FOIA Number: 2008-1524-F

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

Collection/Record Group: Clinton Presidential Records

Subgroup/Office of Origin: Office of Science and Technology

Series/Staff Member:

Subseries:

OA/ID Number: 43311

FolderID:

Folder Title:
Communications Assistance for Law Enforcement Act (CALEA) [2]

Stack:	Row:	Section:	Shelf:	Position:
S	1	1	7	3

~~15~~6.1.5.9 Relevant Standards and Specifications

[DOCSIS]	Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-I03-991105, Cable Television Laboratories, Inc., November 05, 1999. http://www.CableLabs.com/
[PKT-PCES]	PacketCable Electronic Surveillance Specification, PKT-SP-ESP-I01-991229, December 29, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com/.
[ISO8802-3]	ISO/IEC 8802-3, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1996. Available via http://www.iso.ch/projects/ics.html, field 35.110.
[J-STD-025]	TIA and ANSI Committee T1, Lawfully Authorized Electronic Surveillance, December, 1997.
[PKT-CODEC]	PacketCable Audio/Video Codecs Specification, PKT-SP-CODEC-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./
[PKT-NCS]	PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I02-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./
[PKT-SEC]	PacketCable Security Specification, PKT-SP-SEC-I01-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./
[RFC0768]	Postal, J, User Datagram Protocol, August, 1980.
[RFC0791]	Postal, J., Internet Protocol, September, 1981.
[RFC0826]	Plummer, D, Ethernet Address Resolution Protocol, November, 1982.
[RFC0894]	Horning, C, Standard for the Transmission of IP Datagrams over Ethernet Networks, April, 1984.
[RFC1889]	Schulzrinne, H, S. Casner, R. Frederick, V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, January, 1996.
[RFC1890]	Schulzrinne, H, RTP Profile for Audio and Video Conferences with Minimal Control, January, 1996.
[RFC2327]	Handley, M, and V. Jacobson, SDP: Session Description Protocol, April, 1998.

~~6.2.2XDSL\~~
~~SDO Lead:~~
~~Contact:~~
~~6.2.3X.25~~

~~SDO Lead:~~
~~Contact:~~

6.1.6 ~~APPENDIX:~~ X.25 over ISDN Basic Rate Interfaces (BRI) technology

T1S1 has completed its investigation into the Packet-Mode Communications issues identified by the FCC Report and Order 99-230[11]. The activity was addressed under T1S1's scope and charter to participate in the development of a joint T1-TIA standard on surveillance.

The T1S1 investigation specifically addresses the issues in FCC 99-230 and the request to identify capabilities which can be used to report ~~Call-Identifying~~ Pen Register and Trap and Trace information for Packet-Mode Data Communications separately and distinctly from call or communication content. The focus of the investigation was on the X.25 over ISDN Basic Rate Interfaces (BRI) technology. The investigation was conducted on a technical merit basis and made no judgment with respect to legal issues regarding the applicability of the Communications Assistance for Law enforcement Act (CALEA).

~~1~~6.1.6.1 Information that can be reported

~~15.2~~6.1.6.1.1 ~~Call-Identifying~~ Pen Register and Trap and Trace Information

For the X.25 Switched Virtual Circuits (SVCs) over ISDN Basic Rate Interfaces (BRI) technology, the packet handler will receive connection setup messaging from the subject. In these cases the setup messaging exchanged between the subject and packet handler can be used as triggers for monitoring and reporting surveillance events. The following ~~call-identifying~~ Pen Register and Trap and Trace information is available for X.25 SVC calls and can be provided to the Law Enforcement Agencies (LEAs) separately from the call content:

- Calling Party Number
- Called Party Number
- Answering Party Number
- Call Redirection/Call Deflection information
- Network User Identification (NUI)
- Recognized Private Operating Agency (RPOA)
- Called Line Address Modification Notification (CLAMN)

For the X.25 SVCs over ISDN Basic Rate Interfaces (BRI) technology, the existing J-STD-025 and J-STD-025A set of Call Data Channel (CDC) messages can be used to report surveillance events of packet-mode data communications during call setup, call progress, and call clearing (i.e., Origination,

TerminationAttempt, Redirection, Answer, Release). The J-STD-025A parameter set does not support the reporting of the Reverse Charging and Reason for Redirection information.

For X.25 PVC service, the ISDN packet handler uses a pre-provisioned connection across the packet network to deliver all transmitted packets between the subject and associate. In these cases no connection establishment signaling is involved and, therefore, no end-to-end routing information is available to the X.25 layer at the packet handler. The packet handler only maps the incoming ISDN connection from the subject to an X.25 PVC across the packet network. Therefore, ~~call-identifying~~ Pen Register and Trap and Trace information for a PVC is not available at the X.25 layer.

For X.25 PVC service, only administrative records and operations personnel have knowledge of the end-to-end connection. This is because the operations personnel used the end-to-end information to provision the connection from the user to the packet handler (via an ISDN Permanent B-Channel Connection or D-Channel Connection) and then from the packet handler to an interoffice facility. At each switch in the PVC's path (which may cross network boundaries), the connection is mapped from one facility to another, until it is connected to the associate. Since the ~~call-identifying~~ Pen Register and Trap and Trace information for X.25 PVCs cannot be derived by information at a given switch, the delivery of such information to LE over the J-STD-025A delivery interfaces cannot be automated.

~~15.3~~6.1.6.1.2 Call Content

While only CDC messages should be sent for Pen Register type surveillances, Title III surveillances will require that call content be delivered over the packet Call Content Channel (CCC).

The call content information is available at the X.25 level. All X.25 packets should be intercepted and ~~call-identifying~~ Pen Register and Trap and Trace information is not separated from call content before being replicated and transported over the packet CCC to LE.

The existing J-STD-025A set of messages to report the assignment and release of packet CCCs for the delivery of intercepted call content from packet-mode data communications can also be utilized (i.e., CCOpen, CCClose). The existing procedure in the J-STD-025A for reporting call content (Fast Select data) over the CDC can be used to report the transport of call content in X.25 SVC call setup, call progress, and call clearing packets.

The call content monitoring impacts for X.25 PVCs are similar to those described for X.25 SVCs. When monitoring call content for X.25 SVCs, the LEAs receive the necessary call parameters within the signaling packets that are also delivered over the packet CCC. However, for X.25 PVCs there are no signaling packets, and the call parameters are pre-provisioned for the connection. Consequently, when a court order requires call content monitoring for X.25 PVCs, the call parameters will need to be reported separately via a manual process, similar to the process for ascertaining the ~~call-identifying~~ Pen Register and Trap and Trace information for X.25 PVCs. When call content is to be monitored on a X.25 PVC, certain call parameters may be needed to facilitate the LEAs processing of the call content data packets delivered over the packet CCC delivery interface. These call parameters include the packet modulo sequencing, the packet size, and the window size for the packet call. Without these parameters, it will be difficult or impossible for LEAs to properly extract the call content from the monitored packet-data communication.

~~16~~6.1.6.2 Technical Impacts

The following ~~call-identifying~~ Pen Register and Trap and Trace information is available for X.25 SVC calls but can not ~~can~~ be reported to the LEAs because the existing J-STD-025[iii] and J-STD-025A[iii, iv] [12] set of Call Data Channel (CDC) messages and parameters do not support the reporting of the information:

- Reverse Charging facility
- Reason for Redirection (as reported in the CLAMN facility)

When an X.25 PVC is re-provisioned to a different remote party (where the intercept subject is the local party), it may be problematic to ensure that LEAs receive timely notification. For X.25 PVCs that cross LATA (and usually state) boundaries, the ISDN service provider is not able to provide the identity of the remote party. Although the service provider may have noted the network address of the remote party in their records, this information has only nominal significance. Since the terminating party is in a different network, the local service provider cannot ensure that the X.25 PVC is actually connected to the network address listed in their records because network addresses do not have any real significance for X.25 PVC. The service provider can only confidently report the identification of the interoffice connection that is used to hand-off the X.25 PVC to the interLATA carrier. The LEAs would need to request that the interLATA carrier provide information about the connection; finally, the LEAs

[12] The monitoring and reporting capabilities currently defined in the J-STD-025 and J-STD-025A for packet-mode data communications to Law Enforcement are the same. This document refers to both interfaces, collectively, as the J-STD-025A interface.

could then request that the remote ISDN service provider confirm the identity of the remote party.

Interception of packet services also does not guarantee that the packets have been received by the terminating system.

~~6.2.4ISDN~~
~~SDO Lead:~~
~~Contact:~~

~~6.3~~6.2 Network layer protocols:

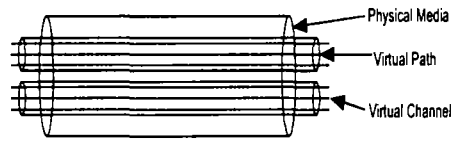
~~6.3.1~~6.2.1 ATM

~~SDO Lead:~~
~~Contact David Hoffman dwhoffm@uswest.com, Jay Hilton.~~
~~17 General~~
~~This contribution proposes a revision to the draft Appendix to the CALEA JEM Report on "ATM Technology". The proposed revision addresses several issues raised after T1S1 review. The nature of the proposed revisions includes the following elements:~~
~~- Clarified that the scope of the Appendix does not cover Switched Virtual ATM Connections;~~
~~- Clarified the scope of the Appendix covers three Adaptation Layers in common use today;~~
~~- Removed references to voice in the section on AAL2 as this aspect is included in previous text. Also removed subjective advantages of using AAL2, as these aspects may not always hold true;~~
~~- Clarified the text regarding VoIP;~~
~~- Reordered text regarding ATM cell processing for readability;~~
~~- Removed the explanation text on PVCs and SVCs, as the scope of the document was clarified in earlier text;~~
~~- Removed text on ATM goals, as this text is redundant;~~
~~- Clarified the conclusion text on the nature and location of information that may be available to LEA;~~
~~- Minor editorial changes throughout the Appendix;~~

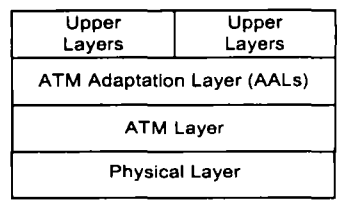
~~These revisions have been agreed by T1S1 and the original author, Mr. David Hoffman, for submission to the CALEA JEM meeting. The final text is presented below.~~
~~18CALEA JEM Report Proposed Text for Appendix on ATM Technology~~

This section describes Asynchronous Transfer Mode (ATM) and its use in transporting voice telephony. It concentrates on the public network where ATM is predominately used as the bearer service for other, upper layer protocols that are concerned with the origination and routing of voice telephony calls. Therefore, the use of Switched Virtual ATM Connections is not described in this Appendix.

ATM is a switching method that uses fixed size units, called "cells," to transport information from the source to the destination. It is designed to be a general-purpose transfer mode for a wide range of services including, but not limited to, the transport voice and data. ATM provides Layer 2 functionality in the Open System Interconnection (OSI) protocol layer model. Each ATM cell consists of a 5-octet header that defines the virtual circuit associated with the cell. Virtual circuits are defined by a combination of a Virtual Path Indicator (VPI) and a Virtual Channel Indicator (VCI). The remainder of the ATM cell consists of a 48-octet payload. In a typical public network large numbers of virtual circuits are carried on the physical media.



Included in the ATM header is a payload-type indicator that describes the cell as containing either user information or network management data. No information is included in the 5-octet header that defines the type of user data that is being transported.



Separating the ATM layer from the user data is an adaptation layer that adapts the services provided by the ATM layer to those required by the higher layers. There are currently only 3 ATM Adaptation Layers (AALs) in common use and are described in this Appendix. Each different adaptation layer defines specific services to the upper layer applications that they are designed to transport.

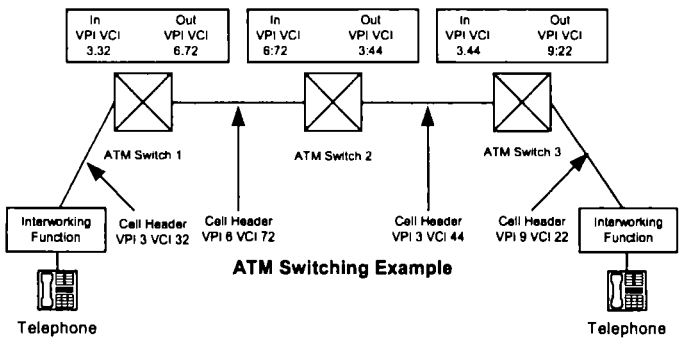
Providing voice telephony over any bearer service requires the use of an Interworking Function to map the user's voice signals into whatever protocol the bearer requires.

Voice telephony in an ATM network can be provided by AAL1 (Circuit Emulation Service), AAL2 (Voice Over ATM) and AAL5 (Variable Bit Rate).

ATM adaptation Layer AAL1 defines how Time Division Multiplexing (TDM) type circuits can be emulated over an ATM network. AAL1 supports emulation of DS1, DS3 and nxDS0 circuits and is used primarily to provide transport of PBX trunks.

ATM adaptation Layer AAL2 defines a method to provide variable length packet payload multiplexing within a single virtual circuit. One of the major advantages to using AAL2 is that it provides for multiplexing of voice packets into a single ATM cell. Either AAL2 or ATM adaptation Layer AAL5 is used to transport signaling data (DTMF, Common Channel Signaling, etc.) to the Voice Gateway.

ATM adaptation layer AAL5 defines a method to provide variable bit rate services primarily for data applications where the bursty nature of the applications can tolerate variations in delay. Voice over Packet (VoP) may be carried over AAL5, but the information above the ATM Layer appears as data to the ATM Layer.



As ATM cells arrive at the ingress to the network, each cell header is examined to determine if the cell contains network management or user information. If the cell contains user information, the VPI and VCI are looked up in a routing table to determine the outgoing facility to use in transporting the cell. Because the outgoing facility may use a different VPI/VCI combination, the node must replace the VPI/VCI with the new values. Cells continue in this way, moving from node to node until they reach their final destination. At no time during this process of *relaying* cells does the network know anything about the upper layer protocols that are being transported. Note that the VPI/VCI only indicates the association between the adjacent nodes and not the end-to-end connection. Nothing about the VPI/VCI defines the final destination of the cell or the user data that is being transported. Thus, ~~call-identifying~~ Pen Register and Trap and Trace information is not available.

ATM switching nodes are designed to relay the ATM cells as quickly as possible. This design effectively prohibits the ATM switch from reassembling and examining the user information encapsulated in each cell due to the processing demand and implementation that would be required. Within an ATM network, it is not technically feasible to extract the upper layer protocol, which contains the information of interest to the LEA from the ATM cell stream. It may be technically feasible, however, to extract call content information at the ingress and egress service interfaces.

~~6.3.2IP, Ipv4, Ipv6~~

~~SDO Lead:~~

~~Contact: Chip Sharp~~

~~7~~6.2.2 IP

†he IPv6 RFC ~~draft standard~~ 2460 is available and ~~IPv6 addressing~~ may become widely deployed in the future. However, as its deployment is limited at this time we considered only IPv4 impact on CALEA and did not consider the impact of IPv6.

6.2.2.1 Introduction

This section analyzes the areas identified in the main text of the document as they apply to networks using the Internet Protocol.

~~CALEA provides requirements for telecommunications carriers to assist law enforcement in lawfully authorized surveillance. In its definition of a telecommunications carrier, CALEA does not include entities that provide information services . Though they both use the term "telecommunications service," neither CALEA nor the FCC third report and order define the term. The definition of "call-identifying information" is also ambiguous when referring to IP. Therefore, rather than try to guess the intent of Congress or the FCC when defining terms such as "call identifying information" for IP-based services, the JEM decided to identify what information may be available in an IP packet flow and then consider technical issues of providing that information. During the discussion in the JEM, the only service that could be clearly identified as a telecommunications service was a POTS-like voice service.~~

~~The JEM also pointed out that various court cases currently underway may change the situation by the time this report is issued.~~

This section first discusses architectural principles of the Internet and the Internet Protocol that apply to the analysis of CALEA. It then follows the basic organization of the main text in that it investigates what information can be delivered and the technical issues of delivering that information both for a provider that supports a Call Management System and a provider that only supports IP transport.

Although the Internet (and IP) supports many applications other than Call Management Systems, due to the special consideration given to voice applications in the JEM this section only deals with Call Management Systems.

~~7.1.1~~6.2.2.2 Scope

This section concentrates on the Internet Protocol and related protocols.

While the Internet Protocol can be carried by a multitude of underlying and protocols technologies (e.g., leased line, dial-up modem, ATM, Frame Relay, X.25, etc.), this section does not consider the implications of CALEA on the underlying protocols. This is left to the appendix for the specific technology.

In addition, this section does not provide special considerations to any applications other than Call Management Systems that run over IP.

~~7.2~~6.2.2.3 Architectural principles related to CALEA

This section briefly describes architectural principles of the Internet that apply to the CALEA analysis.

There are plenty of tutorials and books on IP and routing available. It is assumed the reader is familiar with the operation of the Internet and the suite of Internet protocols. However, discussion of general principles that affect the issue at hand are included.

~~7.2.1~~6.2.2.3.1 End-to-end principle

"The network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes." [RFC1958]

The end-to-end principle is simple, but powerful. It recognizes that there are many functions that only make sense to implement in hosts at the edge of the network. Examples are reliability, security (encryption), etc. This is in marked contrast to other protocols and networks that have been developed over the last 100 years which attempt to subsume these functions into the network.

As an example, the Internet assumes that, in general, reliable data transfer is assured by the end systems instead of the network. What this means is that any retransmission due to packet loss is done end-to-end instead of inside the network. As a counterexample, X.25 and similar protocols provide retransmission on a hop-by-hop basis.

Quoting from [Saltzer], "The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

This does not mean that a service provider cannot offer enhanced services over such a network. What it means is that the enhanced services are either provided as part of the transport mechanism (e.g., Quality of Service) or are enabled on hosts reachable via the Internet. Examples of such systems are DNS, email servers, Web servers, etc. The customer reaches these services just like it would any other service not offered by the service provider (i.e., via IP).

A by-product of this principle is that the IP transport network will not necessarily know what applications are being run over the network since there is no "setup" in which the network participates. In fact the network is designed not to know what application is being carried. The applications run end-to-end and the network just routes packets. Where the network does provide a application-level service, it is through a host that it manages that communicates end-to-end with the customer's host over the provider's network.

The end result of this is an explosion of innovation in applications. Anyone with a link to the Internet can develop and offer new and innovative services to anyone else on the Internet (e.g., Napster). This applies to voice applications just as much as any other applications.

[SALTZER] End-To-End Arguments in System Design, J.H. Saltzer, D.P.Reed, D.D.Clark, ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288.

[RFC1958] Carpenter, B., "Architectural Principles of the Internet", RFC 1958, June 1996.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, February 2000.

~~7.2.2~~6.2.2.4 Security

Security encompasses many areas including, but not limited to, encryption. In general, the end-to-end principle applies to security (i.e., end-systems are responsible for their own security). However, service providers can provide assistance in some areas of security. For example, even though two end-systems may have adequate security in their locations and use strong cryptography between them, unless they have the cooperation of their service provider they are susceptible to denial of service attacks from third parties that flood their link to the Internet such that communications is degraded.

As discussed in Section 6 of [RFC2804], the introduction of capabilities for electronic surveillance tends toward making the network itself less secure, even when the capability is not being exercised. Much effort is underway in the industry to make the Internet more secure, not less. Development of specific protocols and methods for delivering an end-user's information to a third-party without the knowledge of the end-user does not contribute to making the Internet more secure.

Encryption has been a controversial topic for a long time. However, with the advent of more powerful computing devices and more powerful and available encryption algorithms, strong encryption is now technically available (but possibly not legally or politically available) to most people on the Internet. Following the end-to-end principle, encryption should take place between two hosts, not in the

network itself. The network may use encryption for its own purposes, but the hosts using the network ultimately must take care of themselves. The end systems may have a trust relationship with the service provider that enables the service provider to share in the security mechanism and encryption of data; however, the fact that CALEA may require the service provider to provide decrypted information (or keys) to an outside body (i.e., LEA) without the user's knowledge will force the service provider to implement mechanism that could make the system less secure than it might otherwise be, even if the subject is not under surveillance.

[RFC2401] Kent, S. and Atkinson, R., Security Architecture for the Internet Protocol, November 1998

[RFC2804] IAB, "IETF Policy on Wiretapping", RFC 2804, May 2000

~~7.2.3~~6.2.2.5 Encapsulation

"IP on everything" - Source Unknown

The Internet Protocol is designed to operate over a wide variety of network technologies and protocols. In fact the term internetwork (thus internet) derives from the fact that it was designed to interwork over multiple networking . Normally, an encapsulation method is defined for how to run IP over a particular networking technology. Encapsulation methods have been defined by the IETF for a wide variety of networking technologies (e.g., HIPPI, X.25, Frame Relay, ATM, FDDI, Ethernet, Token Ring, Arcnet, leased line, dialup, etc.) . As IP is routed from one network type (e.g., SONET) to another (e.g., Ethernet) it is encapsulated into a different mechanism that is usually specific to a the particular network type.

IP also encapsulates upper layer protocols inside its data field. These upper layer protocols are usually transparent to the IP layer and to the internet between two hosts. IP provides a Protocol ID that identifies the protocol contained in its data field. TCP and UDP are two predominant protocols that run over IP; however, other protocols can be run directly over IP (e.g., IPSEC, IP, RSVP, SCTP, etc.). Over 100 Protocol numbers have been assigned by IANA for use in the IP Protocol ID field. Normally for user data transfer, the Protocol ID does not identify the application the hosts are running. The applications normally run over a transport protocol (e.g., UDP or TCP) that runs on IP. The end systems can identify which application a particular packet is destined for by the TCP (or UDP) port number. There are several thousand port numbers currently registered with IANA for use with TCP or UDP.

Thus the application data is usually encapsulated in UDP or TCP which is encapsulated in IP which is encapsulated in a link or network specific mechanism.

~~7.2.4~~6.2.2.6 Connectionless Orientation

The Internet Protocol is a connectionless protocol. In general, each packet contains all the information needed to route the packet from one host on a network to another host on the same or different network. Each packet is routed through the network(s) independent of the previous packet and may take a different path through network(s) than a previous or subsequent packet. There is no explicit setup mechanism between a host and the network to provide communication between two hosts. There is no "call" in IP. Loop Start in the analog telephony world and Q.931 in the ISDN world are examples of signaling protocols between a host (e.g., telephone) and network that set up connections (i.e., calls) between two hosts (e.g., two telephones).

As mentioned earlier, a service provider can provide services by deploying hosts in the network to which customers' hosts can communicate. A customer's host can request service from the provider's host; however, the network provides the connectivity for the packets. An example of this is DNS. A host wants to communicate with another host, but only knows the host name and not the IP address. The host sends a query to the DNS server via IP and the DNS server responds with the destination host's IP address. This is still a connectionless service.

~~7.2.5~~6.2.2.7 Boundaryless

"There's a freedom about the Internet: As long as we accept the rules of sending packets around, we can send packets containing anything to anywhere." [Berners-Lee]

One by-product of the above principles is that IP inherently has no concept of geopolitical boundaries. While a network's design may provide some loose constraints as to what path a packet may take, there is usually no guarantee a packet will take a particular path at any particular time.

For example, host in Tuscaloosa, Alabama may download a file from another host in Mobile, Alabama. There is no guarantee that the packets in this download will stay in the state of Alabama. They may transit part of the network in Mississippi, Florida or any nearby state. This is considered part of normal operation of the Internet. Therefore, information that may be reasonably available in a connection-oriented network may not be available in an IP network.

~~7.3~~6.2.2.8 Call Management System

The main text contains general information for packet mode technologies concerning information derived from a call management system. This section contains information specific to the Internet Protocol.

Call Management Systems don't exist for the Internet Protocol. However, call management systems exist for applications that run, end-to-end, over IP. In

general on an IP network, a call management system is a host attached to the IP network running call management protocols end-to-end over IP to its clients. For VoIP applications, the encoded voice stream is also carried over UDP/IP. In VoIP, the IP packets carrying voice are usually carried directly between the two endpoints involved in the call. The Call Management System is not involved in transporting the voice packets.

~~7.3.1~~6.2.2.8.1 Information that could~~n~~ be reported

The information discussed in the main text also applies to IP-based Call Management Services. Since the information available from Call Management Services tends to be specific to the application (i.e., Voice) as opposed to IP, the information itself is pretty much the same as the main text. The call events described in J-STD-025 are examples of information that can be reported

In a network that provides a call management system, only call events that are triggered by messages between the target and CMS are available.

For IP, the call content flow within the immediate network can be characterized by the source and destination IP address and source and destination UDP port numbers negotiated between the CMS and target during call establishment. This only applies to call control protocols that exchange IP address and port numbers with the CMS. This applies to most VoIP signaling protocols currently defined, but may not apply to future applications.

The following are IP-specific items:

- IP information for call management protocol:
  - IP address used by target
  - TCP or UDP port number used by target
  - IP address used by Call Management System
  - TCP or UDP port number used by Call Management
- IP information for voice packet stream
  - IP address used by target for voice packet stream
  - TCP or UDP port number used by target for voice packet stream
  - IP address used by target's associate for voice packet stream
  - TCP or UDP port number used by target's associate for voice packet stream

Other call events similar to those defined in J-STD-025 may be available to the extent that the Call Management supports similar services (e.g., Call Forward).

~~7.3.2~~6.2.2.8.2 Technical issues

The issues addressed in the main text also apply to IP. This section discusses issues specific to IP.

~~7.3.2.1~~6.2.2.8.3 Location and Ownership of Call Management System

Since it runs over IP the Call Management System can be located anywhere on the IP network. It can be provided by the Service Provider that also provides the Internet access service to a customer, by another Service Provider on the Internet or by a customer on another Internet Service Provider. Thus, the CMS may not be within the same jurisdictional boundaries as the client host to which it is providing service even if the two endpoints involved in a call are within the same jurisdictional boundaries. The only real requirement is that the user have reachability via IP to the CMS. In the extreme case the CMS could be in a different country from the hosts to which it is providing service.

This follows the principle laid out in Section 10.2.4.

Given that Call Management protocols are end-to-end protocols over the Internet, a Service Provider will only have access to call events detected on its Call Management System. This section only discusses issues with what information can be gleaned from a Call Management System operated by the Service Provider.

The Call Management Server in an IP network can only report events based on packets that are terminated on or originated from the Call Management Server. If the target knows the destination address of the person it wants to call or if the target uses a Call Management System not under the control of the service provider, the target can establish a VoIP call without the knowledge of the service provider's Call Management System. Call Events for such calls will not be available to the service provider.

Even when the target uses the provider's Call Management Server, not all call events for call manipulation may go through the Call Management Server. For example in the middle of a call the endpoint under surveillance may exchange call control information with a Call Management Server not under the control of the service provider. These packets will not necessarily go through the Call Management Server, but will be routed normally as data packets.

~~7.3.2.2~~6.2.2.8.4 Call Management Protocols

The Internet places no restriction on the protocols used between the CMS and client for managing calls. In today's PSTN, the base protocols used for call control are limited to a small number due to the technology and the small number of providers. Each country or network may define its own variant of the base PSTN protocol but they all have the base in common.

The following is a list of some of the protocols defined for call management over IP by various industry groups

- H.323,
- SIP,

- H.248/megaco,
- MGCP,
- PINT (based on SIP)

More protocols are being developed. Each of the above listed protocols is fairly flexible in allowing different services based on the core protocol. Therefore, nailing down a complete, fixed set of call events that are available via each protocol is close to impossible.

In addition, some of these protocols (e.g., SIP) can be used for provision of information services. In fact the same CMS host could offer information services using the same protocol at the same time as offering VoIP service.

Since the CMS and the client usually run on open computing systems, new call control protocols are usually easily downloaded and installed. The CMS and client don't have to run standard protocols as long as they agree with each other what protocol to use.

The ubiquitous HTTP (i.e., protocol used to support the world wide web) is also being used by various entities to offer VoIP services such as "click-to-dial". In this case there is not necessarily a specific call control protocol and the CMS is a web server.

In some protocols (e.g., SIP, H.323), the information exchanged between the client and the CMS may only be sufficient to resolve an identifier such as an email address to an IP address which the client uses to negotiate the call further. In this case, subsequent call events may not be available to the CMS.

Although the call control protocols have UDP/TCP port numbers assigned to them via IANA, there is no hard requirement in the Internet to use these port numbers. The port numbers used for call control is a bilateral agreement between the CMS and client. Most of the time, applications will utilize the IANA-assigned port numbers at least for the initial information exchange; however, this is easily changed by agreement.

The port number negotiated between the CMS and the end-systems for the actual voice stream is variable and dynamic. It is assigned to each end of the call on a call-by-call basis. In addition, some call control protocols may use a dynamically assigned port number for negotiating supplementary and other services.

In conclusion:

- There is not a clear, fixed definition of CMS for VoIP
- There is not a complete, fixed, limited set of services defined for VoIP. However, a limited, fixed set of services can be defined that might be available by most providers (e.g., connect, disconnect, forward, transfer, etc.).

- There are multiple protocols a client can use to communicate to the CMS
- The UDP or TCP port numbers used between CMS and client for call control are via bilateral agreement. Most of the time they are IANA-assigned.
- The CMS used for VoIP support can also offer Information Services at the same time using the same protocol.

~~7.3.2.3~~6.2.2.8.5 Service Paradigms

The CMS does not necessarily follow any traditional paradigm in terms of the services it offers. Some Service Providers will use a CMS to offer VoIP services that mimic today's PSTN as closely as possible, thus recreating the current phone system on IP. In this case, it is reasonable to expect that call events similar to those defined in J-STD-025 or PacketCable(TM) may be available. Other Service Providers, or end-users on the Internet, may provide innovative services that are not possible or available on today's phone system and may not offer many of the services that are available on today's phone networks. In fact, some of the new services may not be recognizable as traditional voice services and could be interpreted as information services. This is the anticipated result of the end-to-end principle which enables anyone attached to the Internet to develop and offer services.

The distinction between an "electronic messaging service" which as defined by CALEA includes audio (e.g., voice) and is not included in CALEA requirements and a VoIP service will tend to blur as time goes on and the market develops. For example, an end-user could send an email with an audio attachment. The receiver of the email could listen to the attachment and send back an email with an audio attachment as a response. This would fall under the "electronic messaging service" and could also be seen as a voice conversation with a long delay.

The amount of control a Call Management Server exercises over a target's endpoint varies greatly depending on the standard used and how it is used. It can exercise very little control, such as in some SIP or H.323 RAS cases, or detailed control such as in H.248 or MGCP. Thus the amount of information available will depend on the service offered by the service provider and by the protocols used for providing the service.

If the Service Provider is providing a traditional telephony service over IP, then call events such as those defined in J-STD-025 or the PacketCable specification should be available.

~~7.3.2.4~~6.2.2.8.6 Redirection of Calls

As discussed previously, packets carrying the call content are not guaranteed to follow a particular path through the Internet. Nor are they guaranteed to stay on the provider's network even if the two endpoints are on the provider's network. If the target is communicating with another endpoint off the provider's network and redirects the call to another endpoint off the provider's network, then most likely all packets involved in the redirected call will not transit the provider's network (although it is possible they will). Therefore, these packets are not available to the original service provider and cannot be provided. In addition, since the call is redirected, the service provider's Call Management Server is no longer involved and may not have access to any call events related to the redirected call.

~~7.3.2.5~~6.2.2.8.7 Target Identification

In order to provide the information required, the correct target must be identified.

If the service provider has a relationship with the target and the target uses the service provider's CMS, then it will probably be able to identify the target via either a login, pre-assigned IP address or other pre-assigned identifier (e.g., calling party number).

If the IP address of the target is known, it can be used to identify call events from the target. Usage of IP addresses has the same issues discussed below for IP Transport.

However, some services offered on the Internet may not require a specific relationship between the provider and the client. For example, these may be ad-hoc services offered via the world wide web. The provider of the service may not know who is using the service, much like a web server today. In this case, the only information it may have about the target is the information the target sends it. The target's IP address would be one constant. that could be used to identify the target. Again, correlating the IP address to the target will have the same difficulties as defined below for IP transport.

In traditional PSTN telephony, the telephone number can be used to identify the called and calling party. It is recognized that this usually identifies a physical telephone that anyone can use, including people that are not under surveillance. In VoIP, a telephone number may not be used to identify the caller. For example, SIP allows the use of email-like addresses (e.g., foo@bar.com) to identify the called and calling party. Therefore, existence of telephone numbers is not guaranteed on the CMS.

~~7.3.2.6~~6.2.2.8.8 Performance and Complexity

The performance impact on the Call Management System will depend on the services offered and the information required. If information similar to J-STD-025 is provided, the performance implications will be similar.

If the protocol used to deliver the information to the LEA is significantly different from the protocol used by the CMS for its other communication, it could have an affect on the complexity and performance of the system. For example, if the CMS is using IP to provide service but must use X.25 to communicate to the LEA, the separate drivers and software to run X.25 may introduce additional complexity. Also, if the data formats used to deliver to the LEA are substantially different, then this will also introduce additional complexity (e.g., a CMS that does not use ASN.1 to provide service but must use ASN.1 to provide CALEA information).

~~7.3.2.7~~6.2.2.8.9 Delivery Format

The various call control protocols listed above utilize different encoding mechanisms. For example, SIP is text encoded with syntax defined in Augmented Backus-Naur Format (ABNF) while H.323 is binary-encoded with syntax defined in ASN.1. H.248 allows both. Thus, it is not possible to define a delivery protocol that is consistent with the encoding mechanism of each protocol.

However, it is possible to define a delivery mechanism for all the identified protocols that runs over IP and reduce the complexity of using multiple network protocols for delivery.

~~7.3.2.8~~6.2.2.8.10 Points of Intercept

For CMS, the point of intercept would most likely be on or near the CMS.

~~7.4~~6.2.2.9 IP Transport

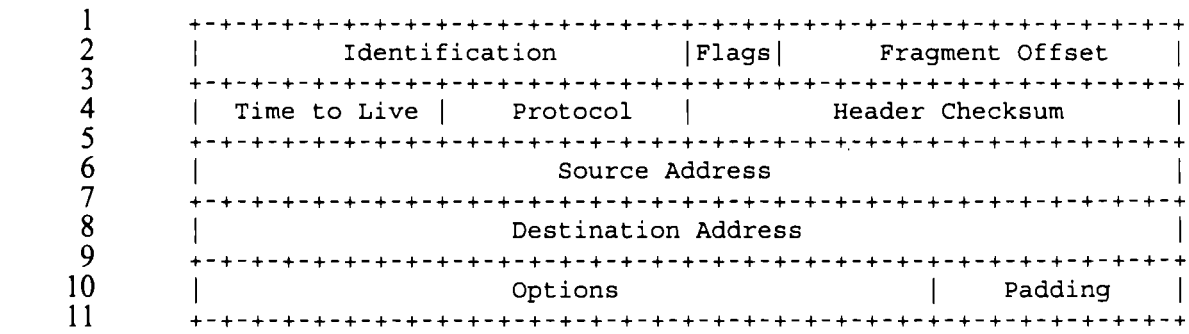
This section focuses on information available from a service provider that is offering IP transport. In this case, the ~~provider~~ subject is not ~~providing~~ using a Call Management System offered by the service provider. ~~It is just routing packets. This section also applies to Service Providers that offer a Call Management System but it is not used by the target.~~

~~7.4.1~~6.2.2.9.1 Information that can be reported

The IP transport provider utilizes the information in the IP packet for providing service. In general, routers are optimized to operate on the IP header for providing service. Layer 2 switches are optimized to operate on Layer 2 headers to support transmission of IP.

A copy of the IPv4 header is shown below:

```
 0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |Version|  IHL  |Type of Service|          Total Length         |
```



The information in this packet header that identifies the source and destination endpoints are the Source and Destination Address fields.

Since the provider in this case does not participate in any call control, it does not have access to information identifying a call. All it does is transport packets. Note that this discussion also applies to a Service Provider that provides a CMS when the target is not using the CMS.

The next layer protocol is identified by the Protocol field. The valid values for the Protocol field are defined by IANA. The next layer protocol could be UDP, TCP or could also be IP. There are several hundred Protocol Numbers defined by IANA for protocols running over IP.

The following three cases were identified at JEM I concerning information that can be provided:

a) Transmission of entire packet stream: In this case, the provider transmits the entire packet stream to and from the target to an LEA and the LEA uses minimization to extract the information to which they are legally entitled. However, it should be noted that this is similar to the original solution which caused the FCC to request this report. In other words, there is no separation of ~~call-identifying~~ Pen Register and Trap and Trace information from call content. In this section, transmission of the entire packet stream means transmission of the packets whose source or destination IP address match the target's.

b) IP source and destination address: This is the source and destination address contained in the IP header. In the case of tunneling, this would be the information contained in the outermost IP header. This could also include the Protocol ID field.

c) Extraction of information in the IP data field: This consists of the provider examining the data field of each IP packet in the packet stream to discover "~~call-identifying~~ Pen Register and Trap and Trace information." Since IP uses successive encapsulations to carry data, the question of how deep into a packet a provider must go to retrieve the information. Examples of information discussed included:
   - TCP or UDP port numbers
   - Call Control (e.g., SIP Invite, H.323 SETUP) information extracted from data field.

~~7.4.2~~6.2.2.9.2 Technical Issues

This section deals with technical issues specific to IP. The main body of the text contains general issues for packet mode that apply to IP as well.

This section discusses the issues surrounding delivering the information identified above as well as several general issues related to IP technologies.

~~7.4.2.1~~6.2.2.9.3 IP Packet Fragmentation

The maximum packet sizes supported by the various networks in the path from source to destination may be different. When a router receives a packet on one interface that is larger than the maximum packet size of the interface to which the packet is routed, the router might fragment the large packet into multiple smaller packets. A host might also perform this fragmentation, but it is recommended that the application not generate packets that are too big.

If an IP packet is fragmented, only the first packet will contain the upper-layer protocol headers. For example, only the first packet will contain the TCP header and thus the port numbers. The subsequent packets will not contain the port numbers. Therefore, port numbers may not be available in each IP packet.

~~7.4.2.2~~6.2.2.9.4 Target Identification

This is a general issue related to all three cases in addition to the Call Management System case. In any of the above cases, the LEA must identify the target

There are two general issues involving target identification:

Use of Network Address Translation

Use of Dynamic IP Address Assignment

~~7.4.2.2.1~~6.2.2.9.4.1 Use of Network Address Translation

The global Internet uses globally unique IP addresses. However, provision is made [RFC1918] for useage of private addresses. Two non-overlapping private networks may use the same private IP address space

When end-systems on different networks using private addresses (or an end system on a private network and an end system on a public network) need to communicate, a method called Network Address Translation is used to translate the IP addresses between the two networks. Therefore, the IP address contained in an IP packet in one network may be different from the IP address for the same packet in another network. The address translation between two networks can be fixed (address in one network statically mapped to an address in another network) or dynamic (address in one network dynamically mapped to one of a pool of addresses in the other network). In the case of dynamic mapping, the

address seen in one network may be mapped to a different address in the other network depending on time of observation.

~~7.4.2.2.2~~6.2.2.9.4.2 *Use of Dynamic IP Addresses*

IP addresses can be "leased" for a period of time, released and reused. These addresses are usually called "dynamic" IP addresses as opposed to "static" IP addresses which are assigned to a user for an extended period of time. A dynamic IP address only identifies an endpoint for the duration of usage by that endpoint. Several mechanisms have been defined to assign IP addresses dynamically. The most common are Dynamic Host Control Protocol (e.g., in LANs and cable networks) [RFC1541] and Internet Protocol Control Protocol (A control protocol used by PPP endpoints, e.g., ., in dialup or xDSL networks) [RFC1332]. Therefore, an IP address may only identify the target or its associate during the duration of a particular connection or session. The target and its associate may have a different IP address at a different time, even if connecting from the same location.

In some of the dynamic addressing schemes, the user authenticates with the network before being assigned an IP address. For example, in dialup Internet access the user usually has to authenticate using PPP before it is assigned an IP address. The user database is stored in a server and the Remote Authentication Dial In User Service (RADIUS) [RFC2138] protocol is used between the network access device and the server to determine if the user is allowed to access the network. However, in many cases the IP address is allocated from a pool on the network access device and not from the RADIUS server. Therefore, even the RADIUS server that authenticates the user may not be aware of address assigned to the user. If the provider uses RADIUS Accounting [RFC2139], then the accounting messages sent from the network access device to the accounting server may contain the address information. RADIUS is an example of an authentication and accounting protocol and is not necessarily the only one used in a network

[RFC2138] Rigney, C. et. al. " Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2138, April 1997.

[RFC1541] Droms, R., "Dynamic Host Configuration Protocol", IETF RFC 1541, October 1993.

[RFC2139] Rigney, C., "RADIUS Accounting", IETF RFC 2139, April 1997.

[RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", IETF RFC 1332, May 1992.

[RFC1918] Rekhter, Y., et. al., "Address Allocation for Private Internets" IETF RFC 1918, February, 1996.

[RFC1631] Egevang, K., et. al., "The IP Network Address Translator (NAT)", IETF RFC1631, May 1994.

[RFC2663] Srisuresh, P. and Holdrege, M., "IP Network Address Translator (NAT) Terminology and Considerations", IETF RFC 2663, August 1999.

~~7.4.2.3~~6.2.2.10 Transmission of entire packet stream

In the case of transmission of the entire packet stream, there is no separation of ~~call-identifying~~ Pen Register and Trap and Trace information from content since the provider is providing all the data to and from the target.

In order to transmit the entire packet stream to the LEA, the packet stream must be extracted from the aggregate packet stream. There are a several methods for doing this:

- Packet replication: In this method the service-providing equipment (e.g., router) replicates the packet stream to/from the target and transmits the packet stream to the LEA (possibly from a different interface). A simple example of this is to connect to a span port on an ethernet switch.
- "Sniffing" the packet stream: In this method, the provider or LEA connects equipment to the physical medium to extract the packet stream from the aggregate packet flow. A simple example of this is to tap into a coax ethernet cable and copy off packets.

In the first case, if packet replication is performed on the service-provider equipment, the capacity used for replication will not be available for providing service. This may affect service to the provider's customers including the target. Packet replication may require hardware support that is not available in all equipment.

The second case requires non-obtrusive physical access to the transport medium. Some physical media (e.g., fiber optic) is not conducive to a non-invasive tap unless a tap is preinstalled for such activity.

There are several issues with transporting the entire packet stream. One is based on the service provided. For example, a virtual private dial service encapsulates the PPP packet from the customer into an IP packet (using L2TP) destined for a gateway into another network. In this case, the Network Access Equipment does not normally assign or look at the IP addresses in the customer's packets. In addition, multiple user sessions can be multiplexed into one tunnel to the remote side. Monitoring behind the NAS would require specialized equipment to de-encapsulate the tunneled packet (and possibly de-encrypt) to extract the original IP addresses.

~~7.4.2.4~~6.2.2.11 Transmission of IP Source and Destination Address

To transmit the IP source and destination addresses requires the equipment to read the IP header, ~~separate~~ extract the source & destination address and deliver that information to the LEA.

Service providing equipment may not be designed to extract IP header information and deliver it to the LEA. Other equipment may be able to do this. In any case, the processing capacity used for delivering the header information is not available for routing packets. The amount of load on the system will depend on the system. There are a multitude of vendor equipment of different types deployed for Internet service and each one would have to be tested to determine what load it would support.

On the other hand, specialized equipment exists today that can extract the IP header information and some other information (e.g., TCP or UDP port number) from a real-time stream.

~~7.4.2.5~~6.2.2.12 Extraction of Information from Packet Stream

The extraction of information from a packet stream for delivery to the LEA was one option discussed at the JEM and other fora. For example, the provider would be required to monitor the packet stream, detect a call control packet containing ~~call-identifying~~ Pen Register and Trap and Trace information (e.g., for VoIP), extract the ~~call-identifying~~ Pen Register and Trap and Trace information from the packet and deliver it to the LEA.

Routers supporting service on the Internet typically only make routing decisions based on the IP addressing information. Service providing equipment is not generally designed to look past the IP headers (some may look at TCP or UDP port numbers for filtering) when switching or routing packets. Any processing capacity used for extracting information from a packet stream is not available for routing packets. Given the increase in capacity of Internet connections and that systems generally run at peak load much of the time, there is very little capacity to monitor data fields.

An alternative is to use equipment that is not providing service to the customer but has access to the data stream (e.g., via a port on an ethernet switch). This equipment could acquire the information required and deliver it. This would require extra equipment by the service provider and new operating procedures. In addition, any time new equipment is added to a network it introduces the possibility of errors and misconfiguration and can disturb the functioning of the network.

However, as noted in the main text, there is no reliable method for determining the ~~call-identifying~~ Pen Register and Trap and Trace information when

monitoring a packet stream. If given a specific IP address and port number and if encryption or tunneling isn't used and if the call control protocol is identified then it might be possible to extract the call control information for VoIP calls. However, there is no guarantee that the session is a telecommunications service or an information service. It would be similar to requiring telecommunications carriers to monitor inband communications, detect and demodulate modem tones, detect and decode the information carried in the modem signal and ~~separate~~ extract ~~call identifying~~ Pen Register and Trap and Trace information that may be carried. This is not equivalent to detecting in-band DTMF.

~~7.4.2.6~~6.2.2.13 Tunneling

One of the issues with identifying the target and providing information is the use of tunneling. In essence, tunneling is the act of encapsulating network protocol packets into IP packets to be routed across the network. In this section, the tunneling of IP packets is considered. The tunneling method defines a mechanism to encapsulate IP packets inside other IP packets. The outer IP header is used to route the packet across the network. The source and destination addresses of the outer IP header identify the tunnel endpoints. The IP addresses in the IP header may not be the IP address of the final endpoints. For example, the tunnel endpoint could de-encapsulate the IP packet and route it onward using the encapsulated IP address information.

There are several methods that can be used for tunneling IP packets across an IP network: Generic Routing Encapsulation [RFC1702], IP-in-IP [RFC1853], Layer 2 Tunneling Protocol [RFC2661], IP Encapsulating Security Payload (ESP) [RFC2406], etc.

The network routes packets based on the outer IP headers and not on the inner headers. In some cases, such as in IPSEC ESP [RFC2406], the encapsulated IP packet is encrypted and isn't available even if the service provider could sniff into the data packet.

For tunnels originated from the target, the destination IP address in the IP packets from the target and the source IP address of IP packets to the target are not necessarily the IP address of its associate. This IP address could be a tunnel endpoint which will de-encapsulate and route the tunneled packet onward. The source IP address of IP packets from the target and destination IP address of IP packets to the target will normally be the IP address of the target in order for packets to be routed to it properly.

For tunnels originated in the network, the original IP headers may be available. However, in some cases, such as L2TP, the original IP addresses may not be readily available. In L2TP, the network access device encapsulates all PPP frames from the user into IP packets into another IP packet destined for another location. In this case, the IP addresses of the outer IP header will be the IP address of the network access device and the remote tunnel endpoint. The

target's IP address will not be in the outer IP header at all. The IP address of the target is assigned by and is only seen by the remote tunnel endpoint. The tunnel from the network access device to the remote tunnel endpoint may be shared by many users including the target.

[RFC1702] Hanks, S., et. al., "Generic Routing Encapsulation over IPv4 networks", IETF RFC 1702, October, 1994.

[RFC1853] Simpson, W., "IP in IP Tunneling", IETF RFC 1853, October 1995.

[RFC2661] Townsley, M., et. al., "Layer Two Tunneling Protocol 'L2TP' ", IETF RFC 2661, August 1999.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406, November 1998.

[RFC2002] Perkins, C., "IP Mobility Support", IETF RFC 2002, October 1996.

[RFC1661], Simpson, W., "The Point-to-Point Protocol (PPP)", IETF RFC 1661, July 1994.

~~7.4.2.7~~6.2.2.14 IP Address Spoofing

Another issue that will affect the integrity of the information provided to the LEA is IP address spoofing.

A destination IP address must be authentic or else it cannot be routed to an endpoint. However, a source IP address may or may not be authentic since it is not required for the network to route packets to the destination properly. A valid source IP address is required for the destination to transmit packets properly back to the source. However, there may be cases in which an entity may not care about receiving responses.

Although there are several methods available to do so, in general network access devices do not check for invalid source IP addresses before accepting packets into the network and forwarding them. Therefore this allows endpoints to spoof the source IP addresses.

There are two cases when dealing with spoofed IP addresses and CALEA:

Target spoofing source IP addresses to a destination

Associate spoofing source IP addresses to the target

In the first case, if the provider is keying on the source IP address in order to provide information to the LEA and the target is using a shared line to access the network, the provider would not necessarily detect and supply information on IP packets with spoofed source IP addresses from the target. A consequence of this is that the target could carry out a Denial of Service attack on a remote host without it being detected by the tap.

In the second case, a remote endpoint could send packets to the target with spoofed source IP addresses. This could result in several things happening:

Under a Trap & Trace order the remote endpoint could cause the LEA to investigate users who have no relationship with the target by spoofing their IP addresses.

Under Title III, the remote endpoint could incriminate the target (and other users) by sending illegal material to the target with spoofed source IP address.

Although the information required to carry out the above attack is not necessarily readily available (e.g., the fact the target is under surveillance, the IP address of other endpoints, etc.), it is possible for a sophisticated user with knowledge.

Software to spoof IP packets is readily available on the Internet. Tracing a packet stream with spoofed source IP address back to the originator is extremely difficult to do on the Internet, especially if the packet flow is intermittent.

~~7.4.2.8~~6.2.2.15 Delivery format

In defining the delivery format for IP, the characteristics of internet connections should be taken into account.

The connection speeds from providers to their customers is continuing to increase. The delivery vehicle for the information collected may have to be substantially different for a customer connected via Gigabit Ethernet to one connected via a dial-in modem.

For deliverying IP addresses, the provider could provide large amounts of effectively the same information for large data flows since the IP addresses don't usually change for a data flow. Or the provider could supply the information once per data flow. The latter option could reduce the amount of information transmitted to the LEA and the strain on the system.

~~7.4.2.8.1~~6.2.2.15.1 Transport Protocol

In defining the protocol used between the POI and the LEA, the characteristics of the transport protocol must be taken into account.

The following characteristics must be taken into account:

- Reliability: While TCP will provide a reliable connection between the LEA and the POI, it will also require more processing in the end-systems. If a real-time packet stream is required to the LEA, TCP may not be suitable since it is not designed for real-time transport. A UDP based protocol will require the least processing; however, UDP does not provide reliability.
- Security: If IPSEC is used between the POI and the LEA, the processing requirements of IPSEC must be taken into account.

~~7.4.2.9~~6.2.2.16 Performance and Complexity

Due to the different types of network access, the different types of equipment and different vendors, acquiring hard performance numbers on the impact of providing information is not possible. It would require testing of each piece of equipment in each scenario.

However, some general principles can be considered.

Introducing new features and new code into a system introduces complexity into the system along with probable errors. For service providing equipment, since monitoring streams is a real-time activity that touches the mainline of packet forwarding, the complexity is added directly to the part of the system that can least afford added complexity. If the monitoring is provided in off-line equipment that is monitoring the communications then the system can be optimized for monitoring and filtering functions without necessarily affecting service to customers.

~~7.4.2.10~~6.2.2.17 Points of Intercept

The point of intercept for an IP transport provider would preferably be as close to the edge of the network. The closer to the core of the network, the heavier the traffic flows and the more random the traffic patterns.

The point of intercept should be flexible based on the provider's network design and equipment capabilities. The following are possibilities:

> One location for the Point of Intercept is the first equipment that routes the target's traffic. Another location is an aggregation router through which the target's traffic flows. However, as discussed previously, performing packet monitoring an delivery from equipment that is providing service to a customer detracts from the resources available to service customers.
>
> Another Point of Intercept is within the access POP for the provider. The raw packet stream can be provided via a port on a POP switch (e.g., ethernet switch) or via a line monitor. Non-service providing equipment can be used to take the raw packet stream as input and provide the required CALEA information as output.

No matter where the Point of Intercept is located, some correlation has to be provided to correlate the target's current IP address with the surveillance stream.

~~7.4.3~~6.2.3 Frame Relay

~~SDO Lead:~~

~~Contact: Dave Hoffman~~

~~1.Frame Relay~~

This section describes Frame Relay (FR) technology and its use in transporting voice telephony. It concentrates on the public network where FR is predominately used to transport packetized data. Traditionally FR has been used to transport LAN to LAN and legacy traffic such as bisync and SNA. Recently, non-traditional uses (Voice over Frame Relay [VoFR]) have begun to materialize.

Early transport of packetized data made use of X.25. X.25 includes considerable overhead that Frame Relay was designed to overcome. The major differences between X.25 and Frame Relay are:

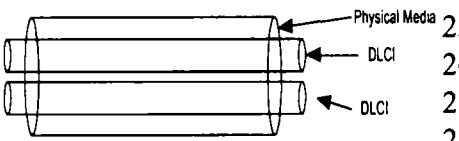
- Logical connection multiplexing and switching takes place at Layer 2 rather than Layer 3.
- Frame Relay leaves end-to-end flow and error control to upper layers
- User data and call control signaling are carried on separate connections.

The advantage of Frame Relay lays in the fact that the communication process has been streamlined to take advantage of modern transmission systems that are less prone to error. By lowering the overhead necessary to transport data, increases in throughput and decreases in delay have been realized.

Flag 1 octet	Address 2-4 octets	User Data Variable	FCS 2 octets	Flag 1 octet

Frame Relay switching is best understood by examining the frame format:

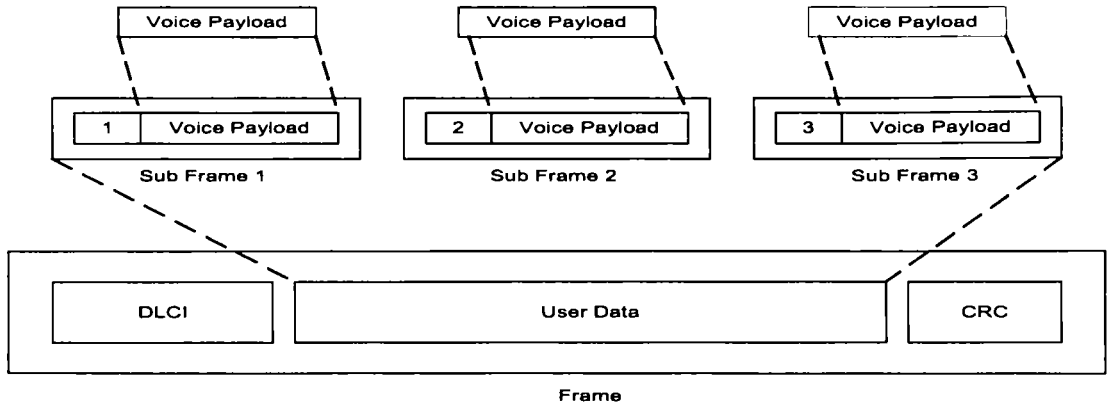
The address field has a default length of 2 octets, but can be extended to 3 or 4 octets. Included in the address filed is the data link connection identifier (DLCI) that is used to define the virtual circuit number. This arrangement allows for the multiplexing of many virtual circuits onto a single physical media.



Voice over Frame Relay (VoFR) offers the promise of consolidating data and voice traffic over the same Frame Relay network. Recent advances in Frame Relay features, specifically to support real-time services such as voice, have made Frame Relay an attractive alternative for carrying voice traffic. The Frame Relay Forum introduced the Voice Over Frame Relay Implementation Agreement (FRF.11) in December 1998.

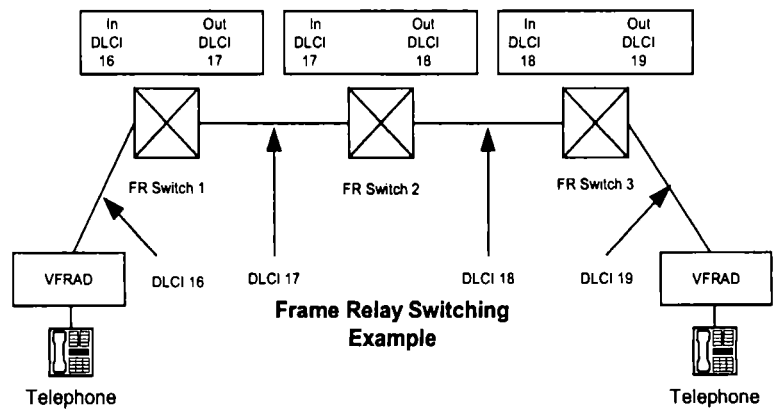
The Voice Over Frame Relay Implementation Agreement (FRF.11) includes features to support real-time transport of voice traffic over a Frame Relay network. Service Multiplexing, defined in FRF.11 is a feature that allows for the multiplexing of many voice circuits onto a single VoFR DLCI. The relationship

between voice payload sub-frames and Frame Relay frames is illustrated in the following diagram:



Each sub-frame carries a Sub Channel Identifier that identifies the voice payload sub-frame that is used to carry each individual voice channel.

A Voice Frame Relay Access Device (VFRAD) accomplishes encapsulation of voice traffic into frames. A VFRAD is positioned between a PBX or key set and the Frame Relay network. The VFRAD multiplexes voice, fax and data from a variety of sources into a common Frame Relay connection. In addition, the VFRAD can provide other services such as compression, encryption, silent suppression, etc. Using voice compression, up to 255 voice sub-channels can be multiplexed within a single Frame Relay DLCI. Addressing is accomplished in VoFR by the transmission of binary representations of dual tone multi-frequency (DTMF). Many aspects of VoFR implementations are left to vendor specific implementations.



As frames arrive at the ingress to the network, the Frame Relay header is examined to determine the DLCI. The DLCI value is mapped to an outgoing facility, which may use a different DLCI. Note that the DLCI value has only local significance. Each end of the Frame Relay connection can, and probably

will utilize a different DLCI value. Nothing about the DLCI value at any node in the network identifies the final destination of the frame and the user data that is being transported.

At no time during the transport of user data does the Frame Relay switch examine the user data to determine anything about the nature of the upper layer protocols, including the nature of voice traffic being transported. The voice sub-channels that are being carried within the DLCI have significance only at the edges, where they are de-multiplexed by the VFRAD.

It is not technically feasible to examine the user data that is being switched by the Frame Relay switch. Switching nodes are designed to relay the frames as quickly as possible. This design effectively prohibits the Frame Relay switch from examining the user information encapsulated within the frame due to the processing and implementation that would be required. Due to the vendor specific implementation of most aspects of VoFR, having the ability to examine the voice payload could be a moot point because of proprietary compression and encryption.

~~*7.5*~~*6.3* ~~*Application layer protocols:*~~

~~7.5.1SIP~~

~~SDO Lead:~~

~~Contact:~~

~~7.5.2 H.323~~

~~SDO Lead:~~

~~Contact:~~

---

[i] FCC 99-230, *Third Report and Order (In the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (FCC, August 31, 1999).

[ii] ANSI, J-STD-025, *Lawfully Authorized Electronic Surveillance*, TIA, December 8, 1997.

[iii] Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, Notice, Federal Register, Vol. 63, No. 48, March 12, 1998.

[iv] TR-45, J-STD-025A, *Lawfully Authorized Electronic Surveillance*, PN-4465, April 2000.

Capitol Hill hears about wiretapping

By FRED BAKER
Network World Fusion, 04/10/00

Congress last week held hearings about whether law enforcement should be able to implement wiretapping via the Internet.

"The Internet offers new ways to engage in communication and commerce, but it also gives thrid parties unprecedented abilities to compile and search data on every person who uses it," says Rep. Bob Barr (R-Ga.), who requested the hearing. "These hearings will provide information that will help Congress do a better job of balancing civil liberties and crime prevention in the Internet age."

Hosted by the Judiciary Committee's Constitution subcommittee, the hearings featured testimony from Fred Baker, chair of the Internet Engineering Task Force, Internet Alliance Director Jeff Richards, Center for Democracy and Technology Counsel Jim Dempsey and other experts on the law and the Internet.

--By Carolyn Duffy Marsan

Here's the testimony Baker presented:

Report on the Raven Process

More Info
Connect to additional info on this topic.

Feedback
Tell us your thoughts on this article or the issues it raises.

Today's News
Women, minorities could solve the country's critical shortage of high-tech workers
What lies ahead for WorldCom and Sprint?
WorldCom hit by 'Net problem
Exchange 2000 delayed

Wiretap discussions

With the publishing of RFC 2804: "IETF Policy on Wiretapping", it would be worthwhile to report and ruminate on the process and its conclusions. The reader should understand that these notes are the personal thoughts of their author, and not necessarily the opinion of anyone else. But they reflect that discussion as seen by one who participated in it.

These ruminations should not surprise those who are familiar with the IETF and its processes, but others may find them interesting and useful to understand, as the process and outcome seemed to surprise others. The IETF is not a lobbying or political organization in that sense, but the discussion and outcome unavoidably have distinct political ramifications. The reasoning and outcome may therefore be useful inputs to those who engage in political discussion and debate.

The IETF was approached, by engineers building equipment for Internet Telephony, with a suggestion that it should add features to a specific protocol to support what is known as "legal intercept", or wiretapping. This triggered a debate within the working group, which was reflected to IETF leadership, and ultimately became a discussion involving much of the IETF.

At this point, it would appear that people whose primary interest was not in the Internet, but in Civil Liberties, also joined the debate and conducted much of it. The IETF received a fair bit of free advice, not all of which reflected an accurate knowledge of the relevant laws or the technical considerations. But in the end, the discussion resulted in a viewpoint that the IETF accepted, according to the rule of "rough consensus."

The IETF considered a number of legal theories and national laws. Much of the discussion centered on a U.S. law known as the Communications Assistance to Law Enforcement Agencies (FCC doc. CC Docket No. 97-213), or CALEA, and some discussants tried to challenge viewpoints supporting wiretap in CALEA-

delayed
European official vows to go forward with U.S. data-privacy deal
All of today's news

Compendium
Indian politician to IT: Go away
Plus: Nerdpops and the gallery of half-baked ideas.

Webcast
Hacking back
Is cyber-vigilantism justified? Watch our live Webcast today, 1 p.m., EDT.

Test Pilots
User reviews
HP Jornada 690 beats the Palm; Gyromouse rules in presentations; more.

This Week
Printing to get 'Net facelift
Ethernet and IP storm factory nets
Vendors to speed Web content delivery
My breakfast with David
Editor in Chief John Dix recently met with David Oran, a Cisco Fellow.
More news, reviews and features from Network World

Webcast
Hacking back
Is cyber-vigilantism justified to protect

centered language. This was helpful in understanding that particular law, which is complex, but also led the discussion to ignore the range of laws.

Two examples suffice to demonstrate the range of laws concerning legal intercept. Most countries practice wiretap under some circumstances to gather evidence of criminal behavior. In Sweden, it is illegal to attribute a statement to a person in electronic mail, or to refer to him by name, without his consent, and in general wiretap is strongly supported in the law of the European Community. In the People's Republic of China, on the other hand, there is little or no inhibition on government surveillance of its citizens – or its visitors.

If the IETF were to establish protocol procedures for the systematic interception of communications – regardless of whether done for valid law enforcement objectives or more sinister policing of free thought – it would have to do so in a way that met the specific requirements of law in every country the Internet is deployed in. This is obviously a complex and exacting requirement.

The IETF has considered wiretap questions before, notably when it considered a procedure known as Key Escrow or Key Recovery. In that case, it documented the result of its discussion in RFC 1984: "IAB and IESG Statement on Cryptographic Technology and the Internet", the number for which is indicative of the viewpoint it expresses. But in this case, the IETF leadership felt that it should have its final discussion, presenting a viewpoint that would guide it for the foreseeable future. The mailing list, and the discussion that took place on it, took its name from Poe's Raven, which said "Nevermore!".

The issues in wiretapping

In any country, the government has two fundamental objectives: to make and enforce its laws, and to preserve and protect its citizens. To the extent that it fails in either objective, it is undermined; if it cannot enforce its laws, they are meaningless, and if it cannot protect its citizens, it

meaningless, and if it cannot protect its citizens, it is only a matter of time until it is replaced. It is common (although not universal) for the citizens to accept that the government must do some things, that no citizen would do, in pursuing those objectives, among which are the surveillance of its citizens.

At the opposite extreme are criminals, which may view their activities as anything from a quick way to make a profit to a business that requires unusual protections. In general, they view their activities as deserving secrecy and protection.

A problem that the citizen faces is that sometimes he is caught in government's net for criminals, or runs afoul of some other "official purpose". This is the reason we have courts – to evaluate evidence and determine whether law enforcement has successfully caught a criminal. The citizen's perspective tends to be that government has no legitimate reason to investigate him, as he is not knowingly in violation of any law. He quickly becomes concerned when the government approaches. In the words of Tevye's Rabbi's blessing on the Czar, "May God bless and keep him, far away from us!"

The problem at the heart of the Raven discussion was the limits on law enforcement, including both the investigative equivalent of drift net fishing and the unwarranted targeting of individuals, and the availability of the technology, once deployed, to extra-legal interests such as industrial espionage.

The proposals

Several proposals have been made which enhance law enforcement's ability to gather intelligence and evidence on criminal activity in a world filled with computers. These include, at minimum, Key Escrow (also known as Key Recovery), Legal Intercept, banning or licensing of the export of encryption, and the outright ban of encryption.

Key Escrow

The premise underlying Key Escrow is a simple and seductive line of reasoning. If a person uses

encryption to secure his data or his communications, clearly he is doing little more than throwing away his information unless he manages to remember the encryption key. This being the case, it is in a business's interest to maintain a copy of its employee's keys in some way in order to avoid losing their work when the person leaves the company, and the key is available to a court's subpoena. Why not enforce their escrow in some place that the government potentially has access? If one does this, then the legitimate interests of government are supported, should encryption be used to hide a crime or plans to commit one.

There are a number of issues that this raises. Some of them are business and technical issues; the key and the database that stores it are potentially expensive and sensitive resources. In the United States, where wiretapping is only legal for telephony, one wonders why the proposals suggested the escrow of keys for data, although in other countries, such as the United Kingdom, any information is essentially fair game. There are questions of the technology supporting the database. If every access of the data requires an access of the database to obtain the key, two problems result. The repeated key transfer itself creates an opportunity for the illicit recovery of the key by an unauthorized person, and the necessity for the key transfer slows down access to the protected data by the time required to access the key from the network database. The simple solution, of course, is to maintain the key locally, but then the database is defeated, because there is no assurance that every key is in the database.

Beyond that, once a key escrow database or key recovery procedure has been instituted, the key is potentially available to anyone, and once a key has been obtained it is permanently known and all documents it protects are permanently accessible. Legitimate government interests may obtain it with a warrant, of course. In so doing, they cannot but obtain overbroad results due to the fact that the key applies to more data than the warrant requires, or force the corporation to have a separate key for every communication and document, which is a costly and time consuming

process. But corporate competitors and gangsters may also obtain it by corrupting or blackmailing the people who maintain the database, or by breaking into the computer that holds it. As a result, the information itself, theoretically secured by encryption, is no longer secure. Placing all the keys into one database, even a distributed one, makes the database all the more tempting (and insecure) a target for those who would violate it.

This loss of security and availability of the key undermines the fundamental purpose for which law enforcement sought access to the key. Because the key has potentially become available to anyone willing to exercise himself to obtain it, it has again become possible for a forger to store data or send messages in the name of the user of the key. As a result, the use of the key to encrypt information is no longer prima facie evidence that the owner of the key is a criminal. But it is precisely this – to gain intelligence about criminals and criminal activity and in the end convict criminals – which motivated law enforcement to request the escrow of the key.

There is one final question: a key issue is that Key Escrow demeans the society's view of the citizen. Consider what one does in building a home. One puts a door on the entry, and a lock on the door, because the owner of the home believes that there are some people who should knock on the door before entering the home. Does the owner then make a copy of the key to the lock and present it to the local magistrate, saying "should you ever decide that I may be a criminal, here is the key so that you may search my home"? Of course he does not, and his reason is that no government views its citizens as criminals that have not been caught yet – it views them rather as members of its constituency which may occasionally become criminals. If this is true of the door on the home or place of business, why would it be less true of the computer located in the home or place of business? If our home and business are themselves increasingly found on the disk drive, to not extend it the protections of the fourth amendment borders on the bizarre.

Legal intercept

Most, perhaps all, governments tap telephones to gather intelligence on criminals and criminal activity and other sanctioned purposes. An important part of the procedure is that the person being monitored has no knowledge of the tap; if he did, he might alter his behavior. Therefore that tap is invariably placed somewhere out of his control, usually in a telephone company office. This procedure has not always been universally accepted. In the United States, wiretap evidence was not acceptable to a court until the Telecommunications Act of 1967; prior to that wiretap was unregulated and was not accepted as evidence in court. However, in many countries, wiretap by law enforcement is a normal and accepted procedure. The extension to the Internet is obvious: if the modes of communication change, why would common procedures not be extended to the Internet?

A fundamental problem is that the nations have not agreed to a common law concerning wiretap. Some tap everything, some tap only voice, and depending on the terms of a warrant one may get various kinds of information in different ways. As a result, in the worst case, multinational vendors are forced to consider wiretap law on a nation by nation basis, creating slightly different software and perhaps hardware for sale in each nation.

The technical issues in wiretap are not in identifying or copying the information. While not free, this is relatively straightforward; the one question would be to what extent deployed equipment would have to be upgraded to support it and what the implications of that upgrade would be. The more substantive technical issues revolve around the fact that although tapping an Internet session is not fundamentally different than tapping a telephone session, Internet technology does not mirror telephone technology, around which procedures and laws for legal intercept are designed.

The Internet equivalent of a pair of alligator clips involves a management action on a computer that is normally owned or operated by the person whose data one wants to intercept. This is because Internet data is a stream of messages addressed from a process on a computer to a process on

another computer, but there is no concept of a personal owner of that data stream anywhere in the network other than on those two computers. Multi-user computers, are common, and even single user computers such as laptops and mobile telephones are frequently available to multiple users serially - the computer the author is writing this article on is occasionally used by his family to send electronic mail or look up material on the web. So if someone is tapping a data stream in order to find out what a person is thinking or saying, apart from access to the end systems in the conversation, he cannot determine which person originated the data stream. As a result, either Internet wiretap requires us to enable law enforcement to successfully hack any computer in the Internet (a fact that hackers would welcome), or results beyond those in any well-defined warrant are highly likely.

The most basic issue is one of intent. Security issues concerning Internet technology, which may be viewed as a research experiment that escaped the laboratory, have been raised in recent years. The engineering and business community that operates the Internet is working diligently to improve that security. This includes assuring that message switching equipment cannot be compromised, that end systems cannot be compromised by hackers and crackers, and that electronic commerce is supported by authentication and encryption technologies which incontrovertibly trace an exchange back to a source. Enabling random persons to gain management access to computers - whether corporately owned or privately owned - and message switching equipment, reroute or duplicate its data exchanges, and generally access its contents is clearly a direct weakening of that security infrastructure. As hackers have repeatedly demonstrated, it is possible for someone to gain control of sensitive computers, change financial records, modify web pages, forge messages, and even retarget military assets. Is it in the best interest of the state or of the Internet to deliberately weaken security and allow uncontrolled management access to computers? But this is precisely what is required to implement Legal Intercept, as currently defined, in the Internet.

Making encryption technology illegal to sell to some countries

The COCOM treaty has been invoked over the past thirty years to prevent the sale of encryption technology across certain borders and to generally license it. The theory is, of course, that the technology is a munition that does not exist in the targeted country, and by not selling products containing encryption to the country one denies the country access to it. In another century, when bodies of water and armed guards controlled borders and theorists had difficulty communicating, this was a reasonable theory. However, in computer technology and especially in the Information Age, this has become trivial to bypass. The technology may be developed or redeveloped in the targeted country in several ways. To begin with, many countries have their own cryptographic research. If a particular nation's technology if of interest, a traveler can purchase a book and return home, or the equivalent web page can be accessed. A recent decision by the US Federal Courts calls rulings that prevent the discussion and spread of the technology prior restraint of the freedom of speech. A necessary result is that the implementation can be done in the country to which the product may not be exported. COCOM export restrictions are therefore protectionist legislation which one country enacts to favor industry in another, something that boggles the mind.

Banning encryption

Some countries go as far as to ban the use of encryption entirely. This approach, of course, makes the entire concept of Key Escrow moot, and can only be supported if one starts from the assumption that all information is available to random wiretap. It therefore has all the problems of Key Escrow and Legal Intercept, and no definable controls. It only makes sense in a country which fundamentally views its citizens as untrustworthy, which is an interesting observation given the stated ideals of some of the countries which take this course.

But this approach has a bigger problem in the Internet. If encryption is unlawful to use at all, it is unlawful to use to secure the Internet infrastructure, and the insecurity of the Internet is enshrined in law. This observation calls for sober consideration.

IETF decision on wiretap, and specifically on legal intercept

The IETF believes that strong privacy, implemented using strong authentication or encryption, is important for the development of Internet commerce and for the safety of both the infrastructure and its users. The IETF itself makes no statement on law, and its specifications are used throughout the world to build a single global network.

Obviously, nations are sovereign, and can pass any laws they like concerning the use of that technology within and across their borders. For the IETF to try to stop that from happening would be futile, and for the IETF to try to develop one comprehensive specification that supports the wiretap laws of every country would be an impossibly complex undertaking. In essence, the IETF concluded that these are national matters and are best left to national bodies.

That observation, however, sidesteps some very difficult legal, societal, and technical problems which the members of the IETF community see, and which this article has attempted to expose. Having observed on them, the IETF is of the opinion that this discussion must continue in venues better suited to it. But the issues are very troubling to the IETF community at large.

The IETF understands that this viewpoint is not helpful to law enforcement interests. It observes that in at least the western democracies, the job of law enforcement is intentionally difficult, and that the rights of the citizen are not normally traded away for the ease of law enforcement. To quote two men who have arguably shaped part of that line of reasoning,

They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.
Benjamin Franklin, 1759

Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves.
William Pitt

In essence, we observe that the concept of a border has changed dramatically over the past decade. A national border used to be a boundary that controlled trade, the transference of people, ideas, and information, and which could be guarded - and was regarded as something that should be guarded - by oceans, walls, and men with guns. With the explosive deployment of communications technology, however, it has become the edge of a legal jurisdiction that is transparent to the communication of information and arguably creates more trouble than it avoids.

Recognizing this, the nations of Europe are coalescing into a European Community with open internal borders and a set of states that with open borders to the European Community. Recognizing this, the North American Free Trade Zone is (at least in theory) lowering barriers to commerce and communication across borders. Recognizing this, financial managers increasingly talk not about geographically and politically separated commercial zones, but about a single global economy with many interdependent parts. It is no longer obvious that governments can or should inhibit the flow of information, as the ultimate responsibility for the information and its use is increasingly forced to rest in the hands of the citizen.

Related links

Baker is chairman of the IETF. He can be reached at intheworks@nww.com.

IETF nixes wiretapping, eyes wireless
Network World, 03/27/00.

Tapping the 'Net

Scott Bradner on the issue. Network World, 11/29/99.

IP telephony tops IETF agenda
Network World, 11/8/99.

IETF - security savior or privacy violator?
Network World on Security newsletter, 10/25/99.

Forum: Internet wiretapping
What do you think? Add your thoughts.

To top

Send this article to a colleague

Recipient's name: Your name:

Recipient's e-mail: Your e-mail:

Comments:

Mail

Feedback

Tell us your thoughts on this article or the issues raised in it. We'll cc: the author and editors on all comments.

Comments:

Name:

E-mail address:

Can we post your comments in an online forum on the topic?

○ Yes ○ No

What did you think of this article?

○ Very useful ○ Somewhat useful ○ Not at all useful

Would you want to see:

○ More articles on this topic

○ Fewer articles on this topic

Submit

Thank you! When you click Submit, you'll be taken back to this article.

Home
Contact us
Site Map
Today's news
This week in NW
Research
Free newsletters
Forums
Opinions
Careers
Terms of Service
Network World, Inc.
Seminars & Events
Advertiser Index
Product Showcase
Vendor white papers
How to Advertise
NW Subscriptions

OMB Control Number: 1110-0030
Expiration Date: June 30, 2000

Communications Assistance for Law Enforcement Act - CALEA

Flexible Deployment Assistance Guide

Department of Justice
Federal Bureau of Investigation
CALEA Implementation Section
January, 2000

TABLE OF CONTENTS

INTRODUCTION

The purpose of this "Communications Assistance for Law Enforcement Act (CALEA) Flexible Deployment Assistance Guide" (Guide) is to assist telecommunications carriers in meeting certain requirements of CALEA.[1] This Guide requests telecommunications carriers to voluntarily submit certain information to the Federal Bureau of Investigation (FBI), and explains under what circumstances, based on a review of that information, the FBI might support a carrier's request to the Federal Communications Commission (FCC) for an extension under Section 107(c) of CALEA.[2] The Guide also provides some general background information regarding CALEA, and discusses lawfully-authorized electronic surveillance, technical solutions being developed by the industry, and cost reimbursement provisions of CALEA.

As explained further in the Guide, telecommunications carriers are under an obligation to meet certain CALEA assistance capability requirements by the June 30, 2000 and September 30, 2001 deadlines specified by the FCC. The "Flexible Deployment Plan" is the FBI's proposed method for evaluating the situations of those carriers proposing to request the FCC for an extension of a deadline of compliance with CALEA's assistance capability requirements. Carriers choosing to submit information in response to the Guide are strongly encouraged to do so on or before March 31, 2000.

If, after reviewing the information submitted, the carrier and the FBI are able to arrive at a mutually agreeable CALEA deployment schedule, the FBI would not oppose the carrier's request to the FCC for an extension, provided that the carrier then proceeded with its deployment in accordance with the schedule. An agreed-to deployment schedule could benefit both parties in many ways, including avoiding a dispute before the FCC regarding an extension request. The FCC has stated that it would accord "significant weight" to such an agreement, in determining whether to grant an extension to a carrier.[3] Carriers should note, however, that the ultimate decision on any extension rests solely with the FCC.

What is Electronic Surveillance?

Lawfully-authorized electronic surveillance is a law enforcement tool that police and other authorized government agencies use to investigate and prosecute criminals. Its use by such agencies is strictly limited by law. Lawfully-authorized electronic surveillance is a law enforcement agency's or organization's collection of either (1) the content[4] of any communication sent by or to a subject of surveillance; or (2) the dialing or signaling information that identifies the origin, direction, destination, or termination of any communication generated or received by a subject of surveillance by means of any equipment, facility, or service of a telecommunications carrier.

In 1968, Congress carefully considered and passed the Omnibus Crime Control and Safe Streets Act (Pub. L. No. 90-351, 82 Stat. 212) which laid out the meticulous procedures law enforcement must follow to obtain the necessary judicial authorization to conduct electronic surveillance in the fight against crime. The law was enacted after Congress exhaustively debated issues concerning law enforcement's need to effectively address serious criminal activity and an individual's right to privacy.

In 1970, Congress amended the federal wiretap statute to require providers of communications services to provide law enforcement with the ". . . technical assistance necessary to accomplish the intercept . . ."[5] In the old telecommunications environment, only minor assistance from telephone companies was needed by law enforcement to accomplish the interception (e.g., identity of "access points," etc.). However,

---

[1] See 47 U.S.C. §1001, et seq.; see also CALEA Cost Recovery Regulations, 28 C.F.R. Part 100; Final Notice of Capacity: Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, Notice, 63 Fed. Reg. 12217; Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act, *Memorandum Opinion and Order,* 13 FCC Rcd 17990; Second Report and Order, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (rel. August 31, 1999); and Third Report and Order, *Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213 (rel. August 31, 1999).

[2] The FBI believes that submission of the requested information by a carrier could facilitate a mutually beneficial agreement between the FBI and the carrier. However, carriers should be aware that submission of information in response to this Guide is completely voluntary; and does not create any legal obligation on the part of the Federal Government or the carrier. The Guide is not intended to make any offers nor provide legal advice. If carriers have any questions regarding their legal obligations under CALEA they should consult their own legal advisors.

[3] See Second Report and Order, *Communications Assistance for Law Enforcement Act*, CC Docket No., 97-213 (rel. August 31, 1999), ¶ 37, n.100.

[4] The content of communications applies to any type of wire or electronic communications sent by or to the subject of lawfully-authorized electronic surveillance (i.e., any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature).

[5] 18 U.S.C. § 2518(4).

in today's telecommunications environment, greater assistance is necessary because newer and more advanced telecommunications technologies, services, and features are now being offered by service providers.

In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA, 50 U.S.C. §§ 1801-1843) to safeguard national security by authorizing select government agencies to conduct electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information. Section 1805(b)(2)(B) of FISA requires that common carriers 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.

In 1986, as a result of developments in telecommunications and computer technologies, Congress found it necessary to enact the Electronic Communications Privacy Act (Pub. L No. 99-508, 100 Stat. 1848), which amended the Omnibus Crime Control and Safe Streets Act by broadening its coverage to include electronic communications (including electronic mail, data transmissions, faxes, and pagers). The provisions of Title III of the 1968 Act, as amended, continue to govern the procedures for obtaining legal authority for initiating and conducting lawful interceptions of wire, oral, and electronic communications.

Types of Electronic Surveillance

For the purpose of this Guide, lawfully-authorized electronic surveillance is considered to consist of both the interception of communications content (commonly referred to as wiretaps) and the acquisition of dialing and signaling information used to identify a call (dialed number information) through the use of pen registers and/or through the use of trap and trace devices.

The interception of communications, or *call content* surveillance, applies to the provision of actual information (e.g., signs, signals, writing, images, sounds, data, or intelligence of any nature) transmitted from one party to another. Authority for initiating a call content surveillance is found in Title III of the Omnibus Crime Control and Safe Streets Act or FISA.

The term *pen register* applies to the recovery and recording of the dialing information that addresses a call from an intercept subject. Authority for initiating a pen register surveillance can be found in 18 U.S.C. § 3123 and 50 U.S.C. § 1842.

The term *trap and trace* applies to the acquisition of an incoming, originating number of any wire or electronic communication. Authority for initiating a trap and trace surveillance can also be found in 18 USC § 3123 and 50 U.S.C. § 1842.

What is CALEA?

In October 1994, Congress again took action to protect public safety and national security by enacting CALEA, (Pub. L. No. 103-414, 108 Stat. 4279). The law clarifies and further defines the existing statutory obligation of providers of telecommunications services in assisting law enforcement in executing electronic surveillance court orders.

CALEA does not change or expand law enforcement's fundamental statutory authority to conduct various types of electronic surveillance. It seeks to ensure that after law enforcement obtains the appropriate legal authority, telecommunications carriers will have the necessary technical capability and sufficient capacity to fulfill their statutory obligations to assist law enforcement. In many instances, telecommunications carriers have neither the capability nor the capacity to handle all electronic surveillance court orders.

CALEA sets forth, in law, the assistance capability requirements that telecommunications carriers need to meet and maintain within their networks to assist law enforcement in conducting lawfully-authorized electronic surveillance. Specifically, CALEA directs the telecommunications industry to design, develop, and deploy solutions that meet specific assistance capability requirements.[6]

CALEA also recognizes that some existing equipment, services, and features would have to be retrofitted and includes a provision by which the Attorney General could reimburse the industry for modifications made to equipment, facilities, and services installed or deployed on or before January 1, 1995.

[6] Section 103 of CALEA, 47 USC § 1002.

Important CALEA dates

October 24, 1994 - Date of CALEA enactment

January 1, 1995 - Reimbursement eligibility date for equipment, facilities, and services installed or deployed in a carrier's network

October 25, 1998 - Original CALEA assistance capability compliance date

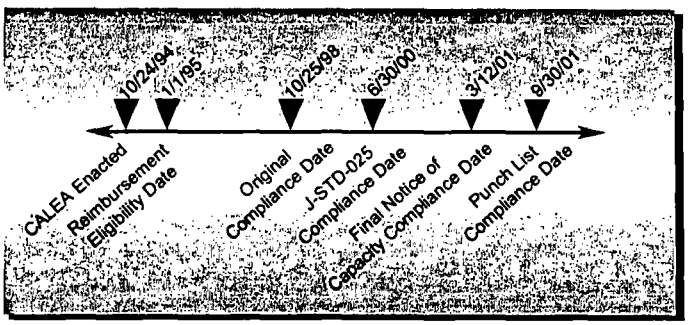


Figure 1 - CALEA Timeline

June 30, 2000 - New compliance date for Section 103 assistance capability requirements for all telecommunications services and technologies (e.g., Telecommunications Industry Association [TIA] interim technical standard J-STD-025 for wireline, cellular, and broadband Personal Communications Services [PCS])

March 12, 2001 - Compliance date of carriers providing local exchange, cellular, and broadband PCS services for capacity requirements as enumerated in the Final Notice of Capacity (63 Fed. Reg. 12217)

September 30, 2001 - Compliance date for wireline, cellular, and broadband PCS to comply with the additional assistance capability requirements as determined by the FCC[7]

TECHNICAL SOLUTION

CALEA was enacted to ensure that ongoing technological changes in the telecommunications industry would not compromise the ability of federal, state, and local law enforcement agencies to conduct lawfully-authorized electronic surveillance. To that end, CALEA obligates telecommunications carriers to ensure that their equipment, facilities, and services are technically capable of expeditiously isolating and delivering to law enforcement agencies all communications content and call-identifying information that law enforcement is authorized to acquire.

Several years before the passage of CALEA, law enforcement began meeting with individual telecommunications companies, as well as industry forums such as the Electronic Communications Service Provider (ECSP) Committee. A primary objective of those meetings was to develop a common understanding of law enforcement's surveillance requirements and to explore options by which a network-based or switch-based interception might be implemented. The ECSP Committee, with law enforcement's endorsement, brought electronic surveillance requirements and issues to the attention of industry standards-setting organizations such as the TR45 and TR46 Committees of TIA.

In May 1995, TIA's TR45.2 Subcommittee formed the Lawfully Authorized Electronic Surveillance (LAES) Ad Hoc Group. Its mission was to develop a technical electronic surveillance standard detailing what information should be accessed to support lawfully-authorized electronic surveillance and how intercepted communications and call-identifying information should be delivered by a telecommunications carrier to a law enforcement agency. In late 1995, PCS and wireline standards bodies agreed to work with the TR45.2 group, which normally represents the cellular industry, on a standard for wireline and wireless networks.

Core J-Standard

On December 8, 1997, TIA published an interim technical standard[8] (J-STD-025, or J-Standard) concerning electronic surveillance assistance capability requirements for telecommunications carriers providing wireline, cellular, and broadband PCS. J-STD-025 describes advanced electronic surveillance capabilities intended to provide law enforcement the ability to collect call-identifying information and call content pursuant to lawful authorization.

[7] On August 31, 1999, the FCC adopted its Third Report and Order regarding the assistance capability requirements of CALEA. In it, the FCC determined that the industry's interim technical standard did not contain all the assistance capabilities required by CALEA.

[8] An interim technical standard was jointly published by TIA and Committee T1 (sponsored by the Alliance for Telecommunications Solutions) as J-STD-025, *Lawfully Authorized Electronic Surveillance*.

The original assistance capability compliance date for CALEA, October 25, 1998, was extended by the FCC[9] for J-STD-025 to June 30, 2000. The FCC determined that carriers could not comply with the original October 25, 1998 compliance date because of the absence of available technology during the compliance period.

Missing Capabilities

On March 27, 1998, the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) filed a joint petition before the FCC. The DOJ/FBI petition argued that the industry's J-STD-025 was deficient in that it failed to include nine capabilities determined by DOJ as necessary to meet the requirements of this law.

On August 31, 1999, the FCC released its Third Report and Order, regarding Section 103 assistance capability requirements.[10] The FCC determined that, in addition to the assistance capabilities included in J-STD-025, wireline, cellular, and broadband PCS carriers must provide *six* additional assistance capabilities sought by the DOJ and FBI.[11] These assistance capabilities must be implemented by September 30, 2001.

The six capabilities determined by the FCC to be required by CALEA are:

- Content of subject-initiated conference calls
- Party Hold, Join, Drop messages
- Access to subject-initiated dialing and signaling
- In-band and out-of-band signaling (Notification Message)
- Timing to associate call data to content
- Dialed digit extraction (post-cut-through dialed digits)

For a description of each of the six capabilities outlined above, please refer to Appendix C.

[9] Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act, *Memorandum Opinion and Order,* 13 FCC Rcd 17990.

[10] Third Report and Order, *Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213 (rel. August 31, 1999).

[11] See *In the Matter of Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities under the Communications Assistance for Law Enforcement Act,* Public Notice, CC Docket No. 97-213, DA 98-762, (rel. April 20, 1998) (encompassing petitions filed by CDT, TIA, CTIA, and DOJ/FBI).

Location Information

J-STD-025 includes a *location* capability that is intended to provide law enforcement, where authorized, with the location of a subject of lawfully-authorized electronic surveillance. The information regarding the location of a subject is limited to the cell site of the subject's terminal only at the beginning and end of a call. Under the law, this information is not available when a law enforcement agency is acting solely under the authority of a pen register order.

In its Third Report and Order, the FCC determined that ". . . a subject's cell site location at the beginning and end of a call is considered call-identifying information under CALEA."[12] Further, the FCC required that this capability be deployed by telecommunications carriers by the previously established June 30, 2000 CALEA compliance date.

Packet Mode Communications

J-STD-025 provides law enforcement the capability to access call-identifying information regardless of the transmission mode (circuit-switched or packet-mode) utilized by carriers in providing service.

In its Third Report and Order, the FCC determined that carriers could provide the capability to intercept packet-switched communications in accordance with J-STD-025. The FCC mandated that the capability to intercept packet-switched communications be made available by September 30, 2001. The FCC also invited TIA to study alternative technical solutions that would provide for separated delivery of call-identifying information and communications content.

REIMBURSEMENT

To facilitate CALEA's implementation, Congress authorized $500 million to be appropriated to reimburse the telecommunications industry for certain eligible costs associated with modifications made to their networks. Section 109 of CALEA grants the Attorney General discretionary authority to allocate appropriated funds in a manner consistent with law enforcement priorities, and mandates the Attorney General to establish the necessary regulations to effectuate timely and cost-efficient payment to telecommunications carriers. The reimbursement of carriers for any eligible costs will occur under the provisions of Section 109 of

[12] Third Report and Order, *Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213 (rel. August 31, 1999), ¶ 44.

CALEA and the associated Cost Recovery Regulations,[13] and is in no way altered by a carrier's submission of information in response to this Guide.

The Omnibus Consolidated Appropriations Act of 1997 (P.L. 104-208)[14] amended CALEA by adding Title IV which created the Telecommunications Carrier Compliance Fund (TCCF). The purpose of the TCCF is to facilitate the disbursement of funds available for CALEA implementation. Additionally, the Omnibus Consolidated Appropriations Act of 1997 authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF, subject to applicable Congressional reprogramming requirements.

Software

The FBI will utilize two alternative approaches for reimbursing CALEA software solutions: (1) right-to-use (RTU) license agreements, or (2) switch-by-switch reimbursement. Both approaches are designed to be consistent with the FBI's goal of maximizing return on TCCF dollars while at the same time responding to industry concerns regarding CALEA compliance costs and deployment schedules. Under the RTU license agreement approach, the FBI expects to reimburse a facilitating carrier for that carrier's purchase of the CALEA software RTU license for a switch installed or deployed on or before January 1, 1995. The license fee covers the manufacturer's CALEA software development cost for a particular switch platform type. Manufacturers are then expected to grant CALEA software RTU licenses to all other carriers at no charge for all switches of the same platform type installed or deployed on or before January 1, 1995.

In some instances, a manufacturer and its facilitating carrier partner may decline to pursue a RTU license purchase agreement with the FBI, or the FBI, manufacturer, and facilitating carrier partner may be unable to finalize an RTU license arrangement. In these cases, manufacturers will design and develop the CALEA solution in accordance with the industry's normal business practices. When a solution is available for deployment, the telecommunications market will determine the solution's price and carriers are expected to install the developed CALEA solution. Some of the installations may be eligible for reimbursement under CALEA. Under a switch-by-switch reimbursement approach, carriers will be reimbursed for CALEA software on an individual, switch-by-switch basis at solution deployment.

The reimbursement approach chosen will depend on several factors. These factors include, but are not limited to, availability of TCCF funds, the reimbursement cost for a RTU license for the CALEA solution, per-switch commercial prices for CALEA solutions, and a switching platform's priority status to law enforcement.

Software Deployment

Once CALEA software solutions have been reimbursed by the FBI, it is in the interest of the FBI and industry to minimize, to the extent practicable, the costs associated with deploying the CALEA solution in carriers' networks. The costs associated with deploying CALEA-compliant solutions are expected to be significantly reduced if carriers are allowed to incorporate the deployment of CALEA into their normal generic upgrade cycles.[15] To this end, the FBI's Flexible Deployment Plan provides the opportunity for any carrier to voluntarily supply information to the FBI so that the carrier and the FBI may cooperatively develop a CALEA deployment schedule for that carrier. These schedules may be consistent with a carrier's normal deployment processes and schedules if the schedules maximize the timely deployment of solutions on those switches that are of highest priority to law enforcement.

To accomplish this, the FBI will solicit historical electronic surveillance data from carriers in order to refine switch prioritization based on the most current intercept data available. This list of prioritized switches will be compared with normal deployment plans identified by the carrier. Carriers and the FBI may then agree on a jointly-developed deployment schedule based on this data, deploying first on law enforcement's highest priority switches. In some cases, this process may result in certain switches that were installed or deployed after January 1, 1995, not having the CALEA solution deployed by the June 30, 2000 capability compliance date. In those instances where a carrier and the FBI can agree on a deployment schedule, the FBI will support a carrier's petition of the FCC to issue limited extensions of time for compliance on specific switches installed or deployed after January 1, 1995, consistent with Section 107(c) of CALEA. The above described concept is the central tenet of the FBI's *Flexible Deployment Plan*. For more information regarding Flexible Deployment, please see the Flexible Deployment section of this Guide.

[13] CALEA Cost Recovery Regulations, 28 C.F.R. Part 100.

[14] The Omnibus Consolidated Appropriations Act of 1997; P.L. 104-208, 110 STAT 3009 (1996).

[15] For the purposes of this CALEA Flexible Deployment Assistance Guide, normal generic upgrade cycles are carrier-specific timelines of past and / or future-planned software generic deployments.

Capacity

On March 12, 1998, the FBI published in the *Federal Register* a final notice of the estimated *actual* and *maximum* number of simultaneous call content interceptions, pen registers, and trap and trace devices that law enforcement may conduct in a given geographic area. The Final Notice of Capacity,[16] with a compliance date of March 12, 2001, was published pursuant to Section 104 of CALEA[17] and applies to carriers providing wireline local exchange, cellular and broadband PCS services. The Final Notice of Capacity is also available on the FBI Web site at http://www.fbi.gov/programs/calea/capacity.htm.

In addition to the reimbursement of the cost of software, CALEA also provides for reimbursement of the reasonable costs directly associated with modifications made to any of a carrier's systems or services, as identified in the Carrier Statement required by CALEA Section 104(d), which do not have the capacity to accommodate simultaneously the number of communications content interceptions, pen registers, and trap and trace devices set forth in the capacity notice(s) published in accordance with CALEA Section 104.

In July of 1998, the FBI published a Small Entity Compliance Guide for the Final Notice of Capacity. That publication sets forth guidelines and procedures to assist carriers in complying with the Final Notice of Capacity as required by Section 104 of CALEA. The Small Entity Compliance Guide for the Final Notice of Capacity is also available on the FBI Web site at http://www.fbi.gov/programs/calea/capacity.htm.

FLEXIBLE DEPLOYMENT

The FBI's overall CALEA implementation approach includes supporting telecommunications carriers' deployment of CALEA-compliant solutions in accordance with their normal generic upgrade cycles, where such deployment will not delay implementation of CALEA solutions in areas of high priority to law enforcement. This approach is the result of the FBI's recognition of the issues facing carriers and represents an attempt to minimize the costs and operational impact of CALEA compliance on all carriers. Specifically, carriers wishing to participate in this effort may provide the FBI with their projected CALEA deployment schedules for all switches in their network, as well as information pertaining to any recent lawfully-authorized electronic surveillance activity. Using this information, the FBI and carrier will attempt to develop a mutually agreeable deployment schedule.[18] This approach is also the FBI's attempt to minimize the cost to the Government of implementing CALEA by providing the opportunity for carriers and the FBI to agree on deferring the installation of CALEA-compliant solutions in those instances where public safety and national security would not be jeopardized. Please refer to Appendix D for a high-level process overview of the FBI's Flexible Deployment Plan.

If the FBI and carrier are able to agree upon a deployment schedule, the FBI intends to provide support to an individual carrier's petition before the FCC for extensions of CALEA's June 30, 2000 and September 30, 2001 assistance capability compliance dates. In order to reach such an agreement, the FBI must have an opportunity to: (1) review and comment on proposed carrier deployment schedules, and (2) review information provided by carriers pertaining to recent lawfully-authorized electronic surveillance activity. The FBI's support of a carrier's system-wide extension petition will be conditioned upon the carrier's meeting the agreed-to deployment schedule. In addition, the FBI will request the FCC incorporate such a condition into any final decision on a carrier's extension petition. A carrier choosing not to provide information necessary for the FBI to support its system-wide CALEA deployment schedule may still petition the FCC for an extension of the CALEA compliance date(s).

Section 107(c) of CALEA

Under Section 107(c) of CALEA, a carrier is permitted to file one or more petitions with the FCC for an extension of the Section 103 assistance capability compliance deadline. The maximum extension the FCC may grant under this provision is two years. The FCC is required, by statute, to "consult" with the Attorney General prior to deciding whether to grant the extension. Under a flexible deployment arrangement, the FBI would fulfill this consultative role for the Attorney General, by providing support for the carrier's individual extension petition.

The FBI's support would be conditioned upon an agreement between the carrier and the FBI on a deployment schedule. The schedule must ensure that CALEA-compliant

[16] See *Implementation of Section 104 of the Communications Assistance for Law Enforcement Act;* Notice, 63 Fed. Reg. 12217 (March 12, 1998).

[17] 47 U.S.C. § 1003.

[18] In the event that unforeseen circumstances do not allow a carrier to deploy CALEA-compliant solutions according to the mutually agreed-to schedule, the carrier should notify the FBI as soon as possible. In the interest of public safety and/or national security, emergency or exigent law enforcement circumstances may result in the modification of a previously agreed-to schedule between the carrier and FBI.

solutions are deployed on priority equipment in the near term and that other equipment is modified within a reasonable time. Assuming these conditions are met, a carrier would then be able to deploy solutions on the lower priority equipment in accordance with its normal business cycle.

J-STD-025 CALEA-compliant solutions are to be deployed in a carrier's network (see Figure 2, below). Carriers will develop their own deployment cycles based on: (1) the commercial availability of CALEA-compliant J-STD-025 solutions; (2) market conditions and business plans; and (3) historical lawfully-authorized electronic surveillance activity (i.e., law enforcement priorities). The six-, twelve-, and twenty-four-month deployment cycles shown in Figure 2 are illustrative examples of normal generic upgrade cycles. Actual carrier generic upgrade cycles are expected to differ based on the considerations outlined above.

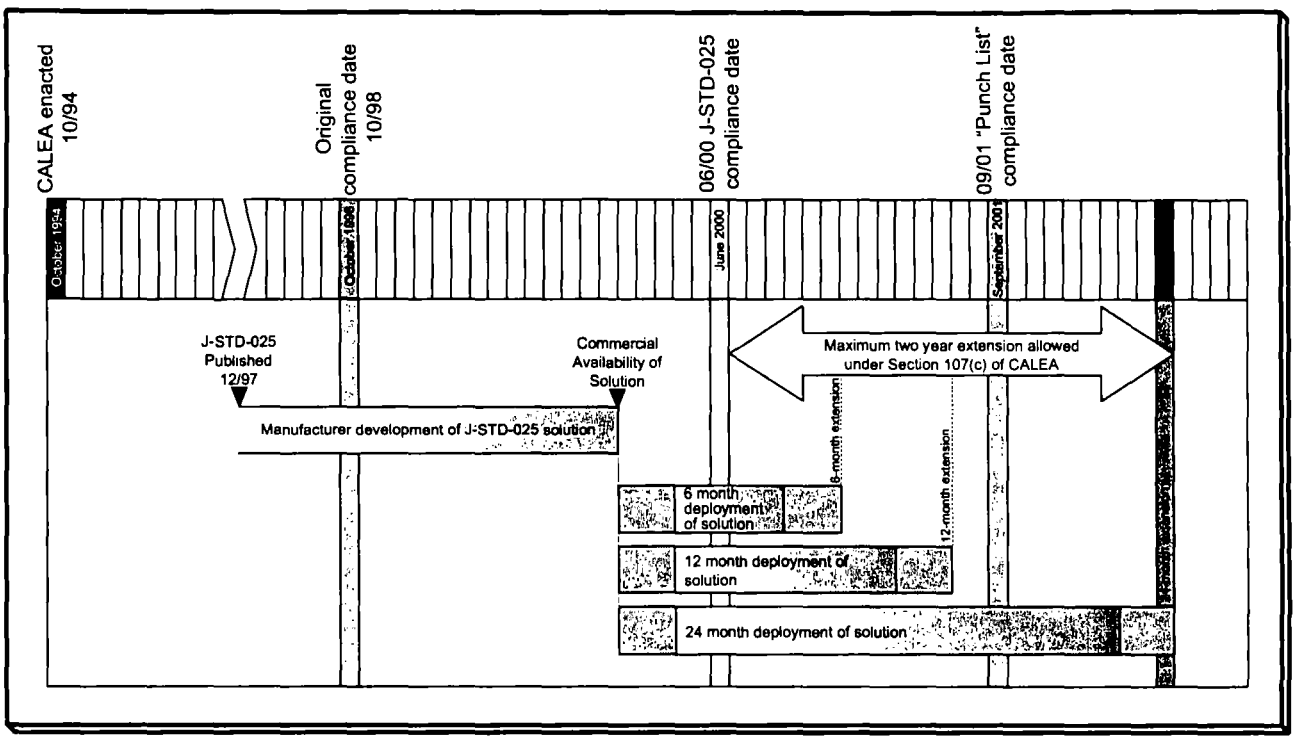


Figure 2 - J-STD-025 & Carriers' Normal Generic Upgrade Cycles

Carriers' Normal Generic Upgrade Cycles

A central element to the FBI's Flexible Deployment Plan is a carrier's normal, or planned, generic upgrade cycle. Individual carriers plan, engineer, and deploy services at different times and at different rates. In order to ensure that carriers can meet their CALEA obligations without being overly burdensome, carriers have the opportunity to advise the FBI of their normal generic upgrade cycles. Past generic upgrades and associated dates can be provided to establish a baseline of previous generic upgrades and validate future expected generic upgrades. See the information descriptions in the following section, Information Collection, and Appendix E for a Sample Flexible Deployment Assistance Guide Template.

Under the FBI's Flexible Deployment Plan, a carrier's normal generic upgrade cycle will play a role in when

Similarly, a carrier's normal generic upgrade cycle will play a role in when "Punch List" CALEA-compliant solutions are to be deployed in a carrier's network (see Figure 3, below). Again, carriers will develop their own deployment cycles based on: (1) the commercial availability of CALEA-compliant "Punch List" solutions; (2) market conditions and business plans; and (3) historical lawfully-authorized electronic surveillance activity (i.e., law enforcement priorities). The six, twelve-, and twenty-four-month deployment cycles shown in Figure 3 are illustrative examples of normal generic upgrade cycles. Actual carrier generic upgrade cycles are expected to differ based on the considerations outlined above.

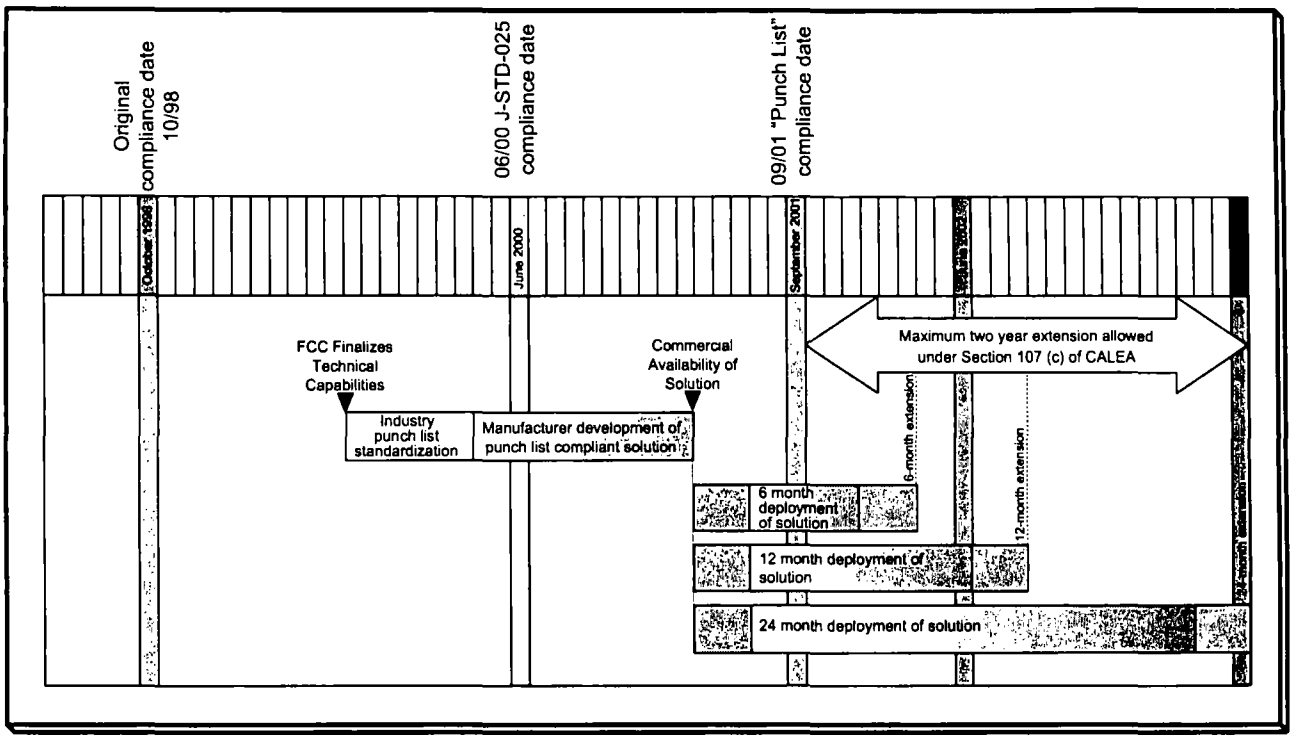


Figure 3 - Final CALEA Capability & Carriers' Normal Generic Upgrade Cycles

Commercial Availability of Solutions

In addition to setting the carriers' assistance capability requirement compliance date of June 30, 2000, the FCC determined that manufacturers of telecommunications equipment (i.e., equipment used in wireline, cellular, and broadband PCS services) had until December 31, 1999, to make compliant solutions commercially available to carriers.

The manufacturers of telecommunications equipment with which the FBI has been holding discussions have indicated that their CALEA capabilities will be made available over a number of software generic releases. The first releases will allow carriers to implement some or all of the core J-STD-025 CALEA capabilities, while later releases will complete the set of capabilities as mandated by the FCC. Some manufacturers have already made initial releases commercially available for carriers to deploy. CALEA-compliant solutions are commercially available on the date a manufacturer first makes its solution available. The FBI recognizes that manufacturers' production cycles may delay a particular carrier's ability to deploy CALEA-compliant software. The FBI expects carriers to incorporate the actual availability of CALEA-compliant solutions (i.e., available to the carrier) when developing their proposed deployment schedules.

Additionally, some manufacturers may not have CALEA-compliant solutions available for carriers to deploy to meet the June 30, 2000, and September 30, 2001 deadlines. Figure 4 shows how a delay in a manufacturer's solution availability may effect carriers' normal generic upgrade cycles for the deployment of a CALEA-compliant J-STD-025 solution. Figure 5 shows how a delay in a manufacturer's solution availability may effect carriers' normal generic upgrade cycles for the deployment of a Final CALEA-compliant solution.

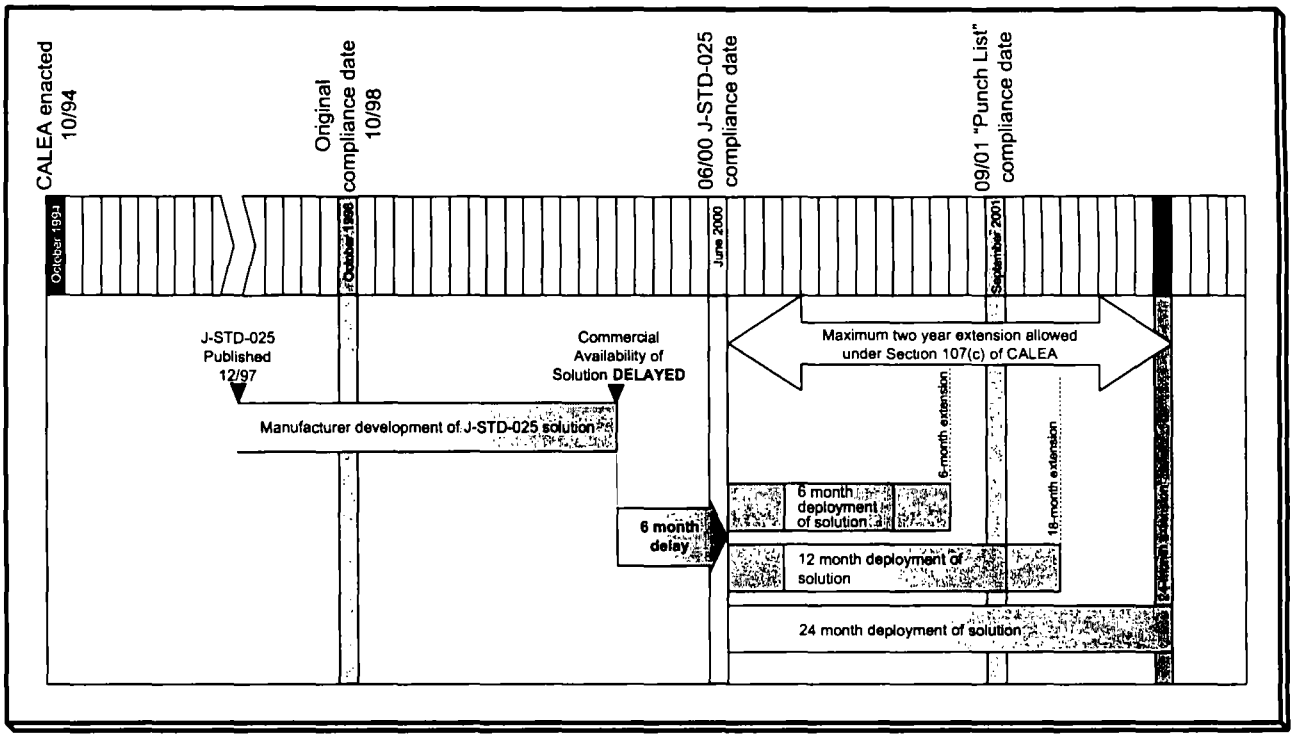


Figure 4 - Delayed Commercial Availability of J-STD-025 Solution

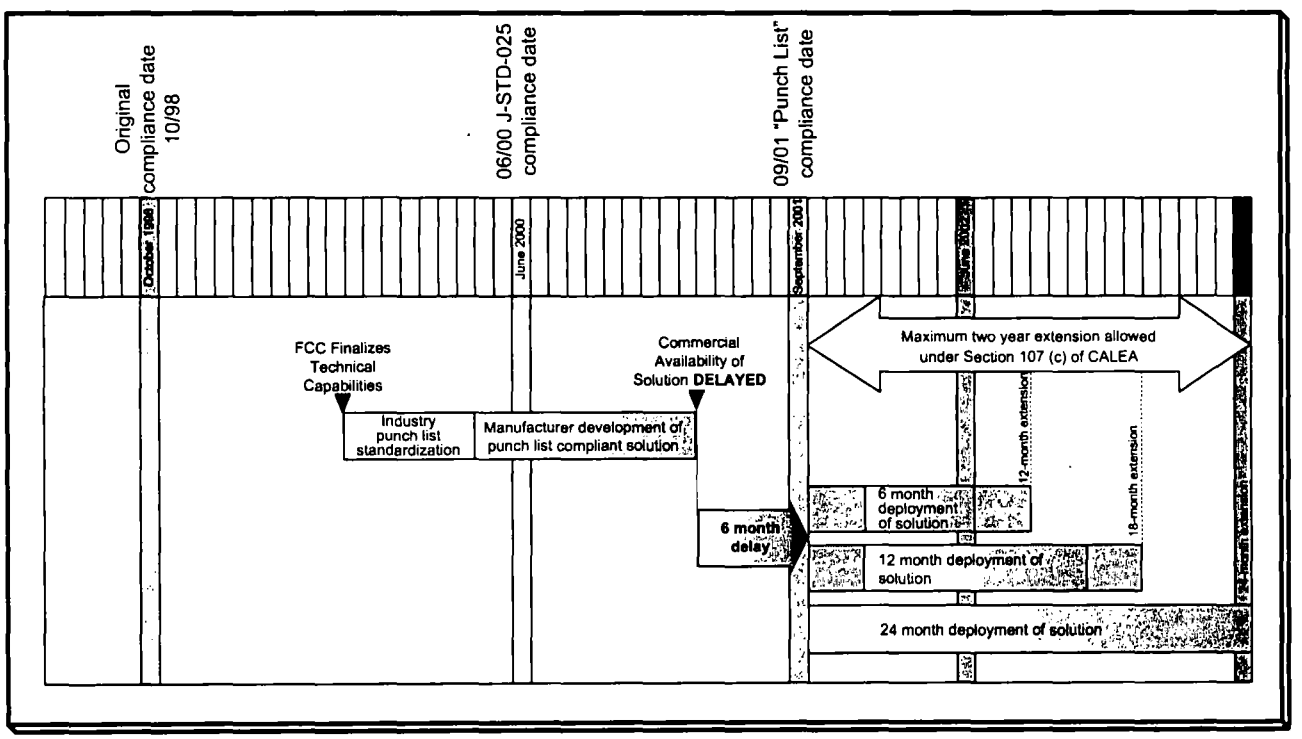


Figure 5 - Delayed Commercial Availability of the Final CALEA Capability Solution

Law Enforcement Priorities

One important factor to the FBI in considering a carrier's proposed CALEA solution deployment schedule is the historical electronic surveillance activity of law enforcement. The equipment, facilities, and services of a carrier which have previously played a role in the execution of lawfully-authorized electronic surveillance are considered by the FBI to be of high priority to law enforcement. These equipment, facilities, and services should be taken into consideration by a carrier when developing its proposed CALEA solution deployment schedule. High priority equipment, facilities, and services scheduled to be replaced should also be identified by a carrier. Figure 6 shows how law enforcement's priorities can be incorporated into a carrier's normal generic upgrade cycle.

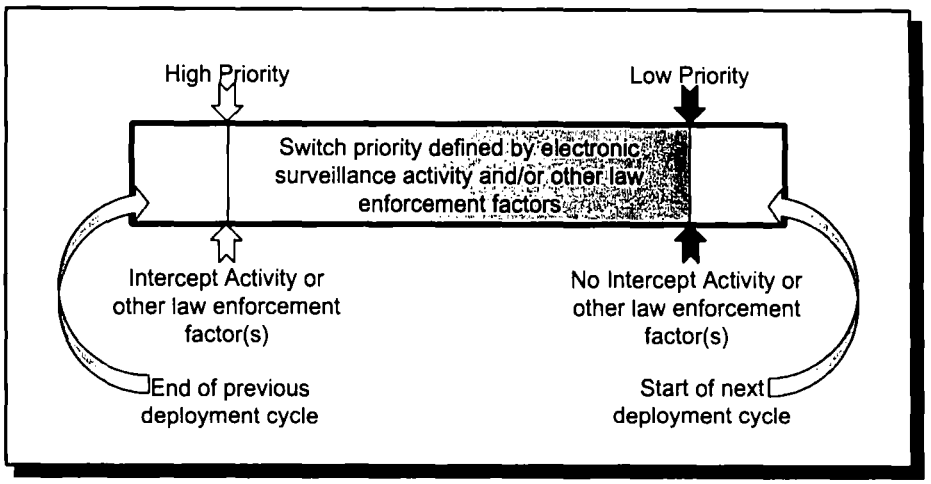


Figure 6 - Law Enforcement Priorities & Carriers' Normal Generic Upgrade Cycles

Section 109(b) of CALEA

In those instances where a carrier finds a solution developed by its manufacturer of telecommunications equipment to be prohibitively expensive for the carrier to deploy, CALEA provides a remedy under Section 109(b). The carrier may choose to petition the FCC with respect to any equipment, facilities, or service on which compliance would not be "reasonably achievable." In its Second Report and Order, the FCC articulated its basis for consideration of individual carrier petitions under CALEA's "reasonably achievable" provision. The FCC stated that: (1) it would be premature to adopt factors in addition to those set forth in Section 109(b), or to assign special weight to any one factor; (2) the Section 109 process should be reserved for the examination of specific carrier compliance problems, not to revisit broad policy goals; and (3) carrier requests for relief from CALEA compliance based on CALEA's costs or impact on rates, quality of service, or introduction of services to the market must be supported by specific facts, including quantitative data.

INFORMATION COLLECTION

As stated previously in this Guide, the FBI's Flexible Deployment Plan is based on (1) a carrier's normal generic upgrade cycle, and (2) law enforcement priorities. In order for the FBI to make an informed decision regarding a carrier's proposed deployment schedule, a carrier may provide information identifying its specific equipment, geographic area(s) served by the equipment, previous generic deployments, future planned generic deployments, and historical lawfully-authorized electronic surveillance activity.

In the following table, the term "switch or equipment" refers to any piece of telecommunications equipment which would need to undergo modification to be compliant with the requirements of CALEA. Examples of "switch or equipment" include end office switches and peripheral equipment such as Home Location Registers (HLR).

A Sample Flexible Deployment Assistance Guide Template is provided in Appendix E. A blank Flexible Deployment Assistance Guide Template is provided in Appendix F. Carriers may use the blank form to provide the above described information. An electronic version of this form is available on the FBI's Website at http://www.fbi.gov. Carriers may submit electronic versions of the Flexible Deployment Assistance Guide Template to the address provided at the end of this Guide.

The intent of the FBI's collection of information is to analyze a carrier's proposed deployment schedule and to assess whether or not the FBI would be willing to support a carrier's petition for an extension of CALEA's assistance capability compliance date(s). Any carrier-provided information marked as proprietary will be treated accordingly by the FBI, and the FBI stands at the ready to enter into an appropriate non-disclosure agreement with any carrier who believes it to be necessary.

Data Type	Description
Carrier Name	The name of the carrier which owns the identified switch or equipment
Contact Person & Telephone Number	The name and telephone number of a person the FBI can contact in the event questions arise with the data submitted
CLLI Code	Common Language Location Identifier or other unique switch or equipment identification
Switch or Equipment Location	The street address, city, and state where the switch or equipment is located
Switch or Equipment Type	The type of host or stand-alone switch or equipment identified by each CLLI Code. For example: 5ESS, DMS-100, EWSD, DMS-MTX, EMX-2500, CMS-8800, S12. In the event that a remote switch will need to be upgraded, include the remote switch type and corresponding host switch
Service Area	The name(s) of the counties, market service areas, or other appropriate geographic areas *where service is provided* by each identified switch or equipment. In the event that a switch or equipment serves multiple areas, each area (county, market service area, or other appropriate geographic area) should be identified. For switches or equipment with remotes, include counties, market service areas, or other appropriate geographic areas where service is provided by each remote
Current Software Generic	The software generic deployed as of January 1, 2000 on the equipment identified by each CLLI Code. For example: 5E12, NAO10
Historical Software Deployment Dates	Previous software deployment dates to establish an individual carrier's normal generic upgrade cycle
Future Planned Software Generic Deployment Dates	The future planned software generic, and deployment dates, to be installed in the identified switch or equipment
Historical Intercept Activity	Number of lawfully-authorized electronic surveillance intercepts (i.e., communications content, pen registers, and traps and traces) which were conducted on each identified switch or equipment by a municipal, county, state, or federal law enforcement agency for the years 1996, 1997, 1998, and 1999

Table 1 - Flexible Deployment Information Elements

Paperwork Reduction Act Notice

The FBI has created this Flexible Deployment Assistance Guide and the associated information collection template (see Appendix F) with the intent for it to be easily understood, and to impose the least possible burden on carriers choosing to provide the FBI with deployment information.

The estimated average time to read this Flexible Deployment Assistance Guide, complete the template, and file the information is as follows: (1) 1 hour to read the Flexible Deployment Assistance Guide; (2) 2 hours to gather the information to complete the Flexible Deployment Assistance Guide Template; (3) 1 hour to complete the Template; (4) 15 minutes to assemble and file the Template; for a total estimated average time of 4 hours and 15 minutes per Template. If you have comments regarding this estimate, or suggestions for simplifying this Guide and the associated information collection template, you can write to both the CALEA Implementation Section (CIS), 14800 Conference Center Drive, Suite 300, Chantilly, Virginia 20151; and the Office of Management and Budget, Paperwork Reduction Project, OMB No. 1110-0030, Washington, D.C. 20503.

ADDITIONAL TECHNOLOGIES
FCC's Second Report and Order

On August 31, 1999, the FCC adopted its Second Report and Order[20] regarding CALEA. In its Second Report and Order, the FCC examined the definition of "telecommunications carrier" set forth in Section 102 of CALEA. The FCC determined that the requirements of CALEA apply to:

- Any entity that holds itself out to serve the public indiscriminately in the provision of any telecommunications service;
- Entities previously identified as common carriers for purposes of the Communications Act,[21] including local exchange carriers, interexchange carriers, competitive access providers, and satellite-based service providers;
- Cable operators, electric, and other utilities to the extent that they offer telecommunications services for hire to the public;
- Commercial mobile radio service (CMRS) providers;
- Specialized Mobile Radio (SMR) providers when their systems interconnect to the public switched telephone network;
- Resellers of telecommunications services to the extent they own equipment with which services are provided;
- Providers of calling features such as call forwarding, call waiting, three-way calling, speed dialing, and the call redirection portion of voice mail; and
- Facilities used by carriers to provide both telecommunications and information services, are subject to CALEA in order to ensure the ability to conduct lawfully-authorized electronic surveillance of the telecommunications services.

The FCC concluded that some categories of entities are not telecommunications carriers subject to CALEA:

- Private mobile radio service (PMRS) providers;
- Pay telephone providers; and
- Information service providers, to the extent they do not provide telecommunications services.

Participation in the FBI's Flexible Deployment Plan is available to all telecommunications carriers subject to the require-ments of CALEA as determined by the FCC in its Second Report and Order. As stated previously in this Guide, a central element to the FBI's Flexible Deployment Plan is a carrier's normal, or planned, generic upgrade cycle. Because individual carriers plan, engineer, and deploy services at different times and at different rates, and in order to ensure that carriers can meet their CALEA obligations without being overly burdensome, carriers have the opportunity to advise the FBI of their deployment schedules.

In order for the FBI to make informed decisions regarding a carrier's proposed deployment schedule, a carrier may provide information identifying its specific equipment, geographic area(s) served by the equipment, previous generic deployments, future planned generic deployments, and historical lawfully-authorized electronic surveillance activity.

In the event that a carrier believes the template provided in Appendix F of this Guide requests information that is not applicable to its network or equipment, or is insufficient for a carrier to characterize its deployment schedule on an equipment-specific basis, a carrier is free to provide deployment information in any form. However, a carrier should provide the name of a contact person and their telephone number, as well as the following switch-, or equipment-specific information: unique equipment identifier; switch or equipment location; service area; current software generic; historical software generic deployment dates; future planned software generic deployment dates; and historical electronic surveillance intercept activity.

FCC's Third Report and Order

On August 31, 1999, the FCC also released its Third Report and Order regarding the assistance capability requirements of CALEA. In its Third Report and Order, the FCC recognized that the industry's J-STD-025 does not cover telecommunications technologies such as paging, specialized mobile radio, and mobile satellite services. In fact, the FCC stated that "[i]ndustry associations or standards-setting organizations that represent such service providers that fit within the definition of a telecommunications carrier under CALEA may establish voluntary standards to achieve compliance with Section 103 by the June 30, 2000 deadline, and take advantage of the safe harbor provision of Section 107(a). The absence of an industry standard, however, does not relieve such carriers from the obligations imposed by Section 103. In the absence of a publicly available standard, a carrier will have to work with its vendors to develop an individual CALEA solution, and a carrier is free to choose a solution that is specifically tailored to its particular system and technology."[22]

[20] Second Report and Order, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (rel. August 31, 1999).

[21] 47 U.S.C. § 153(10).

[22] Third Report and Order, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (rel. August 31, 1999).

ADDITIONAL INFORMATION

How and Where to Provide Flexible Deployment Assistance Guide Information

Carriers can download an electronic Flexible Deployment Assistance Guide Template from the FBI's Website at http://www.fbi.gov. Upon entering the site, proceed to the CALEA link through the available index (http://www.fbi.gov/programs/calea/calea.htm). The Flexible Deployment Assistance Guide page is available by selecting the *Flexible Deployment Assistance Guide* hyperlink.

Carriers that do not have access to the Internet and wish to acquire the Flexible Deployment Assistance Guide Template in electronic form can request 3.5 inch diskettes containing the electronic template from the address listed below. Carriers may either submit a completed Flexible Deployment Assistance Guide Template in electronic form (any spreadsheet or text file format) or use the Flexible Deployment Assistance Guide Template provided in Appendix F of this Guide. Carriers are strongly encouraged to file their Flexible Deployment Assistance Guide Templates by March 31, 2000, and all completed Flexible Deployment Assistance Guide Templates should be mailed to:

CALEA Implementation Section (CIS)

Attention: Flexible Deployment Assistance Guide

14800 Conference Center Drive, Suite 300

Chantilly, VA 20151-0450

Contact Information

Carriers that have additional questions or comments concerning this Flexible Deployment Assistance Guide can call the following toll-free number:

Communications Assistance for Law Enforcement Act (CALEA)
Flexible Deployment Assistance Guide
Help Desk

800-551-0336

APPENDIX A — FREQUENTLY ASKED QUESTIONS

Q What is the difference between the industry's interim technical standard (i.e., J-STD-025) and the missing technical capabilities (i.e., "Punch List")?

A The industry's interim technical standard (J-STD-025) provides the *majority* of electronic surveillance assistance capabilities required by CALEA. However, the standard failed to include some key evidentiary technical electronic surveillance capabilities, including: (1) content of subject-initiated conference calls; (2) party hold, join, drop; (3) access to subject-initiated dialing and signaling; (4) in-band and out-of-band signaling; (5) timing to associate call data to content; and (6) post-cut-through dialing (dialed digit extraction). See Appendix C for a brief description of each of these capabilities.

Q Which telecommunications carriers are eligible to be reimbursed for technical capability?

A CALEA authorized $500 million for the reimbursement of carriers for reasonable costs associated with making equipment, facilities, and services compliant with the requirements of CALEA. Equipment, facilities, and services installed or deployed on or before January 1, 1995, are eligible for reimbursement, provided the equipment, facility, or service has not been replaced, undergone a significant upgrade or undergone a major modification.

Q What information should a carrier provide the FBI to participate in the FBI's Flexible Deployment Plan?

A As described in the Information Collection Section of this Flexible Deployment Assistance Guide, a carrier should provide the name of a contact person and their telephone number, as well as the following switch-, or equipment-specific information: (1) CLLI Code or other unique equipment identifier; (2) switch or equipment location; (3) service area; (4) current software generic; (5) historical software generic deployment dates; (6) future planned software generic deployment dates; and (7) historical intercept activity.

Q Is it mandatory that a carrier complete the Flexible Deployment Assistance Guide Template?

A No. There is no legislative or other mandate for carriers to provide the information outlined in this Flexible Deployment Assistance Guide. Carrier submission of information to the FBI under the FBI's Flexible Deployment Plan is voluntary. However, the FBI will not be able to provide support for any carrier's petition for extension of CALEA's assistance capability compliance date without specific solution deployment information.

Q What are CALEA's compliance dates that a carrier needs to know?

A First, carriers must be compliant with the J-STD-025 capabilities by June 30, 2000. Second, carriers must comply with the missing technical capabilities (i.e., "Punch List") by September 30, 2001. Carriers providing wireline local exchange, cellular, and broadband PCS services have until March 12, 2001, to comply with the capacity requirements as enumerated in the Final Notice of Capacity (63 Fed. Reg. 12217).

Q How is the FBI working with manufacturers of telecommunications equipment to ensure CALEA solutions will be available for carriers to deploy?

A The FBI is holding discussions with a large number of manufacturers to assess the availability of technical solutions for carriers. To date, the vast majority of manufacturers have notified the FBI that they will make CALEA-compliant solutions available.

Q Will filling out the Flexible Deployment Assistance Guide Template ensure that a carrier receives an extension of the assistance capability deadline?

A No. If the Attorney General determines that a carrier's proposed deployment schedule is consistent with law enforcement priorities, she may then provide support, through the FBI, for the carrier's petition under Section 107(c). The FCC will determine whether or not to grant the petition. The FCC has stated, in its Second Report and Order, that it will accord "substantial weight" to the Attorney General's support for a carrier's petition under Section 107(c).

Q How will carriers be notified of their status after supplying the information identified in this Flexible Deployment Assistance Guide?

A Upon review of carrier-provided deployment information, the FBI will notify a carrier whether the carrier's proposed deployment schedule meets law enforcement's requirements. In those instances where a carrier's proposed deployment schedule meet's law enforcement's requirements, the FBI will provide support of a carrier's Section 107(c) petition before the FCC.

APPENDIX B — GLOSSARY[23]

Actual Capacity — the number of simultaneous call content interceptions, pen registers, and trap and traces that law enforcement may conduct 3 years after the publication of the Final Notice of Capacity.

Basic Trading Area (BTA) — a PCS service area defined by the FCC as a collection of counties, based on the Rand McNally 1992 Commercial Atlas & Marketing Guide.

Broadband Personal Communications Services (PCS) — radio communications operating within the 2 GHz band of the electromagnetic spectrum (from 1850 to 1990 MHz), which encompass mobile and ancillary fixed communication services, including a family of communications devices utilizing very small, lightweight, multifunction portable phones, portable facsimile and other imaging devices, new types of multifunction cordless phones, and advanced devices with two-way data capabilities.

Call Content — in substance, Section 103 of CALEA (47 U.S.C. §1002) requires carriers to ensure that law enforcement agencies are able, pursuant to lawful authorization, to intercept wire and electronic communications carried by the carrier. The phrase "call content" used in this Guide refers to the contents of such lawfully-intercepted communications.

Call-identifying Information — defined in 47 U.S.C. §1001(2) to mean "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."

Cellular Service — a mobile radiotelephone service in which common carriers are authorized to offer and provide a mobile telecommunications service for hire to the general public using cellular systems. A cellular radio system is an automated, high-capacity system of one or more multichannel base stations designed to provide radio telecommunications services to mobile stations.

CLLI Code — Common Language Location Identifier or equivalent identifier for carrier equipment.

Commercial Availability — the date on which a manufacturer of telecommunications equipment makes software available.

Electronic Communication — defined in 18 U.S.C. §2510(12), in substance, to include any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or a photooptical system.

Electronic Surveillance — for purposes of this Guide, the word "electronic surveillance" is used to refer to either the interception of call content or call-identifying information. The telecommunications service targeted for electronic surveillance includes all of the services and features associated with the subject's wireline/wireless telephone number, or as otherwise specified in a court order or lawful authorization.

Interception — for purposes of this Guide, the word "interception" is used to refer to either the interception of call content or call-identifying information, or both.

J-STD-025 — industry interim technical standard developed to meet the assistance capability requirements of Section 103 of CALEA published in December 1997.

Local Exchange Carrier — any person or entity that is engaged in the provision of telephone exchange service or exchange access. Such term does not include persons or entities engaged in the provision of a commercial mobile service.

Local Loop — the physical connection between a service provider's end office equipment, most often a switch, and a telephone subscriber's home or office.

[23] This Glossary is provided herein solely for the assistance of the reader.

APPENDIX B — GLOSSARY

Major Trading Area (MTA) — a PCS service area defined by the FCC as a collection of BTAs, based on the Rand McNally 1992 Commercial Atlas & Marketing Guide.

Maximum Capacity — the number of simultaneous call content interceptions, pen registers, and trap and traces that law enforcement may conduct after the date that is 3 years after the publication of the Final Notice of Capacity.

Metropolitan Statistical Area (MSA) — a geographic area based on counties, as defined by the U.S. Census Bureau, that contain cities with populations of 50,000 or more.

Normal Generic Upgrade Cycle — carrier-specific timeline of past- and future-planned software generic deployments.

Notice of Capacity — notice of the estimated actual and maximum number of simultaneous call content interceptions, pen registers, and trap and traces that law enforcement may conduct at some future date.

Packet Mode Communications — a method of communications in which the "conversation" (e.g., voice, video, data, or any other transmission) is disassembled into small packets of information. Each packet is uniquely identified, carries its own destination address, and traverses the network in an efficient manner. At the destination site, each packet is reassembled into the original "conversation."

Pen Register — defined in 18 U.S.C. § 3127(3), in pertinent part, as a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such a device is attached.

Punch List — nine assistance capability requirements missing from the industry's interim technical standard (J-STD-025), determined by the DOJ to be required by CALEA, and petitioned for by the FBI and DOJ before the FCC. Six of the nine missing assistance capability requirements were subsequently determined by the FCC to be required by CALEA.

Rural Service Area (RSA) — a geographic area not included within either an MSA or a New England Country Metropolitan Area for which a common carrier may have a license to provide cellular service.

Title III — the provision of the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. No. 90-351, 82 Stat. 212) that provides law enforcement the necessary authorization to conduct interception of the content of communications.

Telecommunications Carrier — defined in 47 U.S.C. § 1001(8), in pertinent part, as a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; or a person or entity engaged in providing commercial mobile service (See also 47 U.S.C. § 332(d)).

Trap and Trace Device — a device that captures incoming electronic or other impulses that identify the originating number of a wire or electronic communication.

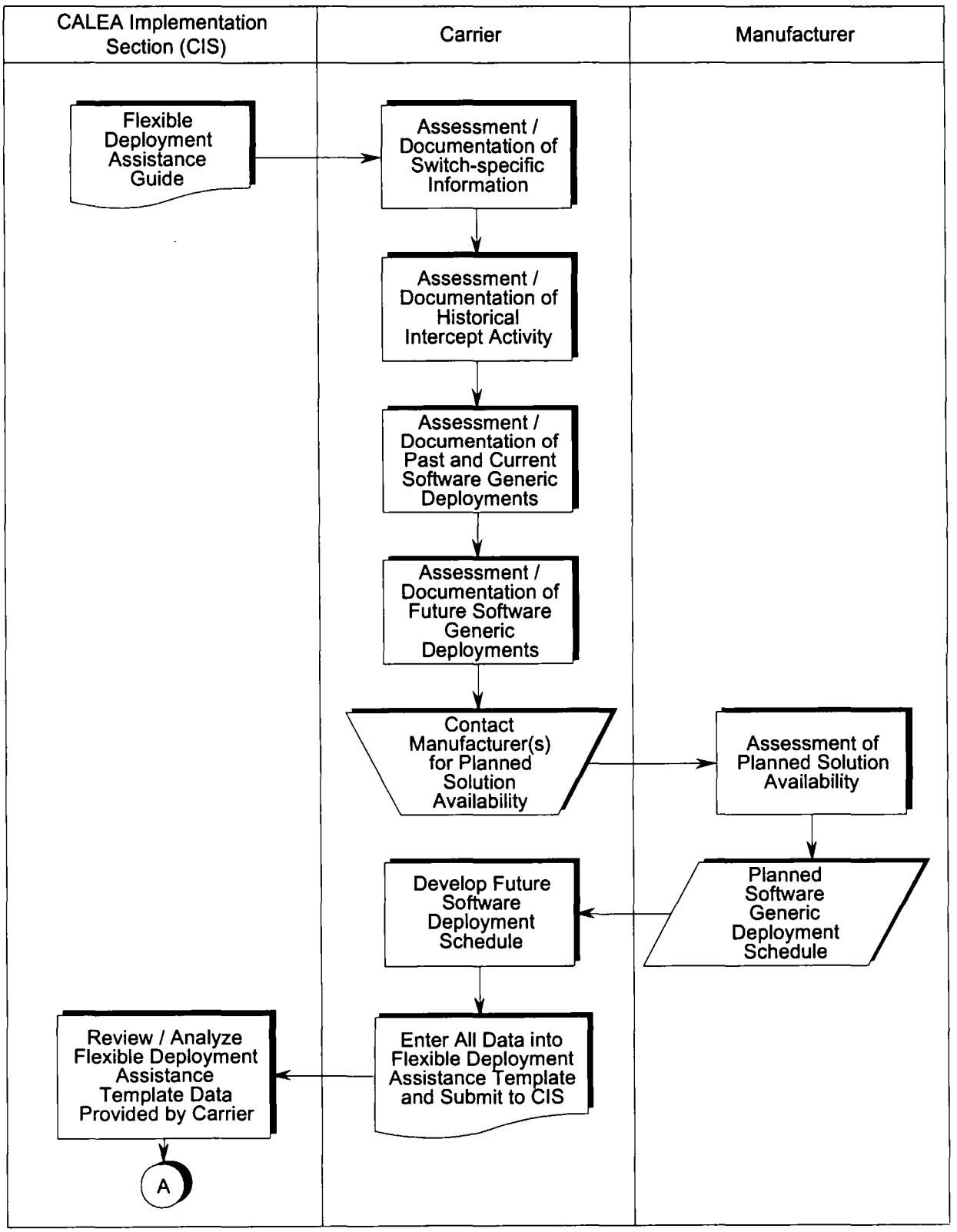
Wire Communication — defined in 18 U.S.C. § 2510(1), in substance, to mean any transfer involving the human voice made in whole or in part through the use of wire, cable, or other like transmission facilities. The term includes communications via cellular telephones.

APPENDIX C - BRIEF DESCRIPTION[24] OF PUNCH-LIST CAPABILITIES DETERMINED BY THE FCC TO BE REQUIRED BY CALEA

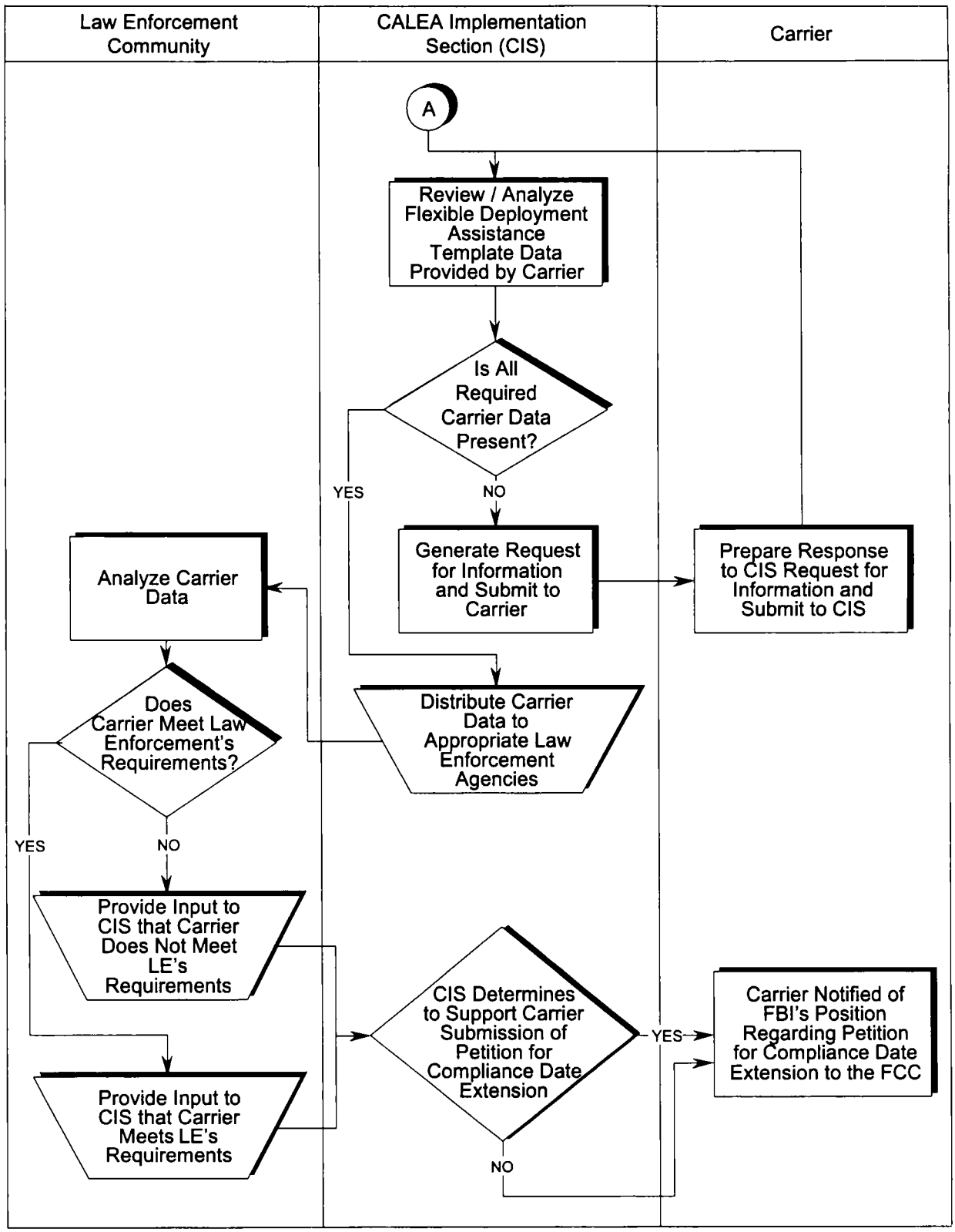
Name	Description
Content of subject-initiated conference calls	This capability would permit a law enforcement agency (LEA) to monitor the content of conversations connected via a conference call. Surveillance of all portions of a conference call would continue, even if any party to the call utilized services such as hold, call waiting, or three-way calling.
Party hold, join, drop	This capability also involves features designed to aid a LEA in the interception of multi-party calls. This capability would permit the LEA to receive from the telecommunications carrier messages identifying the parties to a conversation at all times. The party hold message would be provided whenever one or more parties are placed on hold. The party join message would report the addition of a party to an active call or the reactivation of a held call. The party drop message would report when any party to a call is released or disconnects and the call continues with two or more other parties.
Access to subject-initiated dialing and signaling	This capability would permit the LEA to be informed when a subject, using the facilities under surveillance, uses services such as call forwarding, call waiting, call hold, and three-way calling. This information would be provided for each communication initiated by the subject. This capability would require the telecommunications carrier to deliver a message to the LEA, informing the LEA that the subject has invoked a feature that would place a party on hold, transfer a call, forward a call, or add/remove a party to a call.
In-band and out-of-band signaling (Notification Message)	This technical requirement would enable a telecommunications carrier to send a notification message to the LEA when any network message (ringing, busy, call waiting signal, message light, *etc.*) is sent to a subject using facilities under surveillance. For example, if someone leaves a voice mail message on the subject's phone, the notification to the LEA would indicate the type of message notification sent to the subject (such as the phone's message light, audio signal, text message, *etc.*). For calls the subject originates, a notification message would also indicate whether the subject ended a call when the line was ringing, busy (a busy line or busy trunk), or before the network could complete the call.
Timing to associate call data to content	In those cases where the LEA has obtained authorization to intercept both content and call-identifying information, this capability would require that a telecommunications carrier send call timing information to the LEA so that the LEA could associate the call-identifying information with the actual content of the call.
Dialed digit extraction	This capability would require the telecommunications carrier to provide to the LEA on the call data channel the identity of any digits dialed by the subject after connecting to another carrier's service (also known as "post-cut-through digits"). One example of such dialing and signaling would occur when the subject dials an 800 number to access a long distance carrier. After connecting to the long distance carrier through the 800 number, the subject then dials the telephone number that represents the ultimate destination of the call.

[24] Punch list capabilities as described by the FCC in its Third Report and Order, *Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213 (rel. August 31, 1999).

APPENDIX D - FLEXIBLE DEPLOYMENT DATA SUBMISSION, COLLECTION, REVIEW, AND ANALYSIS PROCESS



APPENDIX D - FLEXIBLE DEPLOYMENT DATA SUBMISSION, COLLECTION, REVIEW, AND ANALYSIS PROCESS



APPENDIX E - SAMPLE FLEXIBLE DEPLOYMENT ASSISTANCE GUIDE TEMPLATE

WIRELINE CARRIER DATA SUBMISSION

Carrier Name **AnyTel**

Contact Person **John Doe**

Telephone Number **703-814-4700**

Switch-specific Information				Deployed Generics										Interceptions			
				Previous -1 n-2		Previous n-1		Current n		Next n+1		Next + n+2					
Host and/or Stand-alone CLLI Code or other Unique Identifier	Switch or Equipment Location	County or Wireless Service Area Served	Switch Type	Generic	Date Deployed	Generic	Date Deployed	Generic	Date Deployed	Generic	Date to be Deployed	Generic	Date to be Deployed	1996	1997	1998	1999
CHANVAWFDS0	Chantilly, VA	Fairfax Cou	DMS-100	NA 9	2/9	NA 0	1/99	AO11	12/99	NAO12	11/00	NAO13	10/01	0	2	2	3

WIRELESS CARRIER DATA SUBMISSION

Host and/or Stand-alone CLLI Code or other Unique Identifier	Switch or Equipment Location	County or Wireless Service Area Served	Switch Type	Generic	Date Deployed	Generic	Date Deployed	Generic	Date Deployed	Generic	Date to be Deployed	Generic	Date to be Deployed	1996	1997	1998	1999
CHANVAWFCM1	Chantilly, VA	Wash. DC MSA#8	Autoplex 1000	5E10	4/98	5E11	11/98	5E12	6/99	5E13	1/00	5E14	8/00	8	6	6	8

APPENDIX F - FLEXIBLE DEPLOYMENT ASSISTANCE GUIDE TEMPLATE

OMB Control Number: 1110-0030
Expiration Date: June 30, 2000

Carrier Name _____

Contact Person _____
Telephone
Number _____

Switch-specific Information				Deployed Generics										Interceptions			
				Previous -1 n-2		Previous n-1		Current n		Next n+1		Next + 1 n+2					
Host and/or Stand-alone CLLI Code or other Unique Identifier	Switch or Equipment Location	County or Wireless Service Area Served	Switch Type	Generic	Date Deployed	Generic	Date Deployed	Generic	Date Deployed	Generic	Date to be Deployed	Generic	Date to be Deployed	1996	1997	1998	1999

CALEA Implementation Section (CIS)
Attention: Flexible Deployment Assistance Guide
14800 Conference Center Drive, Suite 300
Chantilly, VA 20151-0450

Network Working Group
Request for Comments: 1984
Category: Informational

IAB
IESG
August 1996

IAB and IESG Statement on Cryptographic Technology and the Internet

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright

July 24, 1996

The Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, are concerned by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy.

Security mechanisms being developed in the Internet Engineering Task Force to meet these needs require and depend on the international use of adequate cryptographic technology. Ready access to such technology is therefore a key factor in the future growth of the Internet as a motor for international commerce and communication.

The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:

(a) impose restrictions by implementing export controls; and/or

(b) restrict commercial and private users to weak and inadequate mechanisms such as short cryptographic keys; and/or

(c) mandate that private decryption keys should be in the hands of the government or of some other third party; and/or

(d) prohibit the use of cryptology entirely, or permit it only to specially authorized organizations.

We believe that such policies are against the interests of consumers and the business community, are largely irrelevant to issues of military security, and provide only a marginal or illusory benefit to

law enforcement agencies, as discussed below.

The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries.

The IAB and IESG claim:

The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.

Encryption is not a secret technology monopolized by any one country, such that export controls can hope to contain its deployment. Any hobbyist can program a PC to do powerful encryption. Many algorithms are well documented, some with source code available in textbooks.

Export controls on encryption place companies in that country at a competitive disadvantage. Their competitors from countries without export restrictions can sell systems whose only design constraint is being secure, and easy to use.

Usage controls on encryption will also place companies in that country at a competitive disadvantage because these companies cannot securely and easily engage in electronic commerce.

Escrow mechanisms inevitably weaken the security of the overall cryptographic system, by creating new points of vulnerability that can and will be attacked.

Export controls and usage controls are slowing the deployment of security at the same time as the Internet is exponentially increasing in size and attackers are increasing in sophistication. This puts users in a dangerous position as they are forced to rely on insecure electronic communication.

TECHNICAL ANALYSIS

KEY SIZE

It is not acceptable to restrict the use or export of cryptosystems based on their key size. Systems that are breakable by one country will be breakable by others, possibly unfriendly ones. Large corporations and even criminal enterprises have the resources to break many cryptosystems. Furthermore, conversations often need to

be protected for years to come; as computers increase in speed, key sizes that were once out of reach of cryptanalysis will become insecure.

PUBLIC KEY INFRASTRUCTURE

Use of public key cryptography often requires the existence of a "certification authority". That is, some third party must sign a string containing the user's identity and public key. In turn, the third party's key is often signed by a higher-level certification authority.

Such a structure is legitimate and necessary. Indeed, many governments will and should run their own CAs, if only to protect citizens' transactions with their governments. But certification authorities should not be confused with escrow centers. Escrow centers are repositories for private keys, while certification authorities deal with public keys. Indeed, sound cryptographic practice dictates that users never reveal their private keys to anyone, even the certification authority.

KEYS SHOULD NOT BE REVEALABLE

The security of a modern cryptosystem rests entirely on the secrecy of the keys. Accordingly, it is a major principle of system design that to the extent possible, secret keys should never leave their user's secure environment. Key escrow implies that keys must be disclosed in some fashion, a flat-out contradiction of this principle. Any such disclosure weakens the total security of the system.

DATA RECOVERY

Sometimes escrow systems are touted as being good for the customer because they allow data recovery in the case of lost keys. However, it should be up to the customer to decide whether they would prefer the more secure system in which lost keys mean lost data, or one in which keys are escrowed to be recovered when necessary. Similarly, keys used only for conversations (as opposed to file storage) need never be escrowed. And a system in which the secret key is stored by a government and not by the data owner is certainly not practical for data recovery.

SIGNATURE KEYS

Keys used for signatures and authentication must never be escrowed. Any third party with access to such keys could impersonate the legitimate owner, creating new opportunities for fraud and deceit.

Indeed, a user who wished to repudiate a transaction could claim that his or her escrowed key was used, putting the onus on that party. If a government escrowed the keys, a defendant could claim that the evidence had been forged by the government, thereby making prosecution much more difficult. For electronic commerce, non-repudiation is one of the most important uses for cryptography; and non-repudiation depends on the assumption that only the user has access to the private key.

PROTECTION OF THE EXISTING INFRASTRUCTURE

In some cases, it is technically feasible to use cryptographic operations that do not involve secrecy. While this may suffice in some cases, much of the existing technical and commercial infrastructure cannot be protected in this way. For example, conventional passwords, credit card numbers, and the like must be protected by strong encryption, even though some day more sophisticated techniques may replace them. Encryption can be added on quite easily; wholesale changes to diverse systems cannot.

CONFLICTING INTERNATIONAL POLICIES

Conflicting restrictions on encryption often force an international company to use a weak encryption system, in order to satisfy legal requirements in two or more different countries. Ironically, in such cases either nation might consider the other an adversary against whom commercial enterprises should use strong cryptography. Clearly, key escrow is not a suitable compromise, since neither country would want to disclose keys to the other.

MULTIPLE ENCRYPTION

Even if escrowed encryption schemes are used, there is nothing to prevent someone from using another encryption scheme first. Certainly, any serious malefactors would do this; the outer encryption layer, which would use an escrowed scheme, would be used to divert suspicion.

ESCROW OF PRIVATE KEYS WON'T NECESSARILY ALLOW DATA DECRYPTION

A major threat to users of cryptographic systems is the theft of long-term keys (perhaps by a hacker), either before or after a sensitive conversation. To counter this threat, schemes with "perfect forward secrecy" are often employed. If PFS is used, the attacker must be in control of the machine during the actual conversation. But PFS is generally incompatible with schemes involving escrow of private keys. (This is an oversimplification, but a full analysis would be too lengthy for this document.)

CONCLUSIONS

As more and more companies connect to the Internet, and as more and more commerce takes place there, security is becoming more and more critical. Cryptography is the most powerful single tool that users can use to secure the Internet. Knowingly making that tool weaker threatens their ability to do so, and has no proven benefit.

Security Considerations

Security issues are discussed throughout this memo.

Authors' Addresses

Brian E. Carpenter
Chair of the IAB
CERN
European Laboratory for Particle Physics
1211 Geneva 23
Switzerland

Phone: +41 22 767-4967
EMail: brian@dxcoms.cern.ch

Fred Baker
Chair of the IETF

cisco Systems, Inc.
519 Lado Drive
Santa Barbara, CA 93111

Phone: +1-805-681-0115
EMail: fred@cisco.com

The Internet Society is described at http://www.isoc.org/

The Internet Architecture Board is described at
http://www.iab.org/iab

The Internet Engineering Task Force and the Internet Engineering Steering Group are described at http://www.ietf.org

A new Request for Comments is now available in online RFC libraries.

RFC 2804

Title: IETF Policy on Wiretapping
Author(s): IAB, IESG
Status: Informational
Date: May 2000
Mailbox: fred@cisco.com, brian@icair.org
Pages: 10
Characters: 18934
Updates/Obsoletes/SeeAlso: None

I-D Tag: draft-iab-raven-01.txt

URL: ftp://ftp.isi.edu/in-notes/rfc2804.txt

The Internet Engineering Task Force (IETF) has been asked to take a position on the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping.

This memo explains what the IETF thinks the question means, why its answer is "no", and what that answer means.

This document is a product of the Internet Architecture Board.

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

This announcement is sent to the IETF list and the RFC-DIST list. Requests to be added to or deleted from the IETF distribution list should be sent to IETF-REQUEST@IETF.ORG. Requests to be added to or deleted from the RFC-DIST distribution list should be sent to RFC-DIST-REQUEST@RFC-EDITOR.ORG.

Details on obtaining RFCs via FTP or EMAIL may be obtained by sending an EMAIL message to rfc-info@RFC-EDITOR.ORG with the message body help: ways_to_get_rfcs. For example:

To: rfc-info@RFC-EDITOR.ORG
Subject: getting rfcs

help: ways_to_get_rfcs

Requests for special distribution should be addressed to either the author of the RFC in question, or to RFC-Manager@RFC-EDITOR.ORG. Unless specifically noted otherwise on the RFC itself, all RFCs are for unlimited distribution.echo
Submissions for Requests for Comments should be sent to RFC-EDITOR@RFC-EDITOR.ORG. Please consult RFC 2223, Instructions to RFC Authors, for further information.