equipment and providers of support services; industry associations; privacy advocates; the Federal Communications Commission and state utility commissions; the Courts, and the law enforcement community all play a critical role in the implementation of CALEA.



What Is CIS

CIS is a Section within the FBI's Laboratory Division. The Laboratory Division is that part of the FBI that has, as part if its organizational mission, the obligation to ". . . provide effective collection, surveillance, and tactical communications systems to support investigative and intelligence priorities." The inclusion of CALEA implementation

responsibilities into this part of the FBI allows CIS to draw upon the extensive telecommunications knowledge and electronic surveillance experience of the FBI.

Why Was CIS Created

CIS was established in response to the delegation of CALEA implementation responsibilities to the FBI by the Attorney General.

Responsibilities and Authority

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, the Federal Communications Commission, and other government agencies involved in the implementation of CALEA, and the telecommunications industry.

CIS views the "implementation of CALEA" to mean all explicit and implicit mandates and responsibilities contained within the legislation. These responsibilities apply to *all* telecommunications technologies and services that are mandated to comply with the requirements of CALEA.

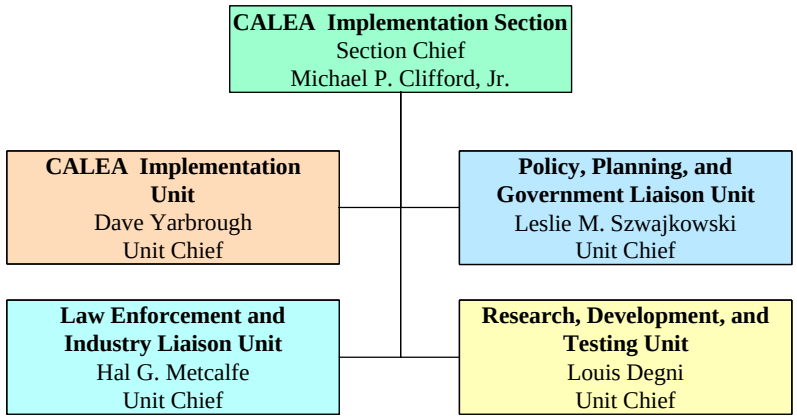
To date, CIS has made significant implementation progress with traditional wireline local exchange, cellular, and broadband PCS services as evidenced by the availability of technical solutions for a majority of equipment currently in use by carriers providing those services.

Other telecommunications technologies and services that CIS is currently pursuing implementation include Specialized Mobile Radio and Enhanced Specialized Mobile Radio; traditional, two-way paging, and ancillary paging services; mobile satellite services; and internet protocol-based telecommunications.

Organizational Structure

CIS is composed of four Units responsible for the technical; research and development; regulatory; policy; reimbursement; and liaison functions critical to the successful implementation of the legislation. CIS is headed by Section Chief, Supervisory Special Agent Michael P. Clifford, a 21 year veteran of the FBI.

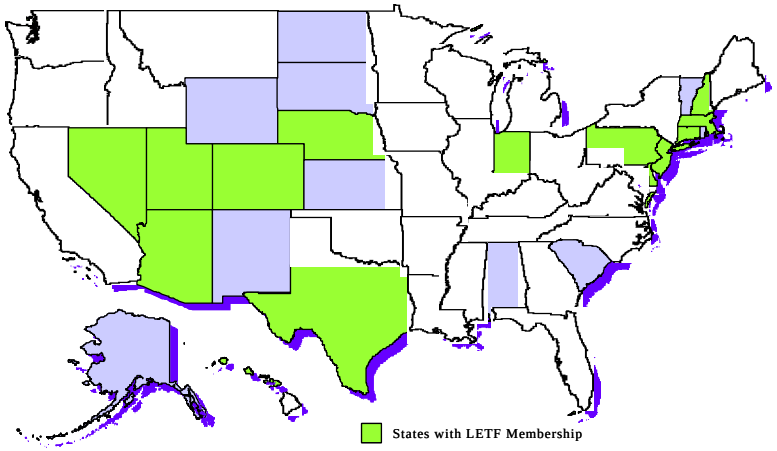
CALEA IMPLEMENTATION SECTION



Law Enforcement Technical Forum

Following the enactment of CALEA, CIS assembled the Law Enforcement Technical Forum (LETF) which consists of representatives from 43 state and local law enforcement agencies from 32 states and the District of Columbia, as well as 15 federal law enforcement agencies. CIS and LETF members have coordinated the resolution of many CALEA

implementation issues and developed consensus positions with several hundred of the major law enforcement agencies and prosecutors' offices across the United States.



Important Publications

The following list of publications and documents are a sample of those created by CIS in order to fulfill its CALEA implementation responsibilities and are available at the CALEA website maintained by CIS (www.AskCALEA.net):

- Cost Recovery Regulations
- Final Notice of Capacity
- Further Notice of Inquiry
- Flexible Deployment Assistance Guide
- Joint Petition for Expedited Rule Making Regarding Technical Requirements and Standards