Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service

Issue 1
January 29, 2003

CALEA Implementation
Federal Bureau of Investigation
P. O. Box 220450
Chantilly, Virginia 20153-0450

The following special requirements for handling and control of this "FOR OFFICIAL USE ONLY" document shall apply to all organizations and individuals receiving this document:

1. This document is the property of the U. S. Government, and is to be used only to satisfy the requirements set forth in the document.
2. Dissemination decisions regarding this document are made by the U.S. Government, and no further dissemination by the recipients is authorized, except within the receiving organization.
3. This document is to be controlled on a need-to-know basis, and shall be made available only to those individuals whose knowledge of the information contained herein is reasonably expected to provide benefit to the U. S. Government and the law enforcement community.
4. This document is not intended for public release. Recipients are expressly denied authorization to print, publish, utter, or otherwise disclose the contents of this document in any materials intended for public dissemination, or to other persons or organizations not having a need-to-know. This restriction includes but is not limited to corporate reports, news releases, publicity documents, newsletters, and the like.
5. This document shall be controlled and protected in such a manner as to preclude unauthorized access to it. Copies may be made, but these copies must contain (1) all "FOR OFFICIAL USE ONLY" markings, (2) all control warnings and instructions, and (3) be subject to the same control and handling restrictions as the original.

This document contains information that the Federal Bureau of Investigation (FBI) and law enforcement desire to protect against unrestricted disclosure. It is information that, if disclosed, could reveal aspects of, harm, or otherwise impede investigative activities or investigative techniques, particularly related to the conduct of electronic surveillance efforts.

Electronic Surveillance Needs for CGVoP Service

Contents

List of Figures

List of Tables

Executive Summary

Carrier-Grade Voice over Packet (CGVoP) Service Providers offer consumers the same types of voice services and features that are offered by traditional local circuit-switched voice telephony service providers (i.e., Local Exchange Carriers and Wireless Service Providers). CGVoP Service Providers use a carrier-grade packet network to carry the communicating end users' conversations and associated signaling information.

CGVoP Service is one of the many evolving packet-based services that are being utilized more frequently as forms of communication. With the growing use of CGVoP Service, communication between users of the service will become increasingly relevant to law enforcement.

Lawfully authorized electronic surveillance (LAES) is a critical tool used by law enforcement for investigative purposes. LAES capabilities have been in place for many years to intercept communication-identifying information and communication content for circuit-switched voice telephony services. However, these capabilities are not sufficient for CGVoP Service. Therefore, LAES capabilities must be defined and deployed specifically for CGVoP Service.

Critical to achieving LAES for CGVoP communications is the exchange of information between law enforcement and industry. This exchange includes law enforcement's presentation of their needs to CGVoP Service Providers and their equipment suppliers, including the need for access to communication-identifying information and communication content for CGVoP Service. Providing law enforcement's needs early in the development process is expected to help ensure timely deployment of effectual and cost-effective LAES capabilities.

To facilitate industry interaction, this document captures law enforcement's needs regarding LAES capabilities for CGVoP Service. The document focuses mainly on communication-identifying information associated with service-related events that are of interest to law enforcement. The document also addresses law enforcement's needs regarding the content of CGVoP communications.

1 Introduction

This document presents law enforcement's electronic surveillance needs regarding Carrier-Grade Voice over Packet (CGVoP) Service.

This section introduces the content of the document. It contains background information and describes the purpose and scope of the document. The section also describes the target audience, defines the service, presents the organization of the document, and introduces the labeling convention used for requirements contained in the document.

1.1 Background

Lawfully authorized electronic surveillance (LAES) is a critically important investigative tool whereby Law Enforcement Agencies (LEAs) are permitted to intercept communications and/or acquire communication-identifying information. Many serious law enforcement investigations would be thwarted without the availability of LAES as an investigative technique and the cooperation of service providers.

The legal authority for LAES is found in federal statutes, including but not limited to the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 3121 et seq.), which governs pen registers and trap and trace devices, and the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.), which governs interceptions of communication content and is commonly referred to as "Title III" or "the Wiretap Act." The assistance of service providers has long been authorized and required pursuant to these federal statutes.

In addition, certain service providers (labeled "Telecommunications Carriers") are required to design their systems so as to ensure that they are capable of enabling the government to conduct LAES, pursuant to the 1994 Communications Assistance for Law Enforcement Act (CALEA).[1] Service providers who meet the definition of "Telecommunications Carrier" must meet the requirements of CALEA.

In May of 1995, the Federal Bureau of Investigation (FBI), in cooperation with federal, state and local LEAs, published *Law Enforcement Requirements for the Surveillance of Electronic Communications*[2]. The document provided guidance to service providers with wireline, wireless, and Broadband Personal Communications Services (PCS) networks. Law enforcement recognizes that, in some instances, a service provider may be able to ensure that an LEA has access to the communication content and/or communication-identifying information associated with an intercept subject's use of a service, without the service provider having to modify its networks or systems. However, for many of the new services offered over packet networks, electronic surveillance has not been adequately addressed. In fact, many of the new packet-based services and architectures impede or even preclude law enforcement's full and proper execution

[1] See generally 47 U.S.C. 1001 to 1010; CALEA applies to Telecommunications Carriers but not to information services. See 47 U.S.C. §§1002(b)(2)(A), 1001(6).

[2] *Law Enforcement Requirements for the Surveillance of Electronic Communications* (May, 1995) is available on www.askcalea.net .

of LAES and challenge the ability of service providers to assist law enforcement. As a result, network-based surveillance solutions will likely be required to address these problems.

In order to stimulate development of effective electronic surveillance solutions for packet-based services, law enforcement developed a set of general capability requirements that identify law enforcement's basic needs when performing electronic surveillance for packet-based communications. These requirements are specified in the *Packet Surveillance Fundamental Needs Document (PSFND) for Telecommunications Carriers, Equipment Manufacturers, and Providers of Telecommunications Support Services*. Law enforcement recognizes that each packet-based service has more-detailed needs based on the specific characteristics of the service and architectures employed for the service.

CGVoP Service[3] is a packet-based service for which law enforcement has identified the need for specific electronic surveillance capabilities. Therefore, law enforcement has selected CGVoP Service for development of requirements for these capabilities. These requirements are the primary content of this document.

1.2 Purpose and Scope

As stated above, capabilities are needed from service providers to assist LEAs in conducting LAES for CGVoP Service. The purpose of this document, *Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service*, is to set forth the surveillance capabilities needed by LEAs for CGVoP Service. This document is intended to:

- Build awareness of law enforcement's needs,
- Provide understanding of the specific electronic surveillance requirements that address these needs, and
- Stimulate thinking towards the development of cost-effective electronic surveillance solutions that meet these requirements and strike a balance between privacy, and national security and public safety.

This document is intended to provide guidance to CGVoP Service Providers and equipment manufacturers in the form of law enforcement's requirements for these electronic surveillance capabilities.

The requirements contained in this document define ***what*** communication-identifying information and communication content are needed by LEAs conducting LAES for Carrier-Grade VoP Service. The requirements do not define ***how*** a CGVoP Service Provider would access an intercept subject's communication-identifying information and communication content within the CGVoP Service Provider network. In addition, this document does not assume a particular physical architecture or implementation for meeting the capabilities identified.

This document is not intended and should not be considered to require any specific design nor prohibit the adoption of any equipment. This document is meant to describe the technical capabilities and features that LEAs view as important to accomplishing their goal in conducting

[3] Section 1.4 contains a definition of CGVoP Service.

LAES, which is to acquire accurate and complete information for their investigations in the best manner possible and in accordance with law.

This document does not address the various types of legal authorizations that dictate the specific information to be provided for LAES. The definition of electronic surveillance capabilities in this document and the subsequent deployment of these capabilities by CGVoP Service Providers do not preclude LEAs from continuing to use existing surveillance techniques for packet-based services.

This document was prepared in cooperation with representatives of the U.S. law enforcement community, including federal, state and local law enforcement.

1.3 Target Audience

This document is intended to offer guidance regarding law enforcement's electronic surveillance needs to entities involved in the delivery of CGVoP Service to end customers, including CGVoP Service Providers offering the service, manufacturers of equipment used to offer the service, and standards bodies and industry associations developing specifications for the service. This document is also intended to inform federal government entities, including the Federal Communications Commission (FCC) and Congress, of law enforcement's electronic surveillance needs. Lastly, this document is intended to assist LEAs that conduct electronic surveillance and manufacturers of electronic surveillance equipment in understanding the inherent complexities in performing LAES for packet-based services and the corresponding necessary electronic surveillance capabilities.

1.4 Definition of Carrier-Grade Voice over Packet (CGVoP) Service

Within the last five years, there has been a significant movement within the telecommunications industry to utilize packet technology to offer voice services that parallel the services provided through the Public Switched Telephone Network (PSTN) and that strive to achieve quality, reliability, security and connectivity comparable to the PSTN. This movement has been an attempt to leverage the inherent flexibility and cost effectiveness of packet technology, mainly for the purpose of migrating existing PSTN infrastructure (for Incumbent Local Exchange Carriers [ILECs] and Wireless Service Providers) or competing with ILECs by deploying new infrastructure (for Competitive Local Exchange Carriers [CLECs]).

The focus of this document is on law enforcement's electronic surveillance needs for CGVoP Service. CGVoP Service is defined as the set of subscription-based voice services and features provided over carrier-managed packet networks, and includes wireline and wireless services.

1.5 Assumptions

The following assumptions have been made in the development of this document:

1. CGVoP Service, as defined in this document, is limited to *voice-band* communications, which includes voice-band telephone calls, voice-band facsimile calls, and voice-band modem calls. Hence, the focus of this document is voice-band communications.

2. This document only addresses CGVoP Service. Other services that might be offered by a provider of CGVoP Service are not addressed. For example, while CGVoP Service Providers might offer other application-level services (e.g., video conferencing, unified messaging, email), such services are not addressed herein. As another example, while CGVoP Service Providers might also offer broadband access services (e.g., Digital Subscriber Line [DSL] service) and CGVoP Service subscribers might leverage these broadband access services to use CGVoP Service, broadband access services are not addressed herein.[4]

3. CGVoP Service only includes services to which an end user must subscribe. Service subscription is defined as establishing with a CGVoP Service Provider static information that uniquely identifies an end user, or an end user's equipment, facilities, or service. Since service subscription makes available unique information that can be used to definitively identify an end user, service subscription is critical to the performance of electronic surveillance for a service.

4. It is not necessary for the document to explicitly address cases where a subscribed-to CGVoP Service Provider re-sells service or hires another provider to offer part of the service. Law enforcement's needs apply to the subscribed-to CGVoP Service Provider, regardless of whether or not the service provider owns the functionality.

1.6 Document Organization

The document is organized into the following sections:

- **Section 1** describes the purpose, scope, target audience and assumptions for the document, provides a definition of the service, and presents the requirements-labeling convention used in the document.
- **Section 2** presents general concepts of packet electronic surveillance and defines key terms used throughout the document.
- **Section 3** describes the CGVoP Service in detail.
- **Section 4** defines the events for which LEAs require communication-identifying information and identifies the required information.
- **Section 5** defines LEA access to communication-identifying information and communication content.
- **Section 6** presents law enforcement's needs regarding the performance, quality, security, and integrity for performing LAES for CGVoP Service.
- The **References** section lists the documents that are referenced within the document.
- The **Acronyms** section presents the acronyms used in the document.

[4] Broadband access services (e.g., DSL service) could be addressed in a future service-specific document.

- The **Glossary** defines specialized terms used in the document.

1.7 Requirement-Labeling Convention

In this document, requirements are presented using special formats to facilitate locating, referencing and distinguishing these types of information from supporting text. The intent of this presentation style is to improve the clarity, readability and overall usefulness of the document.

Each requirement has a label that contains the following information:

- Indication of the type of information presented in the requirement. The following requirement types are used within this document:
  - **Requirement** – A functional capability that is essential to meeting law enforcement's needs for LAES. A Requirement contains the word "requires" and is identified by the letter "R".
  - **Conditional Requirement** – A functional capability that is essential to meeting law enforcement's needs for LAES *in specific cases*. If law enforcement identifies a capability defined in a Conditional Requirement as necessary for a specific case, it shall be treated as a Requirement for the application. A Conditional Requirement states the condition under which the defined capability applies, contains the word "requires" and is identified by the letters "CR".
  - **Objective** – A functional capability that is desirable for meeting law enforcement's needs for LAES. An Objective contains the word "desires" and is identified by the letter "O".
  - **Conditional Objective** – A functional capability that is desirable for meeting law enforcement's needs for LAES *in specific cases*. A Conditional Objective states the condition under which the defined capability applies, contains the word "desires" and is identified by the letters "CO".
- A document-wide sequence number for each requirement type.

Each requirement type is presented in indented, boldface type.

The following is an example of the third Requirement in the document:

R-3 Law enforcement requires …

2 Packet Electronic Surveillance Overview

This section provides an overview of the packet electronic surveillance capability. Also, key terms used in the document are defined.

2.1 Packet Electronic Surveillance Capability

Regardless of the authority under which LAES is performed, there are fundamental electronic surveillance capabilities for packet-based communications.

Law enforcement's fundamental need for LAES is to gain access to the communication-identifying information and communication content associated with an intercept subject's use of a service. This need applies to communications initiated, received and redirected by an intercept subject's equipment, facilities or service.

In performing LAES for packet-based services, law enforcement expects to have access to communication-identifying information that is reasonably available to the provider of the service. For a particular provider, the determination of whether or not information is reasonably available for a service is based on:

- the role that the provider plays in the particular service and
- what information is present at the provider's network entities that support the service.

There are typically multiple providers involved in an intercept subject's use of a particular packet-based service. One of these providers is considered to be the actual provider of the service; the other providers *enable* the service.

A CGVoP Service Provider employs equipment for providing CGVoP Service. Based on the functionality supported by this equipment, certain communication-identifying information about an intercept subject's use of the service is present at the equipment and could be made available by a CGVoP Service Provider without the provider being unduly burdened by network modifications.

The equipment at which communication-identifying information or communication content is accessed is termed an "Intercept Access Point (IAP)". For packet-based services, because the underlying service architecture is often distributed in nature, IAPs for communication-identifying information and IAPs for communication content are commonly different types of equipment. Furthermore, for a given service scenario (i.e., the use of a service in a particular way and the particular chain of occurrences associated with this use), there could be multiple IAPs for communication-identifying information and communication content. Moreover, the IAP for communication-identifying information and/or communication content could vary between different service scenarios.

However, this document does not require or assume the distribution of IAPs. Furthermore, the document does not identify which network elements should or could be IAPs.

Law enforcement needs access to information regarding certain end-user actions or related signals associated with an intercept subject's use of a service that are communication-identifying information or result in the generation of communication-identifying information. For the

purposes of this document, these end-user actions and related signals are termed "surveillance events." For each surveillance event, there are one or more specific cases for which the event is considered to occur and there is a set of information needed by law enforcement.

Section 4 defines the surveillance events and event information for CGVoP Service. Section 5 presents law enforcement's needs regarding lawfully authorized access to communication-identifying information and communication content for CGVoP Service. Section 6 presents general law enforcement needs for LAES for CGVoP Service.

2.2 Key Definitions

This section defines key terms used in the document. Understanding these terms is essential to understanding the requirements contained herein. A complete glossary of terms is provided at the end of the document.

agent – a network-based service or device that acts on behalf of a subscriber to send or receive communications (e.g., an interactive screening service, a reminder service, a delayed transmission service).

associate – a telecommunications user whose equipment, facilities, or services are used to communicate or attempt to communicate with the intercept subject.

call – a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used. A call may have one or more legs.

call leg – a bi-directional call path associated with each network facility usage attempt and subsequent usage.

carrier-grade – indicates that the packet network is a managed network offering services and features that meet or exceed the levels of quality, reliability, security and connectivity found in the circuit switch-based PSTN.

Carrier-grade Voice over Packet (CGVoP) Service Provider – a service provider that offers carrier-grade voice services over a carrier-managed packet network.

communications –encompasses the term "electronic communications," defined in 18, U.S.C. 2510(12) as "any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system." As used herein, the term also includes "wire communications," defined in 18, U.S.C. 2510(1) as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."

communication attempt – initiation of communication by the intercept subject or an associate.

communication content –encompasses the term "contents," defined in 18 U.S.C. 2510 (8) as "when used with respect to any wire, oral or electronic communications, includes any information concerning the substance, purport or meaning of that communication."

communication-identifying information – 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 the service provider. This includes, but is not limited to, directory numbers, call setup information, IP addresses, other routing or addressing information, and parameters of the signaling information that can be used as a means to subscribe to features of the service or activate features of the service, or establish and control a session or communication attempt.

cut-through – when an endpoint has received via call signaling the information needed to communicate.

Intercept Access Point (IAP) – a point within a service provider's network where some of the communications or communication-identifying information of an intercept subject's equipment, facilities and services are accessed.

intercept subject – a telecommunication service subscriber (and other users of such service) whose communications, communication-identifying information, or both, have been lawfully authorized to be intercepted and delivered to an LEA. The information used to identify the intercept subject includes those inputs used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

Internet – collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate intelligence of all kinds by wire and radio.

Lawfully Authorized Electronic Surveillance (LAES) – the interception of communication content and/or acquisition of communication-identifying information. Government's legal authority to perform LAES was established through laws such as the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 3121 et seq.), which governs pen registers and trap and trace devices, and the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.), which governs interceptions of communication content and is commonly referred to as "Title III" or "the Wiretap Act." The use of this term in this document does not include administrative subpoenas for obtaining a subscriber's service usage records and information about a subscriber's service that a LEA may employ before the start of an authorized interception.

Law Enforcement Agency (LEA) – a government entity with the legal authority to conduct electronic surveillance (e.g., the FBI or a local police department).

multi-way call – a call involving more than two parties, where the intercept subject initiated the addition of the other parties to the call. A multi-way call includes a three-way call and a conference call.

packet-based communication – user packet activity sent or received over the course of a communication.

packet-based service – a service that employs packet-mode technology.

packet-mode – a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s).

packet network – a network in which data is transmitted in units called packets.

service – a capability or set of capabilities offered by a service provider to end users, to which end users subscribe.

service feature – a capability offered by a service provider as part of a service, where such a capability cannot be used outside of the context of the service.

service scenario – the use of a service in a particular way and the particular chain of occurrences associated with this use.

service subscription – establishing with a service provider static information that uniquely identifies an end user, or an end user's equipment, facilities, or service.

surveillance event – an end-user action or related signal associated with the use of a service that is communication-identifying information or results in the generation of communication-identifying information..

3 Service Description

CGVoP Service is defined as a set of subscription-based voice services and features provided over a carrier-managed packet network. The modifier "carrier-grade" is used to indicate that the CGVoP network is a managed network in that the services and features offered achieve comparable levels of quality, reliability, security and connectivity as the levels found in the traditional circuit switch-based PSTN.

CGVoP networks are now being positioned to supplement and eventually replace the circuit-switched networks currently comprising the majority of the network components of the PSTN. In fact, a growing percentage of carrier-grade voice calls are already traversing these carrier-managed packet networks. Service providers will want the transition to the new technology to be seamless. Consequently, the differences between the packet network and the present circuit-switched network will be introduced to customers in terms of additional services and features built on the base of present capabilities.

3.1 Service Capabilities

CGVoP Service can be viewed as the packet-mode equivalent of circuit-switched local voice telephony service. As such, CGVoP networks perform the fundamental functions of call control, signaling, switching, and routing inherent in the circuit-switched PSTN.

A Call Management Server (CMS) is a fundamental network element for CGVoP Service. A CMS is typically involved in call control and signaling.

CGVoP Service is characterized by traditional telephony capabilities, such as*:*

- Local calling (which includes number portability)
- Toll calling
- Access to Interexchange Carriers for long distance calling
- Operator services including Operator Intercept and Busy Line Verification
- Directory Assistance
- Access to toll-free (800, 888, 877, etc.) services
- Emergency Services (911)
- N11 services (including 711 Telecommunications Relay Service)
- Integrated Services Digital Network (ISDN) services
- Advanced Intelligent Network (AIN) services

3.2 Service Features

CGVoP Service is also characterized by the availability of service features such as CLASS℠[5] features on an individual caller's line or Business Group features on a group of business lines. These features include, but are not limited to, the following:

- Call Forwarding (Selective Call Forwarding, Call Forwarding Variable, Call Forwarding Busy, Call Forwarding Don't Answer)
- Selective Call Acceptance/Rejection
- Calling Number Delivery/Blocking
- Calling Name Delivery/Blocking
- Call Waiting
- Customer-Originated Trace
- Multi-Way Calling
- Automatic Callback
- Automatic Recall
- Voice Mail
- Distinctive Alerting
- Anonymous Call Rejection
- Outgoing Call Restriction
- Multi-line Hunt Groups

3.3 Use of Service

The calls placed for CGVoP Service can be made using traditional end-user telephone sets or newer telephony technology. While it is a fact that new customer premise equipment (CPE) is available that enables callers to connect directly to a CGVoP network (commonly called "IP phones"), it is not necessary for end-users to purchase and connect such equipment in order to place calls on a CGVoP network. In addition, end-users using traditional telephone equipment, in most cases, are unaware that a CGVoP network is being used to process and transport their calls. The fact that a call is handled by a CGVoP network is generally transparent to end-users, making CGVoP Service appear practically identical to traditional circuit-switched voice telephony service.

[5] CLASS is a service mark of Telcordia Technologies, Inc. CLASS services are a group of subscriber services that provide selective-call screening, alerting, and calling-identification delivery functions. CLASS services take advantage of the calling-number information in common-channel signaling. In some cases, CLASS services are invoked apart from call setup and, therefore, use non-associated call signaling (i.e., signals generated apart from normal dialing).

3.3.1 Addressing Other Parties

For CGVoP Service, a common method by which one end-user addresses another end-user is dialing a standard telephone Directory Number (DN). The DNs assigned to subscribers of CGVoP Service with access to the PSTN are in the E.164 format. In North America, this number will be part of the North American Numbering Plan (NANP) in 10-digit DN format (NPA NXX-XXXX). However, a CGVoP network often has the capability to support an alternate dialing plan (or plans). The alternate dialing plan could provide connectivity to other customers on the same or other networks by using addressing schemes that are based, for example, on IP addresses rather than a traditional DN.

3.3.1.1 On-Net Calling

Providers of CGVoP Service have sought to implement enhanced services and features to be used between end-users served on the same CGVoP network. Consequently, there may be dialing techniques and capabilities such as abbreviated dialing or non-NANP numbers that are made available to end-users in addition to standard dialing capabilities. It is even possible that a separate dialing plan for on-net calls, applicable to all end-users served by the same CGVoP Service Provider, can be invoked distinct from the dialing plan used for off-net calling. This is not unlike the present capabilities on a PBX or Centrex. The key difference is that the unique dialing plan can be applicable for all end-users served by the same CGVoP Service Provider, even though there is no affiliation or association among the end-users other than that they are served by the same CGVoP Service Provider. The CMS would then have two separate addressing schemes for the end-user that the CMS may or may not directly associate internally. Calling where end-users can be connected without dialing a NANP DN is considered part of CGVoP Service.

3.3.1.2 Off-Net Calling

Off-net calling occurs when a call either changes from packet-mode to circuit mode (involving a wireline provider and/or Wireless Service Provider [WSP]) or the network service provider changes at some point in the call. Examples of how these conditions can occur are as follows:

1. The customer dials a NANP DN and the call is directed to a network element on the same service provider's circuit-switched (non-VoP) network. This is an off-net call because the call changes from packet-mode call to circuit-mode call.
2. The customer dials a NANP DN and the call is directed to a network element on another service provider's circuit-switched network. This is an off-net call because the call changes service provider and changes from packet mode to circuit mode.
3. The customer dials a NANP DN or signals another type of address (e.g., Session Initiation Protocol [SIP] Uniform Resource Locator [URL]) and the call is directed to another service provider's network that is a CGVoP network. This is an off-net call because different service providers are involved.

In general, it will not be necessary for customers to dial an access code to egress their CGVoP Service Provider's network. Again, most customers are likely to be unaware that their calls are processed and transported in a CGVoP network.

3.4 Types of Access

Figure 3-1 depicts a typical CGVoP network architecture and illustrates six common types of access to a CGVoP network. This architecture is presented solely for illustrative purposes and is not intended to confine CGVoP Service to services based on this architecture.

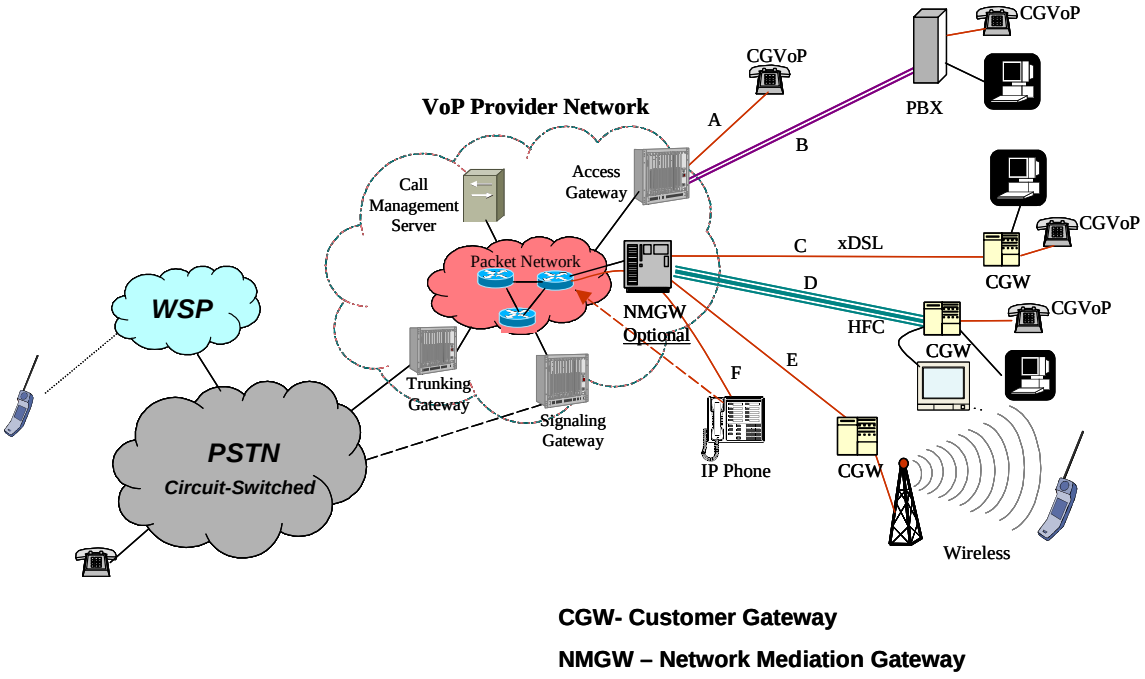

Figure 3-1: CGVoP Network Architecture

The following is a brief generic description of each access type represented in Figure 3-1:

A. Twisted pair copper loop with CGVoP Service capability (the equivalent of Plain Old Telephone Service (POTS) capability) – It is also possible to provide ISDN access in this manner rather than POTS.

B. Four-wire trunk-type connectivity for Private Branch Exchange (PBX) access – This provides access for multiple lines, any of which may be used for data and/or voice services, including CGVoP Service, configured at the PBX.

C. Twisted pair copper loop with digital signaling capability using the upper range of the line transmission above 4KHz (DSL) – Effectively providing digital connectivity including CGVoP Service.

D. Hybrid Fiber Coax (HFC) connectivity – The fiber/coax spectrum is broken down at the customer location using a set-top box or other equipment. This provides access for analog cable television connectivity, digital cable television connectivity and digital connectivity for Internet access and voice services, including CGVoP Service.

E. Wireless connectivity – Depending on the spectrum allocated and the technology used, wireless connectivity can include voice services, high-speed data, and Internet access. At the very least, it provides CGVoP Service.

F. IP phone connectivity – A direct digital packet connectivity is available from a phone set that converts speech into digital packet signaling. Typically, the IP phone accesses the CGVoP network via xDSL, HFC (Cable Modem access), or via a customer LAN.

As illustrated in Figure 3-1, there is different CPE associated with each of the six types of access shown. Note that some CPE associated with each access method can, at the customer's option, be used to make CGVoP calls, including voice-band voice calls, voice-band facsimile calls, and voice-band data calls. Some of this equipment can also be used to access other services/capabilities beyond the voice-band (e.g., a DSL line or an HFC connection). CGVoP Service, as defined in this document, is separate and distinct from these other services and capabilities outside of the voice-band range. CGVoP Service must meet a unique set of industry-defined quality, reliability, security and connectivity requirements that sets it apart from the other digital packet services to which the customer may have access.

The Access Gateway, Customer Gateway (CGW)[6], and Network Mediation Gateway (NMGW)[7] shown in Figure 3-1 can be a separate piece of equipment or may be an integral part of other pieces of network equipment. For access types A and B, the voice transmission for CGVoP Service enters the CGVoP network via an Access Gateway component. The Access Gateway converts the analog voice signal to digital packets. For access types C through F, the voice transmission for CGVoP Service is packetized by the Customer Gateway and enters the CGVoP network through the Network Mediation Gateway (which is an optional gateway since some networks may not implement this function). For access type F (IP phone connectivity), the equipment that performs this conversion/packetization is included as part of the CPE. Whenever a conventional PSTN phone is used to access the CGVoP network, equipment is needed somewhere outside of the telephone itself to perform this conversion. This network equipment could take the form of an Access Gateway or another piece of CPE (e.g., Customer Gateway). As the PSTN evolves toward a network of interconnected VoP components, the conversion of voice to digital packets may come to reside fully outside of any "formal" network equipment components such as an Access Gateway.

[6] Note that a Customer Gateway is typically located at the customer premises. In some cases, it may be just outside of the customer's premises. In addition, the CGW may be network owned or customer owned. The decision of which approach is used is a CGVoP Service Provider policy.

[7] A Network Mediation Gateway is a device that provides entry into the CGVoP Service Provider's network for call signaling traffic and voice media traffic. An NMGW may provide some or all of the following functions: enforcing traffic priority policy, enforcing encoding policy, providing conferencing capability, providing network-based call cut-through, and generating audible ringing for terminating calls. A CGVoP Service Provider may or may not implement an NMGW.

3.5 Call Processing in the CGVoP Network

Figure 3-1 also illustrates another distinctive technical characteristic of a CGVoP network. This is the separation of call/connection management from media routing/switching. It is the function of the CMS to keep track of *when* a call is made by a subscriber and *where* that call is to terminate, either on-net (within the CGVoP network boundaries) or off-net (somewhere in another network [e.g., PSTN]). Once the CMS has performed any call setup functions, it turns over the functions of media transport and routing to other media-related network components. The CMS tracks active calls based on the last information it receives from the Access Gateway, NMGW, and Signaling Gateway. The CMS does not handle the actual communications/media packets as they traverse the CGVoP network. It involves itself in the course of a typical call only when features are invoked that require its call processing capabilities. It is the job of the packet network to route the packets between the various gateways (or IP phones, in the case of access type F).

For CGVoP Service, the CMS typically performs the types of number translations that are performed in the PSTN. As examples, the CMS could translate a toll-free number to a routable number, or a speed dialing code (e.g., #2) to the corresponding directory number. The CMS could also perform number translations that are specific to a CGVoP environment. Translation of an E.164 number to a technology-specific identifier (e.g., H.323 address or SIP URL), and the subsequent translation of this identifier to a network address (e.g., IP address), is likely to become common with the introduction of ENUM (E.164 Number) databases.

3.6 CPE Capabilities

In CGVoP networks, certain key functionality and features are or could be provided by CPE.

In traditional circuit switches, the customer's line is activated in the switching system when the service is initiated. The line remains active (i.e., it can make or receive calls), until some work is done to deactivate the line. In a CGVoP network there is a concept of registration of the equipment making a call with the CMS. It is possible that the registration with the CMS is handled automatically by the CPE or by the network access equipment, but this is not always the case. Therefore, customers may have to proactively register their CPE with the CMS before being able to make or receive calls.

CPE could also support features commonly provided by network components. For example, in the PSTN, when a mid-call service like three-way calling or call waiting is invoked, a circuit switching system's central processor gets involved with managing the second call and bridging the three parties together (for three-way calling) or toggling between calls (for call waiting). In a CGVoP network, for access type A, and the low end of access types C, D, E, and F, the CMS or other centralized network component (e.g., a bridging server) will perform the same functions that a circuit switch does today, because the CPE is not capable of performing these functions. However, for the other access types and for more-capable customer premises-based equipment, it is possible that the CPE will perform these functions and in such a way that the CMS will have no specific knowledge that the use of the feature has taken place. In the three-way calling example, the CMS will know about both calls, but it may not know specifically that the two events are related to each other as a three-way calling event. In the call waiting example, the CMS will know about both calls, but it may not know which call is currently "active."

3.7 Interconnection to the PSTN

CGVoP calls may be placed to and received from subscribers in the PSTN. This requires that CGVoP networks be interconnected with the PSTN. Currently this means interconnection to mostly circuit-switched networks. Under the FCC's rules for interconnection of local telephone companies with long distance carriers, every LEC network is required to provide other interconnecting networks with a very specific grade of service from an inter-network trunking perspective. Therefore, a CGVoP network, if considered a LEC network or an integral part of a LEC's network, must provide a managed network fully capable of a sustainable and guaranteed level and quality of service (QoS) that meets these FCC regulations. This necessitates the presence of network management capabilities to ensure that the network meets industry and tariff standards and that the network does not fail or, if it does fail, does not propagate those failures to other interconnecting networks or into the PSTN as a whole. Therefore, CGVoP Service Providers build or lease transport and transmission facilities that allow their CGVoP networks to meet these industry requirements. Since the level and quality of service on the Public Internet does not currently meet these industry requirements, CGVoP calls are considered to traverse only carrier-provided packet-mode transport facilities and not the Public Internet.

3.7.1 Outgoing Calls

Currently, reaching DNs served by other provider networks requires the CGVoP network to interface with the circuit-switched PSTN. Figure 3-1 illustrates that the CGVoP network has two critical interfaces with the PSTN. The first interface is to the Signaling Gateway[8] that is used to set up calls directed out from the CGVoP network to the PSTN and those directed in for termination in the CGVoP network. The second interface is to the Trunking Gateway that carries the actual communications between the networks.

3.7.2 Incoming Calls

An off-net call incoming from a non-CGVoP network is first detected at the Signaling Gateway. Call setup information (a type of communication-identifying information) passes from the Signaling Gateway to the CMS. The CMS uses the NANP DN number it receives to identify its internal network address for that DN, determines where the call should terminate (commonly from registered address information) and the characteristics of the connection, and initiates ringing to alert the end-user of the incoming call. When the voice content packets arrive at a CGVoP network's Trunking Gateway from the PSTN, the packets are converted from circuit mode to packet mode. Conversion of the voice-band transmission to packet transmission and connection to the end user's CPE are the functions of the gateways and routers in the CGVoP network. As with outgoing calls, the CMS typically involves itself in an active call only when a recognized feature is invoked by the end user.

[8] In some configurations, a Signaling Gateway and Trunk Gateway may be co-located (e.g., in the case of an ISDN Primary Rate Interface (PRI) or a T1 trunk supporting Multi-Frequency (MF) signaling). In some architectures associated with certain signaling protocols (e.g., H.323 and SIP), a Signaling Gateway and Trunking Gateway are necessarily melded into a single gateway. In fact, in this latter case, the processing of signaling (including the call control signaling) is performed at the gateway.

4 Surveillance Events for Carrier-Grade VoP Service

This section presents the surveillance events for CGVoP Service. For each surveillance event, the event is defined, the occurrences of the event are identified and the information needed by law enforcement for the event is presented.

This section focuses on the communication-identifying information to which law enforcement needs access for surveillance events relevant to CGVoP Service. This section does not presume an implementation for providing law enforcement with access to this information.

The following assumptions were made in the development of the material contained herein:

1. The "calls" referred to in this section are CGVoP calls, and include both on-net and off-net calls (as described in Section 3.3).
2. There could be differing amounts of available information for particular surveillance events depending on whether a call is an on-net or off-net call, and whether a call is an originating, terminating or redirected call.
3. Event information for a particular surveillance event can be correlated to event information for previous associated surveillance events. As such, the set of event information identified in this section for a particular surveillance event does not include information elements that are presumed to be available for previous associated surveillance events.
4. The surveillance event that occurred will be known when accessing event information. Hence, the set of event information for each surveillance event defined herein does not include an event identifier.

The following surveillance events are addressed in this section:

- Registration/Authorization Events
  - Address Registration (Section 4.1.1)
  - Address De-registration (Section 4.1.2)
  - Mobility Authorization (Section 4.1.3)
  - Mobility De-authorization (Section 4.1.4)
- Call Management Events
  - Call Origination (Section 4.2.1)
  - Call Termination Attempt (Section 4.2.2)
  - Call Answer (Section 4.2.3)
  - Call Release (Section 4.2.4)
  - Address Resolution (Section 4.2.5)
  - Call Admission Control (Section 4.2.6)

  - Media Modification (Section 4.2.7)
- Signaling Events
  - Subject Signaling (Section 4.3.1)
  - Network Signaling (Section 4.3.2)
  - Post-Cut-Through Dialing/Signaling (Section 4.3.3)
- Feature Use Events
  - Call Redirection (Section 4.4.1)
  - Party Hold (Section 4.4.2)
  - Party Retrieve (Section 4.4.3)
  - Party Join (Section 4.4.4)
  - Party Drop (Section 4.4.5)
  - Call Merge (Section 4.4.6)
  - Call Split (Section 4.4.7)
- Communication Content Events
  - Content Delivery Start (Section 4.5.1)
  - Content Delivery Change (Section 4.5.2)
  - Content Delivery Stop (Section 4.5.3)
  - Content Unavailable (Section 4.5.4)
- Feature Management Events
  - Feature Activation (Section 4.6.1)
  - Feature Deactivation (Section 4.6.2)
- Surveillance Status Events
  - Surveillance Activation (Section 4.7.1)
  - Surveillance Continuation (Section 4.7.2)
  - Surveillance Change (Section 4.7.3)
  - Surveillance Deactivation (Section 4.7.4)

For each surveillance event, the specific case(s) for which the event is considered to occur and the information elements needed by law enforcement for the event are identified. For certain occurrence cases and information elements, examples of the case and information element are presented. Any sets of such examples are not intended to be exhaustive.

Any references to specific technologies within this section are for illustrative purposes only, and are not intended to limit the relevance of the corresponding surveillance event to these technologies.

4.1 Registration/Authorization Events

Law enforcement requires access to communication-identifying information for events pertaining to the registration of address information and the authorization of service use.

4.1.1 Address Registration

The Address Registration event occurs when an intercept subject attempts to register network address information. Note that the registration of a gateway (e.g., Access Gateway) that serves multiple users (including the intercept subject) is not considered an address registration for the intercept subject.

R-1 Law enforcement requires access to information for the Address Registration event when the intercept subject attempts to register network address information (whether or not the registration is successful).

R-2 Law enforcement requires access to the information contained in Table 4-1 when the Address Registration event occurs.

Table 4-1: Information for Address Registration Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Visited Provider Identity	Identifies the other service provider, when the network address information attempted to be registered is associated with another service provider.
Address Information	Address information that was attempted to be registered (e.g., E.164 telephone number, IP address, Asynchronous Transfer Mode (ATM) address, SIP URL).
Result	Indicates whether the address registration was successful or unsuccessful.
Failure Reason	Indicates the reason for an unsuccessful address registration, when address registration

Information Element	Description
	was unsuccessful.

4.1.2 Address De-registration

The Address De-registration event occurs when network address information for an intercept subject is de-registered. Note that the de-registration of a gateway (e.g., Access Gateway) that serves multiple users (including the intercept subject) is not considered an address de-registration for the intercept subject.

R-3 Law enforcement requires access to information for the Address De-registration event in the following cases:

1. **The intercept subject attempts to de-register network address information.**
2. **The CGVoP Service Provider de-registers network address information for the intercept subject (e.g., based on registration timeout).**

R-4 Law enforcement requires access to the information contained in Table 4-2 when the Address De-registration event occurs.

Table 4-2: Information for Address De-registration Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Visited Provider Identity	Identifies the other service provider, when the network address information attempted to be de-registered is associated with another service provider.
Address Information	Address information that was attempted to be de-registered (e.g., E.164 telephone number, IP address, ATM address, SIP URL).
De-registration Reason	Indicates the reason for address de-registration (e.g., requested, timeout)

Information Element	Description
	(e.g., requested, timeout).

4.1.3 Mobility Authorization

The Mobility Authorization event is the authorization attempt by an intercept subject with terminal or personal mobility to receive service. This event applies when the intercept subject has terminal or personal mobility in association with the CGVoP Service to which the intercept subject subscribes.

R-5 **Law enforcement requires access to information for the Mobility Authorization event in the following cases:**

1. **The intercept subject with terminal or personal mobility attempts to become authorized for service with a service provider other than the provider of the CGVoP Service to which the intercept subject subscribes (whether or not the authorization is successful).**
2. **The intercept subject with terminal or personal mobility attempts to become authorized for service in another service area with the intercept subject's CGVoP Service Provider or a different service provider (whether or not the authorization is successful).**

O-1 **Law enforcement desires access to information for the Mobility Authorization event when the intercept subject with terminal or personal mobility attempts to become authorized for service in the intercept subject's home service area (whether or not the authorization is successful).**

R-6 **Law enforcement requires access to the information contained in Table 4-3 when the Mobility Authorization event occurs per R-5.**

O-2 **Law enforcement desires access to the information contained in Table 4-3 when the Mobility Authorization event occurs per O-1.**

Table 4-3: Information for Mobility Authorization Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case

Information Element	Description
	Identity.
Visited Provider Identity	Identifies the other service provider, when another service provider is requesting authorization.
Network Address	Identifies the network node serving the intercept subject, when known.
Result	Indicates whether the authorization was successful or unsuccessful.
Failure Reason	Indicates the reason for an unsuccessful authorization, when authorization was unsuccessful.

4.1.4 Mobility De-authorization

The Mobility De-authorization event is the de-authorization of an intercept subject with terminal or personal mobility to receive service. This event applies when the intercept subject has terminal or personal mobility in association with the CGVoP Service to which the intercept subject subscribes.

R-7 Law enforcement requires access to information for the Mobility De-authorization event in the following cases:

1. **The intercept subject with terminal or personal mobility becomes de-authorized for service with a service provider other than the provider of the CGVoP Service to which the intercept subject subscribes.**
2. **The intercept subject with terminal or personal mobility becomes de-authorized for service in another service area with the intercept subject's CGVoP Service Provider or a different service provider.**

O-3 Law enforcement desires access to information for the Mobility De-authorization event when the intercept subject with terminal or personal mobility becomes de-authorized for service in the intercept subject's home service area.

R-8 Law enforcement requires access to the information contained in Table 4-4 when the Mobility De-authorization event occurs per R-7.

O-4 Law enforcement desires access to the information contained in Table 4-4 when the Mobility De-authorization event occurs per O-3.

Table 4-4: Information for Mobility De-authorization Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Visited Provider Identity	Identifies the other service provider, when another service provider is requesting de-authorization.
Network Address	Identifies the network node serving the intercept subject, when known.
De-authorization Reason	Indicates the reason for de-authorization (e.g., normal power-off, roamed out of service area).

4.2 Call Management Events

Law enforcement requires access to communication-identifying information for events associated with the management of a call.

4.2.1 Call Origination

The Call Origination event occurs when the intercept subject originates or attempts to originate a call.

R-9 Law enforcement requires access to information for the Call Origination event in the following cases:

1. **A call or call leg is originated by the intercept subject and routed toward an on-net or off-net destination.**
2. **The destination number for a call or call leg originated by the intercept subject is translated to another address (e.g., speed dialing number translation or toll free number translation).**
3. **A call is attempted by the intercept subject, but, after the intercept subject performs complete dialing or signaling of the destination address, the CGVoP network cannot complete the call.**

4. **A call is attempted by the intercept subject, but, after the intercept subject performs complete dialing or signaling of the destination address, the intercept subject abandons the call before it could be routed toward its on-net or off-net destination.**
5. **A call is attempted by the intercept subject, but the intercept subject does not perform complete dialing or signaling of the destination address (i.e., intercept subject dials or signals no or partial destination address).**
6. **A feature code is dialed or signaled by the intercept subject.**

R-10 Law enforcement requires access to the information contained in Table 4-5 when the Call Origination event occurs.

Table 4-5: Information for Call Origination Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Calling Party Identity	Identifies the originating party (e.g., E.164 number), when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Called Party Identity	Identifies the called party, when known.
Initial User Input	Identifies the input provided by the calling party as part of initial call setup.
Interim Translation Input	Identifies the input to a translation process, when different from the Initial User Input (e.g., toll free number that was translated from an Initial User Input of a speed-calling number [e.g., #12], SIP URL that was translated from an Initial User Input of an E.164 number [for ENUM]).
Location	Identifies the location of the intercept subject's terminal (e.g., cell site/sector and/or other geographic information), when the intercept subject has terminal or personal mobility and

Information Element	Description
	access to location information is authorized.
Transit Carrier Identity	Identifies the transit carrier, when a transit carrier is involved and the transit carrier identity is known.
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the media, when known.
Media Information	Identifies media characteristics (e.g., media format) for the call, when known.

Note (a): If the media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.2.2 Call Termination Attempt

The Call Termination Attempt event occurs when a terminating call attempt to the intercept subject has been detected. The Call Termination Attempt event occurs regardless of the disposition of the call (e.g., busy, answered, or redirected).

R-11 Law enforcement requires access to information for the Call Termination Attempt event in the following cases:

1. **An incoming call from an associate to the intercept subject is detected, regardless of the disposition of the call. This includes calls for which the intercept subject receives a call waiting notification tone.**
2. **A recall event involving the intercept subject is detected (e.g., hold recall, transfer recall, or attendant recall).**

R-12 Law enforcement requires access to the information contained in Table 4-6 when the Call Termination Attempt event occurs.

Table 4-6: Information for Call Termination Attempt Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.

Information Element	Description
Calling Party Identity	Identifies the calling party to the extent known.
Called Party Identity	Identifies the called party (e.g., E.164 number), when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Redirected-from Information	Identifies information about a previous redirection, when the incoming call has information about a previous redirection.
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the media, when known.
Media Information	Identifies media characteristics (e.g., media format) for the call, when known.

Note (a): If the media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.2.3 Call Answer

The Call Answer event occurs when a call or call leg has been answered. Transmission is usually cut-through in both directions to the intercept subject or its agent (e.g., voicemail system), due to the receipt of an off-hook indication from the terminating end-user, or other user-network interaction.

R-13 Law enforcement requires access to information for the Call Answer event in the following cases:

1. **The intercept subject answers a call or call leg that has not been previously answered by the intercept subject.**
2. **An agent of the intercept subject (e.g., password screening system) answers a call or call leg.**
3. **A call originated by an intercept subject is answered or cut-through in both directions.**
4. **A call redirected by the intercept subject (e.g., via call forwarding) is answered or cut-through in both directions.**
5. **The intercept subject or its agent answers a recalling associate (e.g., for hold recall, transfer recall or attendant recall).**

R-14 Law enforcement requires access to the information contained in Table 4-7 when the Call Answer event occurs.

Table 4-7: Information for Call Answer Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Answering Party Identity	Identifies the answering party or agent, when known.
Location	Identifies the location of the intercept subject's mobile terminal (e.g., cell site/sector and/or other geographic information), when the intercept subject has terminal or personal mobility and access to location information is authorized.
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the media, when known.
Media Information	Identifies media characteristics (e.g., media format) for the call, when known.

Note (a): If the media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.2.4 Call Release

The Call Release event occurs when a call, call appearance, or call leg is released. It indicates that network resources associated with the call have been released.

R-15 Law enforcement requires access to information for the Call Release event in the following cases:

1. **A call attempt is abandoned by the calling party (intercept subject or associate) or is unsuccessful.**
2. **A completed call is released (including abnormal release detected by the intercept subject's network).**

R-16 Law enforcement requires access to the information contained in Table 4-8 when the Call Release event occurs.

Table 4-8: Information for Call Release Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Release Cause	Identifies the reason the call was released, when known.
Location	Identifies the location of the intercept subject's mobile terminal (e.g., cell site/sector and/or other geographic information), when the intercept subject has terminal or personal mobility and access to location information is authorized.
Visited Provider Identity	Identifies the service provider, when the intercept subject is served by another service provider when the call is released.

4.2.5 Address Resolution

The Address Resolution event occurs when the CGVoP network performs or receives the results of an address resolution and sends the resulting address information to the intercept subject's equipment (e.g., user terminal), facilities, or service. The Address Resolution event also occurs when the CGVoP network performs or receives the results of an address resolution that has as the input and/or results in an address that identifies the intercept subject's equipment, facilities or service, and sends the resulting address information to an associate's equipment (e.g., user terminal), facilities or service (or any other network entity).

Occurrence of this event will depend on the network signaling protocol used by the CGVoP network. This event typically occurs in cases where the CGVoP network is not actively involved in call setup (e.g., for a SIP Redirection Server or certain H.323 Gatekeeper configurations). As an example, the Address Resolution event occurs when a SIP 3xx response (e.g., 302 Moved Temporarily) is sent to an intercept subject's equipment in response to an SIP INVITE request from the intercept subject.

When the CGVoP network performs address resolution or receives the results of an address resolution and uses the resulting address information to route the call, rather than returning the resulting address information to the originator, the results of the resolution would instead be

captured for the Call Origination event, Call Termination Attempt event, or Call Redirection event, depending on the nature of the address resolution and the direction of the call.

R-17 Law enforcement requires access to information for the Address Resolution event in the following cases:

1. **The CGVoP network performs an address resolution on behalf of the intercept subject or receives the results of an address resolution for the intercept subject , and sends the resulting address information to the intercept subject's equipment, facilities or service.**
2. **The CGVoP network performs an address resolution on behalf of an associate or receives the results of an address resolution for the associate, where the resolution input and/or result identifies an intercept subject's equipment, facilities or service, and returns the resulting address information to the associate's equipment, facilities or service.**

R-18 Law enforcement requires access to the information in Table 4-9 when the Address Resolution event occurs.

Table 4-9: Information for Address Resolution Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Subscriber Identity	Identifies the party for whom the address resolution was performed, when the address resolution was for the intercept subject and the identifier is more specific than the intercept subject identity associated with the Case Identity or when the address resolution was for an associate.
Resolution Input	Address information provided as input by the party for whom the address resolution was performed.
Resolution Output	Address information provided as output to the party for whom the address resolution was performed.

Information Element	Description
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the media, when known.
Media Information	Identifies media characteristics (e.g., media format), when known.

Note (a): If media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.2.6 Call Admission Control

The Call Admission Control event occurs when the CGVoP network interacts with an intercept subject's equipment, facilities or service regarding granting permission to the intercept subject to originate and receive calls. This event also occurs when the CGVoP network instructs an intercept subject's equipment, facilities or service to clear a call, or is notified by the intercept subject's equipment, facilities or service of the clearing of a call.

Occurrence of this event will depend on the network signaling protocol used by the CGVoP network (e.g., using the Registration Admission Status [RAS] protocol in an H.323-based network to control use of network resources).

R-19 Law enforcement requires access to information for the Call Admission Control event in the following cases:

1. **The CGVoP network receives a request from the intercept subject's equipment, facilities or service for permission to originate a call.**
2. **The CGVoP network receives a request from the intercept subject's equipment, facilities or service for permission to receive a call.**
3. **The CGVoP network receives a request from the intercept subject's equipment, facilities or service to clear a call.**
4. **The CGVoP network receives a confirmation from the intercept subject's equipment, facilities or service that a call was cleared.**

R-20 Law enforcement requires access to the information contained in Table 4-10 when the Call Admission Control event occurs.

Table 4-10: Information for Call Admission Control Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.

Information Element	Description
	detected.
Service Identity	Identifies CGVoP Service.
Admission Control Type	Identifies the type of call management transaction (i.e., call origination, call termination, or call clearing).
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Calling Party Identity	Identifies the originating party of the call, when known.
Called Party Identity	Identifies the called party of the call, when known.
Permission Request Result	Identifies the result of the call management transaction (e.g., permission granted or not granted), when the intercept subject requested permission to originate or receive a call.
Denial Reason	Indicates the reason for a denied request, when permission was not granted (e.g., insufficient network resources, poor account standing).
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the media, when known.
Media Information	Identifies media characteristics (e.g., media format) for the call, when known.

Note (a): If media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.2.7 Media Modification

The Media Modification event occurs when the CGVoP network determines that the media characteristics (e.g., media format) of an existing call involving the intercept subject is being modified. Occurrence of this event will depend on the network signaling protocol used by the CGVoP network (e.g., H.323).

R-21 Law enforcement requires access to information for the Media Modification event in the following cases:

1. **The CGVoP network receives a request for, or detects, modification of the media characteristics of an existing call involving the intercept subject.**
2. **The CGVoP network receives a request for, or detects, the addition or removal of a media stream for an existing call involving the intercept subject.**

R-22 Law enforcement requires access to the information contained in Table 4-11 when the Media Modification event occurs.

Table 4-11: Information for Media Modification Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Requested Media Modification	Identifies the requested changes to the media characteristics (e.g., media format, network addresses), when changes were requested.
Resultant Media Modification	Identifies the granted or detected changes to the media characteristics (e.g., media format, network addresses), when changes were granted.

4.3 Signaling Events

Law enforcement requires access to communication-identifying information regarding signals sent from or to the intercept subject.

4.3.1 Subject Signaling

The Subject Signaling event occurs when the intercept subject dials or initiates a signal to control a feature or service operation (e.g., call forwarding, call waiting, call hold and three-way calling). Even if user input may be uninterpretable and would result in no change in the control of the call, the Subject Signaling event is still considered to have occurred.

The subject signal could be in-band or out-of-band and could be call-associated or non-call-associated. However, the Subject Signaling event does not include post-cut-through information. Post-cut-through information is covered by the Post-Cut-Through Dialing/Signaling event as defined in Section 4.3.3.

R-23 Law enforcement requires access to information for the Subject Signaling event when the intercept subject, using the service under surveillance, dials or signals to control services or features provided by the serving system, whether or not sufficient input was provided and whether or not the call or signaling attempt was abandoned with partial or no input.

R-24 Law enforcement requires access to the information contained in Table 4-12 when the Subject Signaling event occurs.

Table 4-12: Information for Subject Signaling Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Subscriber Identity	Identifies the subscriber associated with the subject signal (i.e., the intercept subject), when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Subject Signal	Identifies the signal or dialing originating from the intercept subject.

4.3.2 Network Signaling

The Network Signaling event occurs when signals originated by the CGVoP network are sent toward the intercept subject. These signals could be in the form of audio, text or visual signals.

R-25 Law enforcement requires access to information for the Network Signaling event in the following cases:

1. **Alerting is applied toward the intercept subject.**
2. **An audible signal is applied toward the intercept subject (e.g., dial tone, busy tone, ringback tone).**
3. **Signaling information or a display message is sent toward the intercept subject (e.g., identifying calling name and number, redirecting party name and number, message waiting indicator).**
4. **Announcement is applied towards the intercept subject.**
5. **Any other call control/service control message/signal that might indicate call or service control progress or status is sent toward the intercept subject**

Examples of cases where the Network Signaling event occurs are (list is from TIA/EIA J-STD-025-A):

- Dial tone is applied indicating an intercept subject has gone off-hook and the CGVoP network is ready to accept address information from the intercept subject.
- Recall dial tone is applied indicating that an CGVoP network is ready to accept address information or other information from an intercept subject.
- Expensive route warning tone is applied indicating an intercept subject has accessed the Automatic Flexible Routing (AFR) feature and the CGVoP network selected outgoing route is designated as an expensive route.
- Busy tone is applied indicating an intercept subject-originated incomplete call attempt.
- Reorder tone or Congestion tone is applied indicating an intercept subject-originated incomplete call attempt.
- Receiver Off-Hook (ROH) tone is applied indicating the intercept subject has left the phone receiver off hook and the line is receiving permanent signal treatment. This tone is also used in place of ringing when an operator system needs to alert an off-hook line.
- Special Information Tone (SIT) is applied indicating an intercept subject-originated call has been routed to an announcement. SIT tones precede CGVoP network-generated announcements to permit the user and network equipment to detect the type of recorded announcement that follows the tone.
- Ringback tone or audible alerting is applied indicating an intercept subject-originated call attempt has progressed and the called party is being alerted.
- Barge-in tone is applied indicating someone is about to barge-in on the intercept subject's active call.
- Call-associated out-of-band signal that is normally perceivable (seen or heard) by the intercept subject, such as tone commands (i.e., tones off) or visual call status indicator.
- Alerting tone is applied indicating an incoming call attempt to the intercept subject.
- Distinctive alerting tone is applied to allow classification of incoming calls to the intercept subject based on the called number or based on the calling number.
- Reminder ring is applied to notify the intercept subject when a terminating call has been redirected.
- Call waiting tone is applied, indicating an incoming call to the intercept subject while the intercept subject is in the communications state with another call.
- Distinctive call waiting tone is applied to allow classification of incoming calls to the intercept subject, while the intercept subject is in the communications state with another call, based on the called number or based on the calling number.
- Confirmation tone is applied indicating the CGVoP network has received information and has processed the request, such as the activation or deactivation of a feature or service.

- Message waiting indicator tone is applied indicating message waiting services are available. This tone also indicates that the CGVoP network is ready to accept address information or other information.
- Denial tone (single 2.0 seconds burst of 480 Hz tone added to a 620 Hz tone) is applied towards the intercept subject indicating denial of a feature request.
- Signaling information is delivered to the intercept subject identifying calling name and number and redirecting party name and number.
- Alphanumeric information associated with a call is delivered to the intercept subject, such as text provided in the Q.931 display information element (e.g., calling name, redirecting name).
- Intercept tone or Mobile Reorder tone (alternating 440Hz and 620 Hz tones each on for 250 ms.) is applied toward the intercept subject.
- Answer tone is applied toward the intercept subject.
- Tones off. All tones off.
- Pip tone (four bursts (0.1 second on, 0.1 second off) of 480 Hz tone, and then off) is applied toward the intercept subject .
- Abbreviated Intercept tone (4 seconds of Intercept tone) is applied toward the intercept subject.
- Abbreviated Congestion tone (4 seconds of Congestion tone) is applied toward the intercept subject.
- Warning tone (a single 0.1 second burst of 480 Hz tone) is applied toward the intercept subject.
- Dial tone burst tone (a single 2.0 seconds burst of Dial tone) is applied toward the intercept subject.
- Standard announcement is applied toward the intercept subject as applicable per ANSI-41.
- Number Unobtainable tone is applied toward the intercept subject indicating that the dialed number is invalid or unobtainable.
- Authentication Failure tone is applied toward the intercept subject indicating that an authentication attempt has failed.

R-26 Law enforcement requires access to the information contained in Table 4-13 when the Network Signaling event occurs.

Table 4-13: Information for Network Signaling Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Subscriber Identity	Identifies the subscriber associated with the network signal (i.e., the intercept subject), when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Network Signal	Identifies the audio signals, visual signals or displayed text applied by the serving system, when the signals or text would normally be sensed by the intercept subject.

4.3.3 Post-Cut-Through Dialing/Signaling

The Post-Cut-Through Dialing/Signaling event occurs when the intercept subject dials or signals digits or other potential routing information after an on-net call is established within the CGVoP network or after an off-net call is connected to another provider's network. Post-cut-through information is information dialed or signaled by the intercept subject after the initial call setup is completed and the call path is cut-through in both directions. Law enforcement needs access to post-cut-through information that could represent routing information. However, a CGVoP service provider may report post-cut-through information other than routing information and has no obligation to determine which post-cut-through information actually led or could lead to routing.

R-27 Law enforcement requires access to information for the Post-Cut-Through Dialing/Signaling event when the intercept subject dials or signals digits or other potential routing information after a call originated by or terminated to the intercept subject is cut-through in both directions.

R-28 Law enforcement requires access to the information contained in Table 4-14 when the Post-Cut-Through Dialing/Signaling event occurs.

Table 4-14: Information for Post-Cut-Through Dialing/Signaling Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Post-Cut-Through Input	Identifies the input (e.g., digits) provided by the intercept subject after the call is cut-through in both directions.

4.4 Feature Use Events

Law enforcement requires access to communication-identifying information for surveillance events related to an intercept subject's use of service features. The surveillance events defined in this section focus on *what happens during the use* of particular service features, not on the features themselves.

4.4.1 Call Redirection

The Call Redirection event occurs when a call is redirected such that the intercept subject's equipment, facilities or service is involved in or aware of the call redirection. Call redirection occurs for service features such as call forwarding (e.g., call forwarding variable, call forwarding busy) and call waiting deluxe. Call redirection could also occur for an intercept subject having terminal or personal mobility to redirect calls to the subject's current location.

R-29 Law enforcement requires access to information for the Call Redirection event in the following cases:

1. **An incoming call attempt to the intercept subject is redirected.**
2. **A call originated, received or redirected by the intercept subject is subsequently redirected by an associate such that the intercept subject's equipment, facilities or service is aware of the redirection.**

Examples of Item 1 of the Call Redirection event defined in **R-29** are:

- The incoming call attempt is forwarded. Call forwarding covers any of several features that redirect a call to another directory number (or voicemail) if a certain condition is met (e.g., the line is busy). Call forwarding includes selective call forwarding, which is a type of call forwarding where the condition is complex and/or dynamic (e.g., routing based on calling party number, time-of-day, calling party location).

- The incoming call attempt is deflected. Call deflection is a redirection feature (e.g., call waiting deluxe) that allows the called party to interactively refuse an incoming call and send that call to another directory number, voicemail or an announcement.
- The incoming call attempt is to an intercept subject with terminal or personal mobility and is redirected to the intercept subject's current location.

Examples of Item 2 of the Call Redirection event defined in **R-29** are:

- An associate redirects an incoming call attempt (e.g., using call forwarding) that was originated by the intercept subject. In this case, the redirection by the associate might cause the subject's equipment, facilities or service to establish a media connection to the redirected-to party (instead of establishing a media connection to the associate).
- An associate redirects an incoming call attempt (e.g., using call forwarding) that was previously redirected by the intercept subject.
- An associate redirects an answered call (e.g., using call transfer) that was originated by the intercept subject. In this case, the redirection by the associate might cause the subject's equipment, facilities or service to establish a new media connection to the redirected-to party (in place of the original media connection to the associate).
- An associate redirects an answered call (e.g., using call transfer) that was previously redirected by the intercept subject.
- A call parked on the intercept subject's line (by the intercept subject or an associate) is retrieved using a line other than the intercept subject's line.
- A call parked by the intercept subject on a line other than the intercept subject's line is retrieved using a line other than the line against which the call was parked.

R-30 Law enforcement requires access to the information contained in Table 4-15 when the Call Redirection event occurs.

Table 4-15: Information for Call Redirection Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies the redirected call, call appearance, or call leg within a system.
Feature Identity	Identifies the feature for which the redirection occurred (e.g., call forwarding variable), when

Information Element	Description
	readily available.
Redirected-from Party Identity	Identifies the party (intercept subject or associate) who caused the redirection of a call, when this party is known.
Redirected-to Party Identity	Identifies the party to whom a call is redirected.
Transit Carrier Identity	Identifies the transit carrier, when a transit carrier is involved and the transit carrier identity is known.
Visited Provider Identity	Identifies the service provider to which the call has been redirected, when the intercept subject is currently served by another service provider.
Media Addresses[(a)]	Identifies the originating and/or terminating addresses (e.g., IP addresses) for the resultant media, when known.
Media Information	Identifies media characteristics (e.g., media format for the call, when known.

Note (a): If the media addresses are included in the Media Information element, it is not necessary to provide the Media Addresses information element.

4.4.2 Party Hold

The Party Hold event occurs when the intercept subject places a party on an active call on hold. Placing a party on hold occurs during the use of service features such as call hold, call waiting, three-way calling, conference calling, call transfer and call park.

R-31 Law enforcement requires access to information for the Party Hold event when the intercept subject places an active call on hold.

Examples of the Party Hold event defined in **R-31** are:

- The intercept subject invokes the call hold feature for an active call.
- Using the call waiting feature, the intercept subject places the current call on hold (and toggles to the other call).
- Using the three-way calling feature, the intercept subject places the initial call on hold (to originate the call to the third party).
- The intercept subject places a conference call on hold (to place a call to add another party).
- Using the call transfer feature, the intercept subject places the initial call on hold (to originate the call to the transfer-to party).

- The intercept subject parks a call.

When multiple parties on a call are placed on hold at the same time, the Party Hold event could be considered to occur either once for *each* held party or only once for *all* held parties.

R-32 Law enforcement requires access to the information contained in Table 4-16 when the Party Hold event occurs.

Table 4-16: Information for Party Hold Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies the call, call appearance, or call leg within a system for which a party(ies) was placed on hold.
Feature Identity	Identifies the feature for which the party hold occurred (e.g., call waiting), when readily available.
Removed Party Identity(ies)	Identifies one or more removed parties, when the parties have been temporarily removed from a call due to being placed in a held state for the call.
Communicating Party Identity(ies)	Identifies the party(ies) remaining in a communicating state on a call (i.e., excluding the removed and/or held party(ies)).

4.4.3 Party Retrieve

The Party Retrieve event occurs when a party who had been placed on hold is retrieved using the same facilities that were used to place the party on hold. The retrieval of a party could occur during the use of service features such as call hold, call waiting, three-way calling, conference calling and call park.

R-33 Law enforcement requires access to information for the Party Retrieve event when the intercept subject retrieves a call that was on hold.

Examples of the Party Retrieve event defined in **R-33** are:

- Using the call hold feature, the intercept subject retrieves a call placed on hold.

- Using the call waiting feature, through toggling between calls, the intercept subject retrieves a held call.
- Using the three-way calling feature, the intercept subject retrieves the first call (in merging the two calls).
- Using the conference calling feature, the intercept subject retrieves the held call(s) (in adding the new call/party).
- Using the call transfer feature, the intercept subject retrieves the first call (in transferring the call).
- Using the call park feature, the intercept subject retrieves a parked call.

When multiple parties on a call are retrieved from a held state at the same time, the Party Retrieve event could be considered to occur either once for *each* retrieved party or only once for *all* retrieved parties.

R-34 Law enforcement requires access to the information contained in Table 4-17 when the Party Retrieve event occurs.

Table 4-17: Information for Party Retrieve Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies the call, call appearance, or call leg within a system for which a party(ies) was retrieved from a held state.
Feature Identity	Identifies the feature for which the party retrieve occurred (e.g., three-way calling), when readily available.
Joined Party Identity(ies)	Identifies one or more party(ies) retrieved from a held state.
Communicating Party Identities	Identifies the parties who are able to communicate with each other on the call, including the retrieved party(ies).

4.4.4 Party Join

The Party Join event occurs when a new party joins an active call. A party can join a call during the use of service features such as conference calling.

R-35 Law enforcement requires access to information for the Party Join event when a *new* party joins an existing call involving the intercept subject.

A party is not considered to be a *new* party if the party had been previously put on hold and is added to the active call through retrieval from the held state (see Section 4.4.3 for the Party Retrieve event).

When multiple parties join a call at the same time (e.g., when an active conference call with multiple parties is merged with another active conference call), the Party Join event could be considered to occur either once for *each* joined party or only once for *all* joined parties.

R-36 Law enforcement requires access to the information contained in Table 4-18 when the Party Join event occurs.

Table 4-18: Information for Party Join Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Feature Identity	Identifies the feature for which the party join occurred (e.g., conference calling), when readily available.
Joined Party Identity(ies)	Identifies one or more parties who has/have joined a call.
Communicating Party Identities	Identifies the parties who are able to communicate with each other on the call, including the joined party(ies).

4.4.5 Party Drop

The Party Drop event occurs when a party drops off of a call, such that the call continues (without the dropped party). A party can drop off of a call during the use of service features such as three-way calling, conference calling and blind call transfer.

R-37 Law enforcement requires access to information for the Party Drop event when a party (intercept subject or associate) drops off of a call in which the intercept subject is involved.

Examples of the Party Drop event defined in **R-37** are:

- For an intercept subject-initiated multi-way call, a party other than the intercept subject hangs up, and the call continues (with the intercept subject and at least one other party).
- For an intercept subject-initiated multi-way call, the intercept subject drops a party from the call, and the call continues (with the intercept subject and at least one other party).
- For a blind call transfer, the intercept subject hangs up after transferring the call.
- For a call split, the intercept subject splits a call or call leg from a multi-way call. When a call is split, the "communicating" parties are those parties who remain on the "original" call after the call split, which is the call on which the intercept subject remains, and the "dropped" parties are those parties who are on the "separated" call after the call split.

The Call Release event (see Section 4.2.4) addresses the case where a call ends, including a multi-way or transferred call. Hence, the Party Drop event is not considered to occur when a call ends.

When multiple parties drop from a call at the same time (e.g., when an active conference call is split into two calls, each having multiple parties), the Party Drop event could be considered to occur either once for *each* dropped party or only once for *all* dropped parties.

R-38 Law enforcement requires access to the information contained in Table 4-19 when the Party Drop event occurs.

Table 4-19: Information for Party Drop Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Feature Identity	Identifies the feature for which the party drop occurred (e.g., blind call transfer), when readily available.
Dropped Party Identity(ies)	Identifies one or more dropped parties, when parties have been permanently dropped from a call.

Information Element	Description
Communicating Party Identity(ies)	Identifies the parties remaining in a communicating state on a call (i.e., excluding the dropped party(ies)).

4.4.6 Call Merge

The Call Merge event occurs when two or more active calls are merged. The merging of calls could occur during the use of service features such as three-way calling, conference calling and call transfer.

R-39 Law enforcement requires access to information for the Call Merge event when the intercept subject merges two or more active calls.

Examples of the Call Merge event defined in **R-39** are:

- Using the three-way calling feature, the intercept subject merges the two calls. Consultative call transfer, for which the subscriber waits for an answer to the second call before connecting the two parties, is considered to be a specific case of three-way calling.
- Using the conference calling feature, the intercept subject merges a new active call with the original active call.
- Using the blind call transfer feature, the intercept subject merges the original call with the second call.

R-40 Law enforcement requires access to the information contained in Table 4-20 when the Call Merge event occurs.

Table 4-20: Information for Call Merge Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Feature Identity	Identifies the feature for which the call merge occurred (e.g., subject-initiated conference calling), when readily available.
Previous Call Identities	Uniquely identifies the calls, call appearances, or call legs that were merged.

Information Element	Description
Resulting Call Identity(ies)	Uniquely identifies the call(s), call appearance(s), or call leg(s) that resulted from the call merge and the corresponding Content Identity(ies) [see Table 4-22] if applicable.

4.4.7 Call Split

The Call Split event occurs when one of the calls (or call legs) of a multi-way call is separated by the conference controller. The "separated call" will continue to exist outside of the multi-way call. This separation of a call is the opposite of the Call Merge event (see Section 4.4.4).

Of the two calls resulting from the splitting of the "original" call, one of the calls is considered to remain the "original" call and the other call is considered to be the "separated" call. After the call split, the "original" call is the call on which the intercept subject is an active participant, and the "separated" call is the call on which the intercept subject is *not* an active participant.

R-41 Law enforcement requires access to information for the Call Split event when the intercept subject splits a call or call leg from a multi-way call, thus creating a new call.

R-42 Law enforcement requires access to the information contained in Table 4-21 when the Call Split event occurs.

Table 4-21: Information for Call Split Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Feature Identity	Identifies the feature for which the call split occurred, when readily available.
Previous Call Identity(ies)	Uniquely identifies the call(s), call appearance(s) or call leg(s) that was/were split.
Resulting Call Identities	Uniquely identifies the calls, call appearances or call legs resulting from the split and corresponding Content Identity(ies) [see Table 4-22] if applicable.

4.5 Communication Content Events

Law enforcement requires access to communication-identifying information for surveillance events related to access to communication content. The surveillance events described in this section are only relevant when law enforcement has access to the communication content for the particular LAES.

The surveillance events addressed in this section and the corresponding communication content are relevant to any type of call, including two-party calls and multi-way calls.

4.5.1 Content Delivery Start

The Content Delivery Start event occurs when communication content delivery to law enforcement is being enabled for a call.

R-43 **For communication content interceptions, law enforcement requires access to information for the Content Delivery Start event when communication content delivery is being enabled for a call or call leg. This should occur after an intercept subject originates or receives a call or call leg but prior to cut-through of the communications between the intercept subject and associate. This could occur when the intercept subject places a multi-way call on hold and the intercept subject maintains access to the call.**

R-44 **For communication content interceptions, law enforcement requires access to the information contained in Table 4-22 when the Content Delivery Start event occurs.**

Table 4-22: Information for Content Delivery Start Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Content Identity	Uniquely identifies the communication content to be delivered to law enforcement, to enable correlation with the communication-identifying information.
Originating Media Information	Identifies the media characteristics of the call for the originating endpoint (i.e., the endpoint from which the call was originated), when communication content is delivered in a

Information Element	Description
	packetized form. This information must include the characteristics needed to process the communications content, such as: • Network Address (e.g., IP address) • Encoding Algorithm (e.g., G.711, G.728) • Media Transport Protocol(s) (e.g., Real-time Transport Protocol [RTP]) using the Audio/Video Profile [AVP]) • Encryption Algorithm • Encryption Key This information could be delivered in a bundled form (e.g., as for Session Description Protocol [SDP]).
Terminating Media Information	Identifies the media characteristics of the call for the terminating endpoint (i.e., the endpoint to which the call was terminated), when communication content is delivered in a packetized form. This information must include the characteristics needed to process the communications content, such as: • Network Address (e.g., IP address) • Encoding Algorithm (e.g., G.711, G.728) • Media Transport Protocol(s) (e.g., RTP/AVP) • Encryption Algorithm • Encryption Key This information could be delivered in a bundled form (e.g., as for SDP).

4.5.2 Content Delivery Change

The Content Delivery Change event occurs when there is a modification to the media characteristics (e.g., encoding algorithm, encryption algorithm, encryption key) of an existing call. The Content Delivery Change event is generated for surveillances that require the delivery of communication content and provides LEA collection equipment with the updated information needed to process the voice packets for the call, when communication content is being delivered in a packetized form.

R-45 **For communication content interceptions, law enforcement requires access to information for the Content Delivery Change event when the media characteristics of an existing call involving the intercept subject are being changed and communication content is being delivered in a packetized form .**

R-46 **For communication content interceptions, law enforcement requires access to the information contained in Table 4-23 when the Content Delivery Change event occurs.**

Table 4-23: Information for Content Delivery Change Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Content Identity	Uniquely identifies the communication content being delivered to law enforcement, to enable correlation with the communication-identifying information.
Originating Media Information	Identifies the media characteristics of the call for the originating endpoint (i.e., the endpoint from which the call was originated), when changed. This information must include the characteristics needed to process the communications content, such as: • Network Address (e.g., IP address) • Encoding Algorithm (e.g., G.711, G.728) • Media Transport Protocol(s) (e.g., RTP/AVP) • Encryption Algorithm • Encryption Key This information could be delivered in a bundled form (e.g., as for SDP).
Terminating Media Information	Identifies the media characteristics of the call for the terminating endpoint (i.e., the endpoint

Information Element	Description
	to which the call was terminated), when changed. This information must include the characteristics needed to process the communications content, such as: • Network Address (e.g., IP address) • Encoding Algorithm (e.g., G.711, G.728) • Media Transport Protocol(s) (e.g., RTP/AVP) • Encryption Algorithm • Encryption Key This information could be delivered in a bundled form (e.g., as for SDP).

4.5.3 Content Delivery Stop

The Content Delivery Stop event occurs when delivery of communication content to law enforcement is being disabled.

R-47 For communication content interceptions, law enforcement requires access to information for the Content Delivery Stop event when communication content delivery is being disabled for a call or call leg, including when a call or call leg is released or merged with another call or call leg. This could occur when the intercept subject retrieves a multi-way call from a hold condition.

R-48 For communication content interceptions, law enforcement requires access to the information contained in Table 4-24 when the Content Delivery Stop event occurs.

Table 4-24: Information for Content Delivery Stop Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.

Information Element	Description
Content Identity	Uniquely identifies the communication content being delivered to law enforcement, to enable correlation with the communication-identifying information.

4.5.4 Content Unavailable

The Content Unavailable event occurs when the CGVoP Service Provider determines that the provider does not have access to communication content for a particular call that is under communication content interception. For example, depending on implementation, this situation could occur for certain roaming or redirection cases.

R-49 For communication content interceptions, law enforcement requires access to information for the Content Unavailable event when the CGVoP Service Provider's network does not have access to the communication content for a call under surveillance.

R-50 For communication content interceptions, law enforcement requires access to the information contained in Table 4-25 when the Content Unavailable event occurs.

Table 4-25: Information for Content Unavailable Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Call Identity	Uniquely identifies a call, call appearance, or call leg within a system.
Unavailability Reason	Indicates the reason communication content is not available to the CGVoP Service Provider.

4.6 Feature Management Events

Law enforcement requires access to communication-identifying information for certain feature management surveillance events.

4.6.1 Feature Activation

The Feature Activation event occurs when a service feature (e.g., call forwarding variable) is attempted to be activated for an intercept subject. While, in general, feature activation could occur through direct mechanisms (e.g., dialing a vertical feature code [i.e., *XY], pressing a feature key) or indirect mechanisms (e.g., filling in a Web page form), the Feature Activation event is only considered to occur for indirect mechanisms. Attempts to activate a feature through direct mechanisms would be detected through the Call Origination (Section 4.2.1) and Subject Signal (Section 4.3.1) events.

The Feature Activation event only addresses feature activations that result in attempts to update the CGVoP Service Provider's network. Any feature activations that *only* result in attempts to update the CGVoP Service Provider's operations support systems (e.g., Billing System) are not addressed.

O-5 Law enforcement desires access to information for the Feature Activation event when the CGVoP network is attempted to be updated to reflect the activation of a service feature for the intercept subject through an indirect mechanism (whether or not the activation is successful).

O-6 Law enforcement desires access to the information contained in Table 4-26 when the Feature Activation event occurs.

Table 4-26: Information for Feature Activation Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case Identity.
Feature Identity	Identifies the feature that was attempted to be activated.
Feature Activation Information	Identifies information to be used by an activated feature (e.g., forward-to number for call forwarding), when such information is to be used by the feature. This information may or may not be supplied during the feature activation request.

Information Element	Description
Result	Indicates whether the feature activation was successful or unsuccessful.
Failure Reason	Indicates the reason for an unsuccessful feature activation, when feature activation was unsuccessful.

4.6.2 Feature Deactivation

The Feature Deactivation event occurs when a service feature (e.g., call forwarding variable) is attempted to be deactivated for an intercept subject. While, in general, feature deactivation could occur through direct mechanisms (e.g., dialing a vertical feature code [i.e., *XY], pressing a feature key) or indirect mechanisms (e.g., filling in a Web page form), the Feature Deactivation event is only considered to occur for indirect mechanisms. Attempts to deactivate a feature through direct mechanisms would be detected through the Call Origination (Section 4.2.1) and Subject Signal (Section 4.3.1) events.

The Feature Deactivation event only addresses feature deactivations that result in attempts to update the CGVoP Service Provider's network. Any feature deactivations that *only* result in attempts to update the CGVoP Service Provider's operations support systems (e.g., Billing System) are not addressed.

O-7 Law enforcement desires access to information for the Feature Deactivation event when the CGVoP network is attempted to be updated to reflect the deactivation of a service feature for the intercept subject through an indirect mechanism (whether or not the deactivation is successful).

O-8 Law enforcement desires access to the information contained in Table 4-27 when the Feature Deactivation event occurs.

Table 4-27: Information for Feature Deactivation Event

Information Element	Description
Case Identity	Identifies the intercept subject.
IAP System Identity	Identifies the network node containing the IAP.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Subscriber Identity	Identifies the subscriber to a service, when the identifier is more specific than the intercept subject identity associated with the Case Identity.

Information Element	Description
Feature Identity	Identifies the feature that was attempted to be deactivated.
Result	Indicates whether the feature deactivation was successful or unsuccessful.
Failure Reason	Indicates the reason for an unsuccessful feature deactivation, when feature deactivation was unsuccessful.

4.7 Surveillance Status Events

Law enforcement requires access to information regarding the status of a surveillance. Law enforcement needs access to the surveillance status at the activation and deactivation of surveillance, as well as on a periodic basis. Law enforcement also needs to know about changes to the status of a surveillance while it is active.

The following are the possible surveillance statuses:

- *inactive* – surveillance is not being performed.
- *active* – surveillance is being performed. A surveillance is active between the activation and deactivation of the surveillance. The following are the two possible specific surveillance statuses for an active surveillance:
  - *partially active* – ***not all*** of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.
  - *fully active* – ***all*** of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.

These statuses are addressed for the surveillance status events presented in this section.

4.7.1 Surveillance Activation

The Surveillance Activation event occurs when the CGVoP Service Provider activates a surveillance for an intercept subject for a particular LEA, based on the authorization submitted to the CGVoP Service Provider by the LEA.

When the surveillance activation occurs, the surveillance could have a *fully active* or *partially active* status.

O-9 Law enforcement desires access to information for the Surveillance Activation event when the CGVoP Service Provider activates surveillance for a particular intercept subject for a particular LEA.

O-10 Law enforcement desires access to the information contained in Table 4-28 when the Surveillance Activation event occurs.

Table 4-28: Information for Surveillance Activation Event

Information Element	Description
Case Identity	Identifies the intercept subject.
Reporting System Identity	Identifies the network node reporting the surveillance status.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Surveillance Status	Indicates whether the surveillance is *fully active* or *partially active* at the time that the surveillance status report is generated.

4.7.2 Surveillance Continuation

The Surveillance Continuation event occurs when the CGVoP Service Provider reports the status of an *active* surveillance to an LEA. At the time of reporting, an *active* surveillance could have a *fully active* status (if surveillance is being fully performed) or *partially active* status (if surveillance is being partially performed). This event occurs periodically, and occurs individually for every *active* surveillance (and only for *active* surveillances). The CGVoP Service Provider could perform this reporting at the same time (but individually) for every *active* surveillance or when an independently tracked period ends for each *active* surveillance.

O-11 Law enforcement desires access to information for the Surveillance Continuation event at the end of every period for which the CGVoP Service Provider is to report the status of an *active* surveillance.

O-12 Law enforcement desires a CGVoP Service Provider to be able to administer the period for which surveillance status reports are generated.

O-13 Law enforcement desires the default period for surveillance status reports to be 1 hour, and the period to be settable between 1 hour and 24 hours, in 1-hour increments.

O-14 Law enforcement desires access to the information contained in Table 4-29 when the Surveillance Continuation event occurs.

Table 4-29: Information for Surveillance Continuation Event

Information Element	Description
Case Identity	Identifies the intercept subject.
Reporting System Identity	Identifies the network node reporting the surveillance status.

Information Element	Description
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Surveillance Status	Indicates whether the surveillance is *fully active* or *partially active* at the time that the surveillance status report is generated.

4.7.3 Surveillance Change

The Surveillance Change event occurs when a change is made to the status of an active surveillance. Specifically, the event occurs then the status changes from *fully active* to *partially active* or from *partially active* to *fully active*. A variety of conditions (e.g., failure/recovery of an IAP) could cause the change in status.

O-15 Law enforcement desires access to information for the Surveillance Change event in the following cases:

1. **A *fully active* surveillance becomes *partially active*.**
2. **A *partially active* surveillance becomes *fully active*.**

O-16 Law enforcement desires access to the information contained in Table 4-30 when the Surveillance Change event occurs.

Table 4-30: Information for Surveillance Change Event

Information Element	Description
Case Identity	Identifies the intercept subject.
Reporting System Identity	Identifies the network node reporting the surveillance status.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.
Surveillance Status	Indicates whether the surveillance is *fully active* or *partially active* after the status change occurs.

4.7.4 Surveillance Deactivation

The Surveillance Deactivation event occurs when the CGVoP Service Provider deactivates a surveillance for an intercept subject for a particular LEA (i.e., the status of the surveillance has

become *inactive*), based on the authorization submitted to the CGVoP Service Provider by the LEA.

O-17 Law enforcement desires access to information for the Surveillance Deactivation event when the CGVoP Service Provider deactivates surveillance for a particular intercept subject for a particular LEA.

O-18 Law enforcement desires access to the information contained in Table 4-31 when the Surveillance Deactivation event occurs.

Table 4-31: Information for Surveillance Deactivation Event

Information Element	Description
Case Identity	Identifies the intercept subject.
Reporting System Identity	Identifies the network node reporting the surveillance status.
Time Stamp	Identifies the date and time that the event was detected.
Service Identity	Identifies CGVoP Service.

5 LEA Authorized Access to Communication-Identifying Information and Communication Content

This section presents law enforcement's needs for gaining authorized access to communication-identifying information and communication content.

5.1 Communication Content

This section presents the communication content that law enforcement needs access to for CGVoP Service and addresses law enforcement's needs regarding the state of the communication content.

5.1.1 Access to Communication Content

When legally authorized, law enforcement must have access to communication content for the intercept subject's use of CGVoP Service, regardless of the service architecture used in the communication, including cases where the communications between the intercept subject and associates are sent and received over separate channels, or may be accessed at different IAPs at different geographical locations in the service provider's network. Accessible communications includes communications originated by, terminating to, and redirected by the intercept subject's equipment, facilities, or service, including both two-party and multi-way communications.

Law enforcement agencies need access to communication content when the intercept subject's communication stream is placed on hold during a multi-way communication, but the remaining parties' communications continue to be supported by the intercept subject's equipment, facilities, or service. Law enforcement needs continued access to the remaining parties' communications as long as the carrier continues to carry the communications to/from the intercept subject's equipment, facilities, or service.

R-51 When law enforcement is legally authorized to access communication content for an intercept subject, law enforcement requires access to the following communications when and for as long as the intercept subject's equipment, facilities or service are involved in the communications:

- **Communications originated by, redirected by and terminated to the intercept subject's equipment, facilities, or service.**
- **Communications for two-party calls and multi-way calls, including when the intercept subject places a multi-way call on hold.**

To enable LEA collection systems to identify CGVoP communication content, the unique identifier assigned to the communication content by the CGVoP Service Provider must be provided with the content when the content is delivered in packetized form. This would be the same identifier that is populated in the Content Identity information element for the corresponding Content Delivery Start event (see Section 4.5.1) or Content Delivery Change event (see Section 4.5.2). This unique identifier is used to distinguish between multiple communication content streams that are simultaneously delivered to an LEA and to correlate the communication content to communication-identifying information.

R-52 When communication content is delivered to law enforcement in packetized form, law enforcement requires the unique identifier for the communication content to be provided with the communication content.

5.1.2 Communication Content Decoding, Decompression and Decryption

LEA collection systems must be able to properly understand communication content transmitted by the CGVoP Service Provider. Intercept subject communications are encoded, and could also be compressed and/or encrypted.

Section 103(b)(3) of CALEA addresses the obligation of a service provider regarding encryption of intercept subject communications. If the CGVoP Service Provider provides or controls encoding, compression and/or encryption for the intercept subject or at least is knowledgeable of this processing, the provider must either transmit the communication content in a decoded, decompressed and/or decrypted form, or provide the information (e.g., encoding method, compression method, encryption keys) needed by the LEA collection system to perform this processing.

R-53 When communication content is to be delivered to law enforcement, when the CGVoP Service Provider provides or controls encoding, compression and/or encryption for the intercept subject's communications or is knowledgeable of this processing, law enforcement requires the CGVoP Service Provider to either transmit the communication content toward the LEA collection system in a decoded, decompressed and/or decrypted form, or to provide to the LEA collection system the information necessary to decode, decompress and/or decrypt the communication content.

Law enforcement prefers that the CGVoP Service Provider perform any decoding, decompression and/or decryption prior to the transmission of communication content. This preference is greater if proprietary or specialized encoding, compression and/or encryption had been used.

O-19 With respect to R-53, law enforcement desires the CGVoP Service Provider to transmit the communication content toward the LEA collection system in a decoded, decompressed and/or decrypted form, especially if the encoding, compression and/or encryption is proprietary or specialized.

If the CGVoP Service Provider transmits the communication content toward the LEA collection system in an encoded, compressed and/or encrypted form and the encoding, compression and/or encryption is proprietary, the CGVoP Service Provider needs to make the proprietary algorithms available to law enforcement. Licensing of proprietary algorithms is beyond the scope of this document and would be handled between law enforcement and the licensor.

5.1.3 Non-Alteration of Communication Content

It is paramount that the CGVoP Service Provider ensures against alteration of communication content. A provider must not intentionally alter communication content, other than what is necessary for delivery to law enforcement (e.g., processing associated with the requirement contained in Section 5.1.2 and the objective in Section 5.3).

R-54 When communication content is to be delivered to law enforcement, law enforcement requires the CGVoP Service Provider to transmit the communication content toward the LEA collection system without altering the communication content or meaning (with the exception of any conversions and processing [e.g., protocol/encoding format changes, encryption] required for delivery to law enforcement).

5.2 Delivery Interface

This section addresses the interface used to transmit communication-identifying information and communication content toward a LEA collection system.

5.2.1 Transmission

Communication-identifying information and/or communication content must be transmitted to each LEA entitled to receive the information/content. Each LEA will work with the CGVoP Service Provider to arrange for this transmission.

R-55 Law enforcement requires the CGVoP Service Provider to transmit communication-identifying information and communication content toward the collection system designated by the particular LEA.

5.2.2 Interface Types

To best ensure timely availability of electronic surveillance solutions for CGVoP Service, it is highly desirable that standard, cost-effective and generally available interface types be employed for the delivery of communication-identifying information and communication content.

O-20 Law enforcement desires that the facilities, data communications protocols, and data format used for the transmission of communication-identifying information and communication content toward the LEA collection system be standard, cost effective and generally available.

It is highly desirable to law enforcement for CGVoP Service Providers to reuse or re-apply message formatting and encoding of communication-identifying information from existing specifications. Furthermore, it is highly desirable to minimize the number of physical transmission facilities used to transmit communication-identifying information and communication content toward the LEA collection system. The intention is to consolidate the number of interfaces with which law enforcement will need to comply.

O-21 Law enforcement desires that CGVoP Service Providers reuse or re-apply message formatting and encoding definitions (when appropriate) from existing relevant specifications for the transmission of communication-identifying information toward the LEA collection system.

O-22 Law enforcement desires that CGVoP Service Providers minimize the number of physical transmission facilities used to transmit communication-identifying information and communication content toward the LEA collection system.

For example, for certain CGVoP electronic surveillance solutions, several different types of IAPs may be involved in accessing communication-identifying information and communication content. The communications may be accessed not only at different IAPs, but possibly also at different geographical locations within the service provider's network. In these cases, law enforcement would prefer a connection from a single centralized delivery system to the collection system, rather than connections from each IAP involved in the surveillance.

5.3 Security of Communication-Identifying Information and Communication Content

It is vital that the CGVoP Service Provider take measures to protect the communication-identifying information and communication content as it is being transported. To ensure security and integrity, these measures must include separation of the information/content from public communications if any part of a CGVoP Service Provider's implementation uses network resources also used to support subscribers' traffic, and should include encryption of the information/content using suitable, commercially available key-exchange protocols and encryption algorithms. This encryption is for securing the communication-identifying information and communication content while it is being transported; it is not related to any necessary decryption of communication content resulting from the original encryption of the communications by the intercept subject and/or associate.

CR-1 **If any part of a CGVoP Service Provider's implementation uses network resources that are also used to support subscribers' traffic (i.e., shared network resources), law enforcement requires the communication-identifying information and communication content to be logically, physically or otherwise separated and protected from access by the Service Provider's subscribers.**

CO-1 **If shared network resources are to be used for the transmission of communication-identifying information and communication content toward an LEA collection system, law enforcement desires that the communication-identifying information and communication content be encrypted for transmission toward the LEA collection system using suitable, commercially available key-exchange protocols and encryption algorithms.**

CGVoP Service Providers are not expected to ensure a level of security for LAES beyond the capabilities of their own equipment.

5.4 Network Scope of LAES

A CGVoP Service Provider must perform LAES throughout the service areas operated by the provider. LEAs will coordinate delivery for each service area.

R-56 **Law enforcement requires access to an intercept subject's communication-identifying information and communication content (when authorized) for the intercept subject's communications occurring throughout the service areas operated by the CGVoP Service Provider served with the lawful authorization.**

5.5 Real-time, Full-time Monitoring

A CGVoP Service Provider must perform real-time monitoring of an intercept subject's communications. The term "real-time" refers to the ability to monitor and access communications concurrently with the transmission to or from the intercept subject's equipment, facilities, or service.

R-57 Law enforcement requires a CGVoP Service Provider to perform real-time monitoring of an intercept subject's communications.

A CGVoP Service Provider must perform full-time monitoring of an intercept subject's communications. The term "full-time" refers to the ability to monitor and access all service activity associated with the intercept subject on a 24 hour-per-day basis.

R-58 Law enforcement requires a CGVoP Service Provider to perform full-time monitoring of an intercept subject's communications.

5.6 Real-time Access

The immediacy with which the CGVoP Service Provider must provide access to the intercept subject's communications will vary according to aspects of the communications being accessed, as follows:

- For **communication-identifying information**, this will depend upon the nature of the communication-identifying information:
  - For information used to identify, direct and control the intercept subject's traffic, "real-time" refers to access that occurs concurrently with the establishment and control of a call or communications session. Access to communication-identifying information generated during call or communications session establishment shall be provided before, during or immediately after the transmission to or from the intercept subject.
  - For signaling that could affect service profile changes or subscriber account information changes, "real-time" refers to access that occurs as soon as the subject-signaled information is available to the service provider's network.
  - For subscriber and service subscription information, "real-time" refers to access that occurs as soon as the information is available to the service provider's network and can reasonably be made available to law enforcement.
- For **communication content**, "real-time" refers to access that occurs concurrently with the transmission of communications to or from the intercept subject (in other words, as the communication takes place).

In actuality, there is a small transmission or propagation delay from the moment the intercept subject's communications are intercepted until the moment the communications reach the LEA monitoring equipment.

6 General Surveillance Requirements

This section presents law enforcement's needs regarding the performance, quality, security, integrity and capacity for performing LAES for CGVoP Service.

6.1 Performance and Quality

CGVoP Service Providers must maintain a high level of performance and quality of service in facilitating LAES for law enforcement.

6.1.1 Reliability

Reliability is achieved through availability and fault management capabilities.

6.1.1.1 Availability

CGVoP Service is typically offered with specific levels of reliability as part of service-level agreements. However, CGVoP Service could also be offered with grades of reliability, such that there are no assurances provided for connection establishment or successful delivery of user packets to their intended destination. In these latter cases, the CGVoP network does not make any assurances on the quality or reliability of the service offered to the subscriber.

The required level of reliability of surveillances of the intercept subject's communications is dependent on the level of reliability provided for CGVoP Service.

R-59 When the CGVoP network assures the reliability of the intercept subject's service, law enforcement requires the reliability of the surveillance of the intercept subject's communications to be at least equal to the reliability of the intercept subject's service.

R-60 When the CGVoP network does not assure the reliability of the intercept subject's service, law enforcement requires the reliability of the surveillance of the intercept subject's communications to be higher than the reliability of the intercept subject's service.

Regardless of the level of reliability of the intercept subject's service, the transmission of communication-identifying information and communication content toward LEAs must be reliable.

R-61 Law enforcement requires that the transmission of communication-identifying information and communication content toward LEA collection systems be reliable.

CGVoP Service Providers must prevent disruption or termination of LAES. Law enforcement needs CGVoP Service Providers to establish plans for ensuring that system upgrades, software upgrades, and other network management procedures do not disrupt or terminate ongoing LAES.

6.1.1.2 Fault Management

Fault management capabilities are needed to detect and resolve problems affecting LAES. These capabilities must address problems associated with both the monitoring of intercept subject

communications and the transmission of communication-identifying information and communication content toward LEAs.

If the surveillance is disrupted or interrupted (e.g., due to equipment failure) during a surveillance of a subject's communication, but the subject's communications are not disrupted, the CGVoP Service Provider should restore the surveillance expeditiously and resume delivery of communication-identifying information and communications content.

6.1.2 Quality of Service

With regard to LAES, quality of service refers to the quality of the communications channel or system used to transmit communication-identifying information and communication content toward the LEA collection system. For example, quality of service may be measured based on quantitative factors, such as packet loss, bit error rate, or any other parameter used to measure communications quality.

R-62 **Law enforcement requires CGVoP Service Providers to achieve a quality of service for transmission of communication-identifying information and communication content toward LEA collection systems that is compliant with the quality-of-service standards of the CGVoP Service Provider for the CGVoP Service.**

6.2 Security and Integrity

Adequate security and integrity are achieved through transparency of surveillances, protection of controls and information/content, and procedural safeguards.

6.2.1 Transparency of Surveillances

It is paramount that CGVoP Service Providers maintain the transparency of surveillances. To meet law enforcement needs for transparency, the services and transmission characteristics provided to the intercept subject or any other subscriber should continue to comply with industry standards.

R-63 **Law enforcement requires each lawfully authorized electronic surveillance to be transparent to the intercept subject, the intercept subject's associates, and to all parties except the LEA(s) requesting the surveillance, and specific CGVoP Service Provider individuals involved in implementing the surveillance capability. At a minimum, the transparency of a surveillance must satisfy the following criteria:**

- **Indications that a surveillance is underway should not be discernible to anyone using the intercept subject facilities or any other parties.**
- **If the implementation of a surveillance occurs during an ongoing communication, the surveillance should not disrupt or interrupt the ongoing communication (that is, no interruption or alteration of communications shall occur on active channels).**

- **If the implementation of a surveillance causes changes in the operation of services and features, such changes should not be perceptible to the intercept subject or other parties.**
- **If any noise, packet loss, increased latency or error rate increase is introduced by the implementation of a surveillance, such noise, packet loss, increased latency or error rate increase should not be perceptible to the intercept subject or other parties.**

Law enforcement needs CGVoP Service Providers to notify the appropriate LEA upon learning that surveillance transparency was or may have been compromised. In such a situation, Service Providers should recognize that time is of the essence because the safety of the public and other law enforcement officers may be at risk.

Law enforcement recognizes that there may be cases where the intercept subject possesses sophisticated equipment that is capable of detecting LAES. To meet law enforcement needs for transparency, the services and transmission characteristics provided to the intercept subject or any other subscriber should continue to comply with industry standards.

6.2.2 Protection of Controls, Communication-Identifying Information and Communication Content

CGVoP Service Providers must protect the capabilities used to control LAES, and all communication-identifying information and communication content. Law enforcement requires this protection to be consistent with the provider's security policies and procedures for the prevention of unauthorized access, alteration, mutilation, manipulation and disclosure.

6.2.3 Procedural Safeguards

CGVoP Service Providers are expected to institute prudent procedures and apply technical solutions, where necessary, to maintain the confidentiality and transparency of LAES. Such measures should be consistent with the risk of compromising the information pertaining to LAES activities.

Examples of such procedural safeguards include:

- Restrictions on access to information about LAES capabilities.
- Physical security to limit access to systems controlling or supporting LAES.
- Security mechanisms for activating and deactivating surveillances or accessing captured communication-identifying information or communications content (e.g., via access passwords and possibly case-level security).
- Procedures to prevent subjects from being notified of service changes caused by the implementation of surveillances.
- Restriction of knowledge of surveillances to authorized service provider personnel (i.e., personnel with a "need-to-know").

6.3 Surveillance Capacity

CGVoP Service Providers must be capable of performing multiple, simultaneous surveillances within the service provider's CGVoP network and at each of its relevant network elements (IAPs) located throughout the CGVoP Service Provider's service areas.

The ability to perform multiple, simultaneous surveillances includes the following:

- Ability to access and monitor all simultaneous communications originated, received, or redirected by the intercept subject.
- Ability for multiple LEAs to monitor, simultaneously, the same intercept subject while maintaining transparency, including between agencies. Up to five LEAs must be able to simultaneously monitor the same intercept subject.
- Ability to simultaneously support a number of separate (i.e., multiple intercept subjects) lawfully authorized electronic surveillances, including different levels of authorization for each electronic surveillance (i.e., communication-identifying information only, or communication-identifying information and communication content).

6.4 Transmission Bandwidth

Individual LEAs are responsible, with the assistance of the CGVoP Service Provider, for ordering and acquiring sufficient transmission bandwidth from each CGVoP Service Provider in a timely manner for communication-identifying information and communication content to be delivered, such that the required number of intercept subjects and their service characteristics can be appropriately handled.

6.5 Access to Subscriber and Subscription Information

Law enforcement uses subscriber-identifying information (e.g., DN, login identifier, IP address, account numbers) and subscription information (e.g., service profile) for the intercept subject to effectively perform LAES. This information is obtained through various means, including subpoena, and is needed both prior to and during (for any changes) performance of LAES.

Subscriber-identifying information is used to verify the association of intercepted communications with the intercept subject (per the lawful authorization). Subscription information is needed to determine service features and capabilities the intercept subject might use and, correspondingly, how much transmission bandwidth should be allocated to perform the LAES. For these purposes, law enforcement may need documentation or other information, such as billing and subscriber account information.

References

Documents Referenced within Document

HR 4922, *Communications Assistance for Law Enforcement Act (CALEA)*, October 6, 1994.

Law Enforcement Requirements for the Surveillance of Electronic Communications, May 1995.

Packet Surveillance Fundamental Needs Document (PSFND) for Telecommunications Carriers, Equipment Manufacturers, and Providers of Telecommunications Support Services, Issue 1.0, October 31, 2001.

TIA/EIA J-STD-025-A, *Lawfully Authorized Electronic Surveillance*, December 1, 2000.

Other Documents

FCC 99-230, CC-Docket No. 97-213, *Third Report and Order*, released August 31, 1999.

FCC 02-108, CC-Docket No. 97-213, *Order on Remand*, released April 11, 2002.

PacketCable PKT-SP-ESP-I01-991229, *PacketCable Electronic Surveillance Specification*, Interim Release, December 29, 1999.

SCTE 24-13 2001, *IPCablecom Electronic Surveillance Standard*, May 22, 2001.

TIA/EIA J-STD-025, *Lawfully Authorized Electronic Surveillance*, September 2000.

TIA TR-45 00.08.30.39a, *CALEA Packet Surveillance JEM Final Report*, August 30, 2000.

Acronyms

ATM	Asynchronous Transfer Mode
AVP	Audio/Video Profile
CALEA	Communications Assistance for Law Enforcement Act
CGVoP	Carrier-Grade Voice over Packet
CGW	Customer Gateway
CLEC	Competitive Local Exchange Carrier
CMS	Call Management Server
CPE	Customer Premise Equipment
DN	Directory Number
DSL	Digital Subscriber Line
ENUM	E.164 Number
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
HFC	Hybrid Fiber Coax
IAP	Intercept Access Point
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LEC	Local Exchange Carrier
MF	Multi-Frequency
NANP	North American Numbering Plan
NMGW	Network Mediation Gateway
PBX	Private Branch Exchange
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transfer Protocol

SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS7	Signaling System Number 7
URL	Uniform Resource Locator
VoP	Voice over Packet
WSP	Wireless Service Provider

Glossary

agent – a network-based service or device that acts on behalf of a subscriber to send or receive communications (e.g., an interactive screening service, a reminder service, a delayed transmission service).

associate – a telecommunications user whose equipment, facilities, or services are used to communicate or attempt to communicate with the intercept subject.

call – a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used. A call may have one or more legs.

call deflection – a redirection feature (e.g., call waiting deluxe) that allows the called party to interactively refuse an incoming call and send that call to another directory number, voicemail or an announcement.

call forwarding – any of several features that redirect a call to another directory number (or voicemail) if a certain condition is met (e.g., the line is busy).

call leg – a bi-directional call path associated with each network facility usage attempt and subsequent usage.

call park – a feature that allows the subscriber to put an existing call on hold against another line and to pick up such a held call (from the line against which it was placed on hold or a different line).

call redirection – the use of a service feature to cause the termination of a call to an endpoint other than the original terminating endpoint. Call redirection includes call forwarding and call deflection.

call transfer – a feature that allows the subscriber to connect two other parties and then drop off the call. Call transfer includes blind call transfer, for which the subscriber does not wait for an answer before connecting the two parties (i.e., drops off immediately after dialing).

carrier-grade – indicates that the packet network is a managed network offering services and features that meet or exceed the levels of quality, reliability, security and connectivity found in the circuit switch-based PSTN.

Carrier-grade Voice over Packet (CGVoP) Service Provider – a service provider that offers carrier-grade voice services over its carrier-managed packet network.

communications –encompasses the term “electronic communications,” defined in 18, U.S.C. 2510(12) as “any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system, etc.” As used herein, the term also includes “wire communications,” defined in 18, U.S.C. 2510(1) as “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or

communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."

communication attempt – initiation of communication by the intercept subject or an associate.

communication content –encompasses the term "contents," defined in 18 U.S.C. 2510 (8) as "when used with respect to any wire, aural or electronic communications, includes any information concerning the substance, purport or meaning of that communication."

communication-identifying information – 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 the service provider. This includes, but is not limited to, directory numbers, call setup information, IP addresses, other routing or addressing information, and parameters of the signaling information that can be used as a means to subscribe to features of the service or activate features of the service, or establish and control a session or communication attempt.

cut-through – when an endpoint has received via call signaling the information needed to communicate.

held call – a call for which one or more parties have been placed on hold.

Intercept Access Point (IAP) – a point within a service provider's network where some of the communications or communication-identifying information of an intercept subject's equipment, facilities and services are accessed.

intercept subject – a telecommunication service subscriber (and other users of such service) whose communications, communication-identifying information, or both, have been lawfully authorized to be intercepted and delivered to an LEA. The information used to identify the intercept subject includes those inputs used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

Internet – collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate intelligence of all kinds by wire and radio.

Lawfully Authorized Electronic Surveillance (LAES) – the interception of communication content and/or acquisition of communication-identifying information. Government's legal authority to perform LAES was established through laws such as the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 3121 et seq.), which governs pen registers and trap and trace devices, and the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.), which governs interceptions of communication content and is commonly referred to as "Title III" or "the Wiretap Act." The use of this term in this document does not include administrative subpoenas for obtaining a subscriber's service usage records and information about a subscriber's service that a LEA may employ before the start of an authorized interception.

Law Enforcement Agency (LEA) – a government entity with the legal authority to conduct electronic surveillance (e.g., the FBI or a local police department).

merged call – a call resulting from the merging of multiple calls or call legs. For example, for three-way calling, the bridging of all three parties results in a merged call since it merges the original call with the new call (to the third party).

multi-way call – a call involving more than two parties, where the intercept subject initiated the addition of the other parties to the call. A multi-way call includes a three-way call and a conference call.

packet-based communication – user packet activity sent or received over the course of a communication.

packet-based service – a service that employs packet-mode technology.

packet-mode – a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s).

packet network – a network in which data is transmitted in units called packets.

retrieved call – a held call for which communication has resumed. For example, a call that has been held due to an intercept subject's use of the call waiting feature is considered to be retrieved when the intercept subject toggles back to the call.

service – a capability or set of capabilities offered by a service provider to end users, to which end users subscribe.

service feature – a capability offered by a service provider as part of a service, where such a capability cannot be used outside of the context of the service.

service scenario – the use of a service in a particular way and the particular chain of occurrences associated with this use.

service subscription – establishing with a service provider static information that uniquely identifies an end user, or an end user's equipment, facilities, or service.

surveillance event – an end-user action or related signal associated with the use of a service that is communication-identifying information or results in the generation of communication-identifying information..