

CALEA Compliance Guidance for WISPs

Copyright © 2007 Wireless Internet Service Providers Association (WISPA.org)

Document Revision Date: May 30, 2007

1. Introduction and Usage

1. This document is intended to define the interfaces between a Wireless Internet Service Provider's (WISP) Network Elements that provide wireless broadband Internet access services and a Law Enforcement Agency (LEA) so as to assist the LEA in conducting lawfully-authorized Electronic Surveillance in a manner that meets the requirements of the Communications Assistance for Law Enforcement Act (CALEA). While every attempt has been made to make the information contained in this document acceptable to all LEAs, there may be cases where a deviation from the guidance in this document is required.
2. This document describes the design parameters for a CALEA-compliant Network, as well as describes appropriate methods and locations within the Network where data interception, storage, and transmission of intercepted data must take place. While some of the information in this document may be useful for ISPs who provide wireline or cable-based Internet access services (DSL, cable, etc), it is targeted toward wireless Internet access service providers.
3. This document attempts to explain, where possible, both HOW and WHY certain steps are required.
4. This document describes some of the equipment that will be required in order to be capable of delivering the intercepted data to a requesting LEA, as well as the necessary formatting and methods for delivering intercepted data.
5. This document is not intended to be an industry standard definition and as such will not provide a "safe harbor" as defined by the FCC.
6. This document is NOT a tutorial that includes all the requirements for CALEA compliance. We document here ONLY the technical requirements.

2. Definitions

1. ***CALEA*** – The Communications Assistance for Law Enforcement Act. A statute that defines the statutory obligations of telecommunications carriers (including WISPs) to ensure that their equipment, facilities, and services that provide a customer or subscriber with the ability to originate terminate or direct communications are capable, pursuant to Lawful Authorization, of (1) isolating, and enabling the government to intercept, all of the wire and electronic communications of a subject; (2) isolating, and enabling the government to access, all call-identifying information that is reasonably available in your network contemporaneously with the transmission of a wire or electronic communication in a manner that allows it to be associated with the communication to which it pertains; and (3) delivering intercepted communications content and call-identifying information to Law Enforcement.
2. ***Call-Identifying Information/Communication-Identifying Information (CII)*** – Dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

3. **Communication Content** – Any and all information concerning the substance, purport, or meaning of a Subject/Target’s communications.
4. **Downstream Network** – The portion of the network where a WISP’s direct control ends, and a customer’s network begins.
5. **Electronic Surveillance** – The Interception and monitoring of communications – i.e., Communication-Identifying Information, Communication Content, or both – for a particular customer/subscriber pursuant to Lawful Authorization.
6. **Intercept/Interception** – See “Electronic Surveillance.”
7. **Law Enforcement** – Any officer of the United States or of a State or political subdivision thereof who is empowered to conduct investigations, make arrests, or otherwise enforce and ensure obedience of the law.
8. **Law Enforcement Agency (LEA)** – Any agency of the United States or of a State or political subdivision thereof that enforces the law, including local or [state police](#), and federal agencies such as the [Federal Bureau of Investigation](#) (FBI) and the [Drug Enforcement Administration](#) (DEA). It is an LEA that will deliver the Lawful Authorization to a WISP for action. Lawful Authorization – An order or other form of legal authorization (e.g., Pen Register/Trap and Trace Order, Title III Order, etc.) issued by a court or other competent authority authorizing the Interception of all or specific categories of a Subject/Target’s Traffic. The Lawful Authorization will contain information on the Subject/Target of the Interception, the Subject/Target Facility, the timeframes involved, and other information specific to the investigation at hand.
9. **Network** – The portion of the infrastructure that is controlled by a WISP.
10. **Network Element** – Equipment that is addressable and manageable, provides support or services to the user, and can be managed through an element manager. A group of interconnected network elements form a [network](#).
11. **Pen Register/Trap and Trace Order** – A form of Lawful Authorization that authorizes the Interception of information contained in the broadband communications of a Subject/Target via a Pen Register and/or Trap and Trace device/process (as defined in 18 U.S.C. §§ 3127(3) and (4)).
12. **Sniffer/Packet Sniffer** – A program that can “capture” network communications and either store them locally, send them via a streaming protocol to a remote server (where it can be viewed immediately or stored) or (in some cases) both.
13. **Subject/Target** – An individual who is the object of a Law Enforcement or LEA investigation and whose communications have been authorized by a lawful authorization to be intercepted and delivered to an LEA.
14. **Subject/Target Facility** – The equipment, facilities, and/or services of a Subject/Target, as identified by a unique identifier (e.g., the MAC address associated with the Subject/Target), and listed in the lawful authorization that authorized the Interception of the Subject/Target’s communications.
15. **Subject/Target Traffic** – All communications and IP data traffic, both on the Upstream Network and the Downstream Network, that is bridged at/by the Subject/Target Facility identified in the Lawful Authorization.

16. **Tap** – Historically a “Tap” was a hardware device used for transparently recording communications on a “line”. (Recording a telephone conversation). In this document, we describe two types of Taps. One is a hardware device that will perform the same function on a data network. Another use for the word “Tap” applies to a software Tap. For example, a Packet Sniffer that runs on your Linux-based AP (StarOS, Mikrotik, Imagestream, etc.) would be a software Tap. A special purpose hardware Tap would be (for example) an Imagestream or other Linux router with the OpenCALEA software running on it.

17. **Title III Order** – A form of Lawful Authorization that authorizes the Interception of any and all information concerning the substance, purport, or meaning of a Subject/Target’s communications. Upstream Network – The Internet...this begins where the WISP has no direct influence/control. The demarcation point (“demarc”) where a WISP’s Internet provider’s network ends.

3. Lawful Authorization

1. An LEA will serve a WISP with the necessary Lawful Authorization identifying the Intercept Subject, the communications and information to be provided, and service areas where the communications and information are to be provided. Once this Lawful Authorization is served on the WISP, the WISP must perform the Interception and delivery of the identified communications and information to the LEA via LEA-procured equipment, facilities, or services. This authorization can require up to ALL communications to and from the subject. Because of this requirement, network design choices made by the WISP are important, as these choices will affect HOW and WHERE (within the Network) the identified communications and information is intercepted/collected.

2. Transparency Requirement

- i. CALEA requires that Electronic Surveillance be facilitated and conducted unobtrusively and with a minimum of interference with the subscriber’s (Subject’s/Target’s) service.
- ii. Electronic Surveillance must be conducted in transparent manner, i.e., in a manner that prevents the Subject/Target or the Subject/Target Facility from detecting that an Intercept is being conducted. Service parameters (e.g. bandwidth, latency, availability) must not be impacted in any way by the Intercept.
- iii. The fact that an Interception is being conducted must be transparent (i.e., undetectable) to all non-authorized employees of the WISP, as well as to all other non-authorized persons.
- iv. The fact that there are or may be Interceptions being conducted by multiple different LEAs on the same Subject/Target must be transparent (i.e., undetectable) to each receiving LEA.

4. Network Design Considerations

1. Access Point Configuration Considerations

- i. Because wireless access points have the ability to allow two clients to communicate with one another, the WISP must be aware of the implications of access point configuration. For MOST access points, there is a parameter that will either allow or disallow clients of the same access point to communicate with each other directly. Some common names for this parameter are: interclient communications, interBSS

relay (StarOS and some other Linux based APs), and forwarding (Mikrotik). It is possible that the gear used will call this parameter something else. The main reason for concern is that in many cases (MOST), if this option is not set to disallow communications between clients, the WISP will not be able to sniff this traffic with most commonly available tools. The Packet Sniffer in StarOS and Mikrotik, for example, will NOT see data transmitted between two clients of the same AP unless they are on IP subnets that are different from each other. It is our recommendation, therefore, that this option be turned off on all access points, due to the extreme difficulty in gathering the lawfully-authorized data for a requesting LEA.

2. Bridged, Routed and NAT Network choices

i. Bridged vs. Switched

1. When a Network is bridged, this means that there are multiple devices that are physically on the same “collision domain”. When a network is switched it means that there are multiple devices which are on the same “layer 2 broadcast domain”. When either of these topologies are used it means that the same IP subnet can be used anywhere on the network. The IP network will not be subnetted.
2. 100% of the lawfully-authorized data to and from a Subject/Target customer in a bridged environment can be intercepted, at any point in the network because all packets are heard on all ports of all bridge devices in the backbone.
3. In order to be certain that 100% of the lawfully-authorized data to and from a Subject/Target customer in a switched environment can be intercepted, the point of collection MUST be at the Ethernet interface of the device providing the Subject/Target’s first hop onto the switched network. Usually this will be the access point where the Subject/Target is connected. Some network configurations may require the use of an ethernet switch capable of "port mirroring" for the data intercept.

ii. Routed

1. In a routed Network, lawfully-authorized data to and from a Subject/Target customer could be gathered based on his/her IP address. This means that the Tap should be set up at the head end of your Network, provided that it is impossible for the Subject/Target to communicate with another customer without passing that point on your Network.
2. In a routed Network, the Subject/Target’s IP will “ride” with the packet.

iii. NAT

1. This type of Network is difficult to handle. To gather the lawfully-authorized data from a NAT device, the Tap (hardware OR software) MUST be able to see the Subject/Target IP address BEFORE it is NATted. In other words, the Tap must be BEHIND the NAT device.
2. Some devices may have an option to NAT, but do not provide a mechanism to sniff the Network traffic. If such a device is being used, all traffic will have to be captured from the whole device (gathering data from multiple customers) and Subject/Target Traffic will be isolated and delivered to the LEA.

3. Many hotspot devices use NAT as well. For these devices, you may or may not be able to isolate a specific subject.

3. Network Management parameters

- i. There is some advance preparation that the WISP MUST begin **prior to** receiving a Lawful Authorization/Intercept Request. This is particularly important for facilitating compliance with CALEA's transparency requirements. There are many ways to accomplish this preparation, but the WISP must do it BEFORE being served with Lawful Authorization.

1. IP address information – DHCP

1. DHCP – If customers are provided with an IP by DHCP, the WISP must be able to identify that customer positively even if their IP address changes. **VERY IMPORTANT NOTE:** The WISP may alter their Network configuration now to move to one of the below DHCP design choices. The WISP MAY NOT ALTER the network configuration after being served with Lawful Authorization. Doing so would break the transparency requirement and thus fail to comply with CALEA's unobtrusiveness requirement because it could be detectable to the subscriber/customer who is now a Subject/Target. There are many ways to accomplish this, but listed here are a few suggestions.
2. RADIUS – Some DHCP servers support the provision of DHCP addresses from a RADIUS server. This allows for central management of IP address space and can (in some circumstances) make the positive identification process a bit easier. If the WISP is running a RADIUS server now, and their DHCP server supports this option, it may be a good investment to move over to this option.
3. Static DHCP addresses – most modern DHCP servers support the assignment of a static IP address to a specific MAC address. One advantage to this method is that the WISP will be able to document not only the IP address, but the MAC address of the client as well.
4. Documenting MAC addresses – If the WISP provides dynamic IP leases (“normal” DHCP operation), the WISP will, at the very least, be required to know the MAC address associated with all customers. With the MAC address documented, you will be able to view the “current” leases when you are served with Lawful Authorization and gather the IP address of the Subject/Target.

2. Routing – static and dynamic issues

1. If the WISP has a static routed Network, it is relatively easy to find a place in the Network to place the Tap. If the WISP has a dynamically routed Network, it may be more difficult to identify an appropriate location within the network to place the tap. The tap MUST be placed at a point in the Network where 100% of ALL lawfully authorized traffic can be captured to and from the Subject/Target customer. When required to intercept a Subject/Target's traffic, the WISP must be capable of intercepting ALL traffic to and from the subject, though the authorization may require less than 100% of the subject's traffic.

2. Typically mesh networks are dynamically routed using OSPF or similar routing protocol. If address pools are separately defined for each access point and NAT is not used, it will be possible to identify the AP where the Subject/Target connected and place the collection point immediately behind that AP. On metropolitan networks, for example, it will not suffice to place the Tap at any gateway node in the network, because inter-client communications are possible on the metro network. This is going to be a sticky problem for metro operators using the mesh architecture.

3. PPPoE/VLAN and other tunnels

1. If the WISP employs a tunneling technology within their Network design, it is possible to capture the target data at the termination point of the tunnel, depending upon the equipment used.

4. CPE gear with a built-in sniffer

1. Some gear built for CPE use has a built in Sniffer. This is the case for many of the Linux-based Network devices available today. Imagestream, Mikrotik, StarOS, WISP-DIST and many others have this capability built-in. Many of these devices can either store a file locally or stream the data to a central repository on your Network, or even stream the data directly to an LEA's receiver.

- i. If your CPE gear has a built-in sniffer, you may consider collecting the data directly from the CPE side. It is VERY IMPORTANT that the WISP does NOT cause a change in the way the target will perceive the Network behavior. Doing so would break the transparency requirement. Also, if data is collected on the CPE side, the target MUST NOT have access to the CPE gear's configuration.

- ii. Generally, it is not recommended to use this option, but it is worth mentioning due to the ease with which 100% data capture can be assured without regard to Network topology.

5. Encryption

1. If using encryption technology to protect Network data, or provide encryption services to customers/subscribers, the WISP must either deliver the intercepted communications to the LEA in unencrypted form OR provide information about the encryption algorithms used and the encryption keys to the LEA to enable the LEA to decrypt the intercepted communications. In other words, the WISP must provide the LEA with either the encryption key being used to do the encryption, or simply capture the traffic AFTER it has been unencrypted. The WISP is NOT required to decrypt any data for which they do not provide the encryption key.

2. Some examples regarding encrypted traffic

- i. If WPA is used to encrypt wireless links, the WISP must provide the LEA with a decrypted data collection. This is encryption that

the WISP is providing the keys for, so they must decrypt the information.

- ii. If your customer is running a VPN between two offices and the VPN stream is collected as part of the collection process (if collection is being done properly), the WISP will NOT be required to decrypt that VPN stream since they are not providing that encryption, but are merely a transport for that VPN.

6. Multiple Simultaneous Intercepts

1. The WISP must be able to provision multiple simultaneous Intercepts on a single Subject/Target.
2. The WISP must be able to provision multiple simultaneous Intercepts on multiple Subjects/Targets.

5. Data collection and delivery

1. CALEA does not specifically define a data format. The following describes Law Enforcement's preferred methods for data collection and delivery of that data under CALEA.

- i. Limitations to the data to be collected

1. WISPs building their Network to be compliant with CALEA, should bear in mind what information/data they will be directed to collect pursuant to a Lawful Authorization as well as HOW to collect that information/data and deliver it to the LEA. There are several scenarios that need to be addressed and many of them are dependant upon Network design as well as the specific gear used within the Network.

- ii. Data format

1. For Interceptions of all broadband communications services ***except for VoIP services:***

1. Data should be buffered and collected in PCAP format files, with Communication-Identifying Information (CII) and Communication Content separated into their own, separate PCAP files.
2. The PCAP format is an industry standard format that contains all the information required for a specific capture. Standard Linux distributions (and many of the existing Linux routers and access point gear) have a built-in packet Sniffer that will capture and record data in this format. This type of equipment can be used to capture the data.
3. On a Linux system, there are several programs that can accomplish this type of capture including:
 - i. tcpdump – This is a command line program that will sniff the Network traffic and store it in PCAP format. The following command-line is an example usage for tcpdump

1. `tcpdump -i eth0 -e -n -s0 -w SOMEFILE`

- ii. Refer to the document titled “WISPA Store and Forward IP Collector” by Michael Erskine for more information on using tcpdump for lawfully authorized data collection. That document, also, contains information on storage and delivery of collected data.
 - iii. Ethereal – is a graphical program with versions available for both Windows and Unix-like systems. It can perform a similar function to the tcpdump program, although you will be gathering data from a graphical interface.
2. For Interceptions of VoIP services where the WISP is providing both the Internet access service *and* the VoIP service to the Subject/Target subscriber, the intercepted information should be streamed LIVE (real-time) to the LEA’s collector. In this case, the WISP will require a program like OpenCALEA. The OpenCALEA software is a framework written by Merit Network, Inc. and extended by Imagestream to make it a complete solution for CALEA data collection and delivery. This software is an open source solution that will run on any Linux server and provide the WISP with a complete, tested and approved CALEA solution.