WISPA-CS-IPNA-2.0

WISPA CALEA Standard
IP Network Access (IPNA)
Version 2.0

Effective Date: May 1, 2009

WISPA CALEA Standard for IP Network Access

 Please send comments and corrections regarding this standard to:

caleaquestions@wispa.org

or by written correspondence to:

WISPA CALEA Committee
c/o John Scrivner
PO Box 1582
Mt. Vernon, IL 62864

WISPA CALEA Committee Members

FBI Contributing Committee Members:

Maura Quinn, FBI CALEA Implementation Unit
Michael Bilca, FBI CALEA Implementation Unit (Tridea Works)
Ken Coon, FBI CALEA Implementation Unit (Tridea Works)

Chairman: Marlon Schafer, Odessa Office Equipment

Other Committee Membership in Alphabetic Order by Surname

Brent Anderson, Great American Networks
Norm Brandinger, Global Online Electronic Services
Jeff Broadwick, ImageStream
Kent Claussen, BearHill Security
Michael Erskine, Kaballero.com, LLC
Butch Evans, Butch Evans Consulting
Martha Huizenga, DC Access, LLC
Timothy Kery, BearHill Security
Jesse Norell, Kentec Communications, Inc.
Eric Plikuhn, ImageStream
John Scrivner, Mount Vernon Net
Kris Toomey, Law Offices of Kris E. Twomey P.C.
John Tully, Mikrotik
J.C. Utter, ImageStream
Edward H. Winters, Yellowstone Media Design
Scott Yoder, ImageStream

This document is available from the WISPA website, www.wispa.org, at:

http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-2.0.pdf

This standard may be revised and superseded at any time. Please be sure to check the WISPA Web site at http://www.wispa.org/calea/WCS/ for the latest revision of the WISPA CALEA IPNA standard.

Table of Contents

Table of Figures

Table of Tables

1. Document Scope

1.1 Introduction

This document outlines Law Enforcement requirements in the IP Network Access (IPNA) intercept space. It defines the logical intercept architecture, presents general and architectural element-specific requirements, and describes a method for delivery of intercept communications.

1.2 Document Structure

- Section 3, *Functional IP Network Access Interception Architecture* presents the general functional layout of an IP Network Access intercept solution, and defines logical functions and interfaces upon which later sections place specific requirements.
- Section 4, *General Intercept Requirements* presents generic requirements that apply to the network of a Wireless Internet Service Provider (WISP) involved in an IPNA intercept.
- Section 5, *Intercept Categories* presents a categorization of intercept data that corresponds to the gradation of legal instrument in common use currently. A "Limited Broadband Intercept" category of intercept data is defined, corresponding to a legal instrument that authorizes the collection and delivery of restricted Communication Identifying Information (CmII) to the exclusion of Communication Content (CmC) (akin to traditional "pen" or "trap and trace" orders), and a "Full Content Broadband Intercept" category of intercept data is defined, corresponding to a legal instrument that authorizes the collection of delivery of full CmC and CmII (akin to a traditional "Title III" order).
- Section 6, *Interface "a" Requirements* presents specific requirements on the Interface "a" defined in Section 3.
- Section 7, *File Structuring Function Requirements and File Format* presents specific requirements on the File Structuring Function defined in Section 3.
- Section 8, *Interface "b" Requirements* presents specific requirements placed on the Interface "b" defined in Section 3.
- Appendix A, libpcap Format describes the pcap file format used to store CmC for Full Content Broadband Intercepts.
- Appendix B, Out-of-Band Event Mapping provides a set of mappings of events for several address assignment protocols and other CALEA standards to the WCS (WISPA CALEA Standard) IPNA standard.
- Appendix C, Event Parameters and XML (Extensible Markup Language) Messages describes the Out-of-Band Event message contents, defines the XML schema to describe them, and provides example XML instance documents.

1.3 Scope and Future Considerations

Various topics have not been specifically addressed in the current version of this standard, which may be the subject of further consideration and addressed in a future standard or later version of this standard. These include:

- Internet Protocol version 6 (IPv6). The standard IPv6 address syntax is allowed to be reported, and as such this standard should be usable with an IPv6 network, but no specific consideration has been given to address any other related issues in this version of the standard.
- Stream Control Transmission Protocol (SCTP). The protocol and port numbers should be reported as with TCP; no facility has been made to report individual message streams within a flow, as they are not considered a separate flow under this version of the standard.

- Multicast. Not specifically addressed. Partial support is achieved by capturing the packets or reporting the Packet Signatures of the traffic, but this will not cover multicast group joins and leaves, which can be difficult to ascertain from the network, and may be addressed in a later version of the standard. Multicast traffic that is transport for an IPTV service is to be excluded from capture if possible (see IPTV below), but all multicast traffic that is a part of a subscriber's Internet access is to be included.
- Virtual Private Network (VPN)/Encryption. The VPN Security Association messages should be sufficient for use with IPsec; other VPN technologies may be used as well but have not been given specific consideration in the current version of this standard.
- IP Transport of Non-Internet data. CALEA has been interpreted to apply to "broadband Internet access providers;" IP is sometimes used as a local transport for traffic other than "Internet access;" this standard does not apply to such traffic. An example of such traffic is IPTV (see below).
- Voice over Internet Protocol (VOIP). Not covered by the IPNA series of WISPA CALEA Standards. A carrier who provides both Internet access and VOIP service is subject to CALEA for both; in such a circumstance, this IPNA standard can be used as a component of the overall CALEA solution, but is insufficient in itself, and cannot be used to address the VOIP service. An external VOIP service contained within the Internet access traffic of an intercept subject is not treated differently than any other Internet access traffic, and should be reported or captured in the same manner.
- Internet Protocol Television (IPTV). Television program content provided via IP packet transport is to be excluded from capture and reporting when it is not Internet Access. Content delivered to an IPTV settop box that is considered or is substantially similar to Internet Access is subject to capture, such as access to email, websites, peer-to-peer content sharing, internet videos, weblogs, etc.

2. Acronyms and Definitions

2.1 Acronyms

AAA	Authentication, Authorization, and Accounting
ACK	Acknowledge Character
AF	Access Function
ATIS	Alliance for Telecommunications Industry Solutions
CALEA	Communication Assistance for Law Enforcement Act
CBIS	Cable Broadband Intercept Specification
CF	Collection Function
CHAP	Challenge Handshake Authentication Protocol
CmC	Communication Content
CmII	Communication Identifying Information
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
FCC	Federal Communications Commission
FSF	File Structuring Function
GMT	Greenwich Mean Time
IAP	Intercept Access Point
IAS	Internet Access Services
ID	Identity/Identifier
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPNA	IP Network Access
IPTV	Internet Protocol Television
IPV6	Internet Protocol Version 6
L2TP	Layer 2 Tunneling Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
MAC	Media/Medium Access Control
NACK	Negative Acknowledge Character
OoB	Out-of-Band
PAP	Push Access Protocol
PCAP	Packet Capture
PPP	Point-to-Point Protocol
PPPoA	PPP-over-ATM
PPPoE	PPP-over-Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SHA	Secure Hash Algorithm
SHA256	Secure Hash Algorithm which is 256 bits long
SCTP	Stream Control Transmission Protocol
SFTP	SSH File Transfer Protocol
TCP	Transmission Control Protocol
UTC	Universal Time Coordinated
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WCS	WISPA Calea Standard
WISP	Wireless Internet Service Provider[1]
XML	Extensible Markup Language

2.2 Definitions

Appropriate Legal Authorization – A Broadband Intercept Order or other authorization, pursuant to [18 U.S.C. 2518], or any other relevant federal or state statute.

Authentication – A method by which a network confirms a user's identity.

Authorization – The process by which a network grants access to resources to a user. Usually follows Authentication.

Broadband Intercept Order – A court order signed by a judge, magistrate, or other authority with jurisdiction that authorizes the interception of the broadband-based wire or electronic communications of a Subject or Target.

[1]This standard may be used by any Internet provider to whose network it may be applied, whether wireless or not.

Case Identity – Identifies the specific intercept of a Subject. This identity remains constant for the entire surveillance period.

Flow – A set of packets sharing the same Flow Signature. Also referred to as a Stream.

Flow Signature – The ordered set of packet header parameters that uniquely identify a flow. The parameters are the source and destination IP addresses, IP protocol and the source and destination port numbers if present[2] and applicable to the protocol.

Full Content Broadband Intercept Order – A Broadband Intercept Order that authorizes the interception of any and all information concerning the substance, purport, or meaning of the broadband communications of a Subject or Target.

Intercept Access Point – A point within an WISP domain where some of the Communications Content or Communications Identifying Information of an intercept subject's equipment, facilities, and services are accessed.

Internet – The public Internet.

Law Enforcement – Law Enforcement, as represented by FBI CALEA Implementation Unit

Law Enforcement Agency – A local, state, or federal law enforcement agency.

Limited Broadband Intercept Order – A Broadband Intercept Order that authorizes the interception of limited information contained in the broadband communications of a Subject or Target. This information includes Out of Band data and Packet Signature data.

Location – Information relating to the geographic, physical, logical or network location of an interception subject.

Non-repudiation – The process by which one ensures that a subject cannot deny taking part in a communication.

Quality of Service – Quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate, packet dropping probability, etc.

Session – In the scope of this document, a "session" or "communication session" is the totality of communications performed by a subject from the moment of network authorization to the point of network de-authorization (it is not, for example, the more restricted TCP session definition).

Stream – See "**Flow.**"

SFTP/SSH – SSH File Transfer Protocol (SFTP) over SSH2 (Secure Shell), the protocol use by this standard[3] for securely transferring files.

Subject – An individual who is the object of a LEA investigation and whose broadband communications and/or communications sessions are being intercepted pursuant to a Broadband Intercept Order.

Target – See "**Subject**."

Validation – A process by which one can ensure that the communication intercepted is indeed associated with the correct subject.

Wireless Internet Service Provider – An entity that offers IP Network Access service to customers. This definition includes, but is not limited to, entities that provide Broadband Internet access to customers/subscribers via a wireless network (wi-fi).

[2]IP packet fragments which do not include port numbers are reported as a Flow Signature without port numbers.

[3]This standard requires SFTP version 4 or later.

3. Functional IP Network Access Interception Architecture

Figure 1 depicts the functional IP Network Access interception architecture:

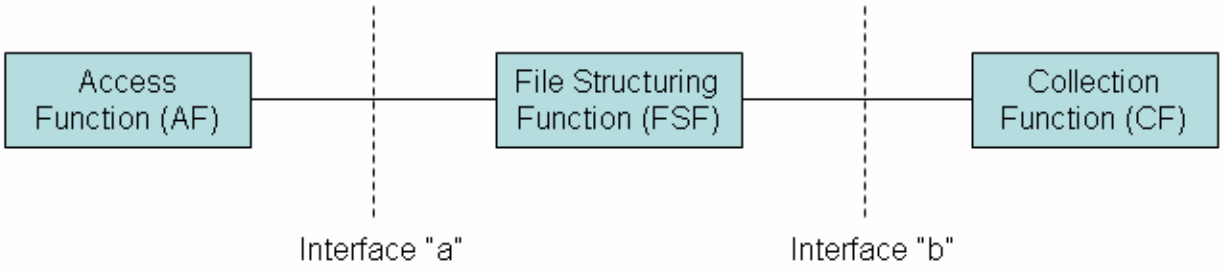


Figure 1 - Functional IP Network Access Intercept Architecture

This document describes in detail Interface “a”, the File Structuring Function (FSF), and Interface “b.” Although some requirements in this document apply to the Access Function (AF) (e.g. isolation of the subject data), it is not described here in detail. The Collection Function (CF) is not described in this document.

In general, the AF isolates the subject stream and forks a copy of it towards the FSF across Interface “a,” along with event messages generated in the network. The FSF correlates the received information and strictly structures it according to this document. The FSF then makes the structured intercept available to the CF across Interface “b,” using SFTP/SSH. The CF then pulls the structured intercepts from the FSF at a later time.

Sections 6, 7, and 8 of this document, respectively, formalize these roles by specifying strict engineering requirements on these three elements of interest:

- Interface “a,” in Section 6,
- File Structuring Function, in Section 7,
- Interface “b,” in Section 8.

Implementations may vary; the AF may need to be distributed across several IAP’s to ensure access to all packets to/from a Subject at all times. The AF may capture locally and perform formatting prior to delivery to the FSF across the “a” interface; alternatively it could capture locally to a pcap file which is subsequently delivered to the FSF across the “a” interface for processing; it could likewise be implemented via live streaming from AF to FSF across the “a” interface, for collection, processing and presentation at interface “b”. The AF and FSF may well be a single machine performing both functions. The limitations are in the timing constraints, and the formatting/presentation of captured data, as specified herein, not in the specific means of acquiring or transferring the data to the FSF.

4. General Intercept Requirements

4.1 General Requirements

This section presents general requirements that apply to a WISP involved in an IPNA intercept.

Requirements 40 through 140 can be related chronologically: Authentication must be performed at the inception of an intercept; Validation is a means to verify during an intercept that an intercepted stream is associated with the subject's equipment, facilities, or service; and Non-Repudiation provides a mechanism to verify and prove after the fact that an intercept was indeed associated with the subject's equipment, facilities, or service.

In unusual cases it may be impossible to perform one or more of these functions. The WISP is expected to make a best effort attempt to satisfy these requirements.

4.1.1 Transparency

R-10 The WISP shall perform the intercept in such a manner that the subject or the subject's terminal equipment cannot detect that the intercept is being performed. Service parameters (e.g. bandwidth, latency, availability) shall not be impacted in any way by the intercept.

R-20 The intercept shall be transparent (i.e. undetectable) to all non-authorized employees of the WISP as well as to all other non-authorized persons.

4.1.2 Confidentiality / Access Control

R-30 Only authorized persons shall have knowledge of an intercept or access to intercept capabilities, communications and data in the WISP's network.

4.1.3 Authentication / Isolation

R-40 The WISP shall, to the extent used in the normal course of business, ensure that the captured communication originates from or is directed to the subject's equipment, facilities, or service, and shall not deliver to the LEA captured communications which do not originate from or are not directed to the subject's equipment, facilities, or service.

4.1.4 Validation

R-60 The WISP shall ensure that the intercepted communications throughout the duration of the intercept are associated with the subject's equipment, facilities, or service.[4]

4.1.5 Non-Repudiation

R-70 The WISP shall keep secure and accurate records of intercept parameters and implementation (e.g. requesting agency, time and date implemented) as per 47 C.F.R. § 1.20004[5], and shall keep intercept hashes either with or in the same manner as, and for the same period of time as the intercept records.[5]

[4] A change in IP address or similar event shall not permit the capture of communications, which are not associated with the subject.

[5] The duration and manner in which Secure and Accurate records are kept are specified in the System Security and Integrity Plan; for more information, see [4].

R-80 The WISP shall keep and secure relevant and sufficient records of service subscriptions to prove, after the intercept has taken place, that the captured communications were associated with the subject's equipment, facilities, or service. Such records shall be kept with, and for the same duration, as those of **R-70**.

R-90 The SHA256 hashing algorithm shall be used for data integrity to ensure at a later time that the intercepted communications and data delivered to the LEA have not been altered.

R-100 Copies of hashes shall be delivered to the LEA along with the intercepted communications and those hashes shall be maintained by the WISP as a business record in the same manner and duration as those of **R-70**.

4.1.6 Correlation

R-110 The WISP shall ensure that the intercepted Out-of-Band Events and IP packet captures (or Packet Data Summary Reports in the case of a Limited Broadband Intercept) delivered to the LEA are accurately correlated within an intercept category per target.

R-120 If more than one category of intercept (see Section 5) is active at any time for a subject, the WISP shall ensure that the intercept categories are correctly correlated in the interception information delivered to the LEA.

R-130 The WISP shall ensure that all systems performing the intercept have coordinated system times, accurate within 200ms of each other.

R-140 The WISP shall use the IAP and FSF timestamps as the basis for OOB message correlation.

4.1.7 Proportionality

R-150 The WISP shall ensure that only the authorized communications categories (see Section 5) are delivered to the LEA.

4.1.8 Completeness

R-160 The WISP shall ensure that the complete communications of the subject, both to and from the subject's equipment, facilities, or service, shall be intercepted for the entire period authorized by the intercept order.

4.1.9 Compression

R-170 If data compression is employed anywhere within the AF, FSF or across the "a" interface it shall not be of a form that will allow the loss of data or prevent the restoration of the original content in unaltered form. The WISP shall not use compression in transmitting, buffering, storing, or delivering the intercept to the LEA (interface "b").

4.1.10 Encryption

C-10 If the WISP provides encryption to the subject and possesses the information necessary to decrypt the communication, the WISP shall either:

- deliver the intercepted data to the LEA in unencrypted form[6], or
- provide information about the encryption algorithms used and the encryption keys to enable the LEA to decrypt the communications.

[6] This method is preferable, as it protects the WISPs encryption keys and methods from disclosure.

4.1.11 Performance

R-180 The WISP shall be capable of provisioning multiple simultaneous intercepts per subject.

R-190 The WISP shall be capable of provisioning multiple simultaneous intercepts on multiple subjects.

4.1.12 Transparency Across Law Enforcement Agencies

R-200 Multiple Law Enforcement Agency intercepts for the same subject or for different subjects shall be transparent to the respective LEAs. No LEA shall have access to the communications or data of any intercept performed for another LEA on the same or any other intercept subject, or performed for the same LEA under a different Case ID.

O-10 An implementation of this standard may allow a single LEA to access the intercept data for multiple subjects or intercept categories within the same Case ID under a single SFTP/SSH login account, or may separate access for each subject or category.

4.1.13 Availability and Reliability

R-210 The WISP shall use appropriate performance and reliability mechanisms and parameters to enable the intercept to be performed in a manner that eliminates the likelihood that the intercept will be corrupted due to dropped packets. This may require a reliable transport protocol across interface “a” or retransmitting data upon failure.

4.2 CALEA Rulemaking Requirements

As a result of the Federal Communications Commission (FCC) conclusion in its Communication Assistance for Law Enforcement Act (CALEA) rulemaking proceeding [10] that indicates providers of broadband Internet access service are subject to CALEA as “telecommunications carriers,” CALEA's requirements (47 U.S.C. §§ *et. seq.*) shall apply to WISPs, including the FCC’s system security and integrity rules, found in 47 C.F.R. § 1.20000 *et. seq*. [1]-[9].

5. Intercept Categories

There are three categories of information of interest to Law Enforcement in the data access intercept area: Full Content (Section 5.1), Limited (Section 5.2) and Out-of-Band Events (Section 5.3).

R-220 A "Full Content" order shall include requirements in Sections 5.1 Full Content Broadband Intercept and 5.3 Out-of-Band events

R-230 A "Limited" order shall include requirements in Sections 5.2 Limited Broadband Intercept and 5.3 Out-of-Band Events.

R-240 The intercept categories ("Full Content" or "Limited") shall be provisionable per intercept.

5.1 Full Content Broadband Intercept

R-250 The full set of IP packets associated with the subject's equipment, facilities or services shall be targeted, isolated, and captured.

R-260 IP Packets shall be delivered by the network to the FSF with the original IP headers intact. Any encapsulation of the original packets used for routing to the FSF shall be stripped off prior to delivery to the CF at interface "b".

R-270 If no packets were detected by an IAP for the duration of the Summary Timer, no packet capture file shall be created.

5.2 Limited Broadband Intercept

R-280 The Packet Signature shall be captured and delivered for each flow. The Packet Signature is a sequence of the Flow Signature that identifies a unique flow and the Packet Count for that flow since the last Packet Data Summary Report.

R-290 For each unique flow the Packet Signature shall be recorded in the Packet Data Summary Report at the start of the flow. The counter, Packet Count, shall be incremented with each packet in that flow. The Packet Signature shall be included in the Packet Data Summary Report if any packets were detected.

R-300 If no packets were detected for the duration of the Summary Timer, the Packet Data Summary Report shall not be sent.

5.3 Out-of-Band Events

"Out-of-Band" is a term with specific meaning in general telecommunications. Here, in the IP Network Access domain, it is used to describe network events that are not subject communications with an associate, but are typically subject equipment to network, or network to subject equipment signaling. For example, depending on access technology and network topology, events related to the intercept can occur before a network-reachable IP address is ever assigned by the network to the subject equipment, such as authentication of a username/password, or the initial DHCPDISCOVER of a DHCP client.

Some events and parameters are technology specific.

5.3.1 Events

This section describes Out-of-Band events that should be reported to the LEA. The hash for each message is contained in a separate file (see Section 7).

5.3.1.1 Access Attempt

R-310 The Access Attempt event shall be reported when a network access, registration or login has been attempted. Examples include:

- a subject's equipment, facility, or service successfully provides an appropriate form of unique identifying information (e.g., userID and password or Media Access Control [MAC] address) to an WISP's Authentication, Authorization, and Accounting (AAA) server or other equivalent functional entity.
- a subject's equipment, facility, or service attempts to access the WISP's network as indicated by a DHCP DISCOVER, DHCP OFFER, DHCP REQUEST or DHCP INFORM.

R-320 If the WISP allows multi-logins, where the same userID and password is used to establish multiple concurrent and distinct sessions, separate Access Attempt events shall be reported for each session attempted.

R-330 If the WISP allows use of multi-link protocols (e.g., Point-to-Point Protocol [PPP] multi-link protocol), separate Access Attempt events shall be reported with an indication that a multi-link login is being attempted if each channel is authenticated separately.

5.3.1.2 Access Accepted

R-340 The Access Accepted event shall be reported when the intercept subject's equipment, facility, or service or associated CPE network device is granted access to the WISP's network. If all parameters are known and reported, an Access Session is thereby initiated or continued; otherwise an Access Session Start event shall also be reported. Examples include:

- a DHCP server sends a DHCP ACK message.
- a subject or a subject's equipment, facility, or service successfully completes a login process.
- a WISP initiates an intercept or a subject moves into an area served by a WISP and one or more sessions are already active for the subject.

R-350 If the WISP allows multi-logins, where the same userID and password are used to establish multiple concurrent and distinct sessions, separate Access Accepted events shall be reported for each session.

R-360 If the WISP allows use of multi-link protocols, separate Access Accepted events shall be reported with an indication that a multi-link related login occurred for each channel that is authenticated separately.

5.3.1.3 Access Session Start

R-370 The Access Session Start event shall be reported when necessary to provide parameters not included in an Access Accepted event as indicated in Table 9, thereby initiating or continuing an Access Session. Examples include:

- an Access Accepted event is sent in response to RADIUS authentication but the IP address is assigned from an address pool local to a Remote Access Server (RAS) or PPPoE server; an Access Session Start event is sent to supply parameters (eg. IP address) as reported by the RAS or PPPoE server.

5.3.1.4 Access Failed

R-380 The Access Failed event shall be reported when attempted network access has failed and the network is aware of the failed attempt. Consequently, an Access Session has either not been successfully established or has ended. Examples include:

- a subject or a subject's equipment, facility, or service provides incorrect identification or authentication information to the WISP and is rejected by the WISP's AAA server or its functional equivalent with no access session established.
- access to the WISP resources has been denied and the subject's equipment has been explicitly denied an IP network address through a DHCP NACK Response.
- the subject has initiated a DHCP RELEASE prior to the DHCP server sending a DHCP ACK message.
- a subject sends a DHCP DECLINE after the DHCP server has sent a DHCP ACK message.
- unsuccessful PPP negotiation.
- a subject is already logged on, attempts to login a second time or to establish a second session with valid identifying information, but the network does not allow multi-logins.

5.3.1.5 Access Session End

R-390 The Access Session End event shall be reported when the intercept subject's access to the WISP has been disconnected and an Access Session is terminated. Examples include:

- a subject's equipment terminates a PPP session.
- a subject or a subject's equipment issues a DHCP RELEASE to release the lease on an IP address.
- a subject or a subject's equipment, facility, or service successfully completes a logout process.
- a subject's equipment experiences a loss of power or connectivity for a duration long enough to disrupt the session
- a WISP automatically drops a session due to inactivity, expiration of a pre-established time period, resource condition, administrative controls, or other reasons

5.3.1.6 Service Change

C-20 The Service Change event may be reported when a registered account being used by an intercept subject has a service type or other service attribute(s) modified either by the WISP or a user (e.g., registered primary account holder or secondary user authorized to request/enact such service changes for the account) which may impact an intercept subject's Internet access, and which is detectable by the network.

The Service Change event is considered to occur when either the WISP or an authorized user:

- adds a userID (subaccount) to an account.
- drops a userID (subaccount) from an account.
- deletes an existing account.
- alters a userID.
- modifies passwords or other authentication keys.
- locks a userID's access for a period of time.
- modifies the QoS parameters (e.g., service tier and associated Type of Service characteristics [e.g. Precedence of Data, Minimum Delay, Maximum Throughput, Maximum Reliability, Minimum Cost], bandwidth, etc.).
- modifies the set of active or subscribed-to features (e.g., encryption).

5.3.1.7 VPN Security Association Establishment

C-30 The VPN Security Association Establishment event should be reported when the WISP provides encryption services to the intercept subject and a VPN connection is established with the WISP VPN system endpoint on behalf of the intercept subject.[7]

5.3.1.8 VPN Security Association Release

C-40 The VPN Security Association Release event should be reported when a VPN connection that was established with the WISP VPN system endpoint on behalf of the intercept subject terminates.

The VPN Security Association Release event is considered to occur in the following cases:

- either the local or remote end of the VPN ends the Security Association;
- the VPN Security Association is terminated due to inactivity or an error.

5.3.2 Summary and Status Reports

5.3.2.1 Packet Data Summary Report

This event is used for Limited Broadband Intercept Orders to report source and destination information derived from the packet headers (i.e. the Flow Signature), and provides summary information for the number of packets transmitted or received by the subject for each packet flow (ie. the Packet Count).

R-400 The Packet Data Summary Report shall be reported when the expiration of a configurable timer per intercept occurs. This Summary Timer is configurable in units of seconds.

5.3.2.2 Surveillance Status Report

R-410 The Surveillance Status Report shall be reported:

- when a WISP activates a surveillance for a subject for a particular LEA.
- when there is a change in status of a surveillance (e.g. partial or complete failure of an FSF or other upstream functions).
- to notify the LEA, on a periodic basis, that surveillance is continuing/still active (i.e. a "heartbeat"). The heartbeat interval is configurable in minutes and should not exceed ten minutes.
- when surveillance on a particular subject is, or has been, deactivated.

The Surveillance Status Report is not hashed.

5.3.3 Event Parameters

R-420 When reporting the above events, the parameters of the messages defined in Appendix C.1 shall be reported.

5.3.4 Message Format

R-430 When reporting the above events, the messages defined in Appendix C.1 shall be reported in XML format. The XML instance documents generated must be valid against the schema defined in Appendix C.2.1.

[7] A VPN connection can be established between the intercept subject and a third party, in which case the WISP only acts as a transit network for the subject and need not report specific events within the subject's data stream such as VPN establishment.

6. Interface "a" Requirements

The following requirements apply to Interface "a":

R-440 The WISP shall deliver the intercept event messages and packet data to the FSF across Interface "a."

R-450 The WISP shall format event messages delivered across Interface "a" according to the format specified in Appendix C.

R-460 The "a" interface shall provide the highest tier of service available and use the highest data rate available in forwarding intercept data from the AF to the FSF.

R-470 Intercept events shall be timestamped at the time of detection at the Intercept Access Point.[8] This timestamp shall not be altered at the AF or FSF.

R-480 The accuracy of the timestamp shall be within 200 ms from detection of the event at the IAP and precision of at least 1 ms.

R-490 The WISP shall implement a reliable mechanism[9] to ensure that intercept event messages and packets have been received by the FSF, and re-transmit if it determines packet loss has occurred on the delivery link. The mode of compliance with this requirement will vary with the network architecture.

R-500 The WISP shall ensure the delivery of un-altered intercepted data. Any network-added headers shall be stripped off before delivery to the FSF.

[8] A second timestamp is included in the filename of files at the FSF (see Section 7.2).

[9] A TCP transport constitutes a "reliable mechanism."

7. File Structuring Function Requirements and File Format

7.1 FSF Requirements

The following requirements apply to the FSF described in Section 3 of this document:

R-510 The FSF shall only buffer and deliver the specific intercept categories (see Section 5) that are authorized by the Broadband Intercept Order served.

R-520 The packets and message information received from the network shall be buffered at the FSF in the format described in Section 7.2 of this document.

R-530 Delivery of intercept data by the FSF shall not begin prior to, nor extend beyond, the dates and times explicitly set forth in the Broadband Intercept Order.

R-540 The file granularity (ie. the number of packets or bytes per file, or capture time period per file) shall be provisionable per intercept.

R-550 The FSF shall implement SFTP/SSH[15] version 4 or later, and serve it to the CF client.

R-560 The SFTP/SSH authentication method between the FSF and CF client (e.g., user/password, PGP/PKI, X.509 certificates) shall be negotiated between the WISP and the LEA serving the Broadband Intercept Order.

R-570 The FSF shall be provisioned with sufficient buffering capacity for 24 hours of intercept uptime.

R-580 Deleting the intercept files off the FSF once they have been downloaded to the CF shall be the responsibility of the LEA. If the intercept runs higher than the provisioned amount of storage space, the stored packets may be automatically deleted in a cyclical first-in, first-out fashion by the FSF.

R-590 The SHA256 hashing algorithm shall be employed to facilitate verification that the communications downloaded by the LEA CF are indeed the communications intercepted by the WISP.

R-600 The hashes shall be calculated on a per-file basis.

R-610 The hashes shall be stored with a naming convention that allows the hash file to be easily paired with the hashed file, as described in Section 7.2.

R-620 The hashes shall be stored in the same subdirectory with the respective hashed file.

7.2 FSF Intercept Directory Structure

A mechanism to allow tools to parse intercepts is needed; this shall be accomplished by employing the following file directory structure and file naming conventions:

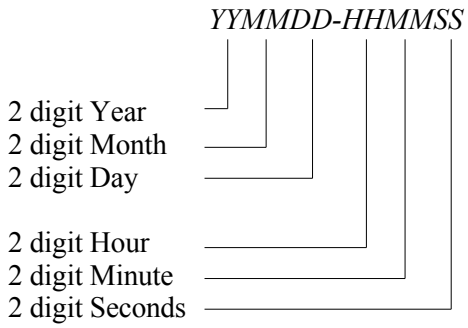
caseIdentity/**full**/*YYMMDD-HHMMSS-iapIdentifier*.**dmp**
caseIdentity/**full**/*YYMMDD-HHMMSS-iapIdentifier*.**dmp.hash**
caseIdentity/**limited**/*YYMMDD-HHMMSS-iapIdentifier*.**xml**
caseIdentity/**limited**/*YYMMDD-HHMMSS-iapIdentifier*.**xml.hash**
caseIdentity/**oob**/*YYMMDD-HHMMSS-mmm-messageName*.**xml**
caseIdentity/**oob**/*YYMMDD-HHMMSS-mmm-messageName*.**xml.hash**

Components in *italics* above are variables (defined below), components in **bold** are constants.

R-630 There shall be one top level directory per intercept, named with the WISP generated Case Identity defined below in Table 6. This is referenced in the directory structure as *caseIdentity*.

R-640 This top level intercept directory shall contain three sub-directories, named **`full`**, **`limited`**, and **`oob`**.

R-650 Each file stored at the FSF shall contain a timestamp, *YYMMDD-HHMMSS*, consisting of:



This timestamp shall be generated from a consistent time source throughout the intercept, and may either be the time at which the file is created or the time at which the event or data contained in the file was detected.

R-660 No two filenames may conflict. The file granularity of **R-540** must be sufficiently large enough that no two **full** or **limited** files from the same *iapIdentifier* are created within a one second interval. **oob** files have an additional 3 digit field, *mmm*, to distinguish multiple events occurring within the same second which otherwise would conflict. *mmm* may be a non-sequential incrementing counter, such as the millisecond resolution of the timestamp.

R-670 *iapIdentifier* is the IAP Identifier of the IAP capturing the packet or data or generating the event message, as defined in Table 6 of Appendix C.

R-680 *messageName* is the filename component of the OOB message defined in Table 18 of Appendix C.

R-690 The intercept data captured for a Limited Broadband Intercept as described in Section 5 of this document shall be stored in the *caseIdentity*/**`limited`** and *caseIdentity*/**`oob`** subdirectories in XML format, as defined in Appendix C. The *caseIdentity*/**full** directory shall either remain empty, or not exist at all.

R-700 The intercepted packets captured for a Full Content Broadband Intercept as described in Section 5 of this document shall be stored in the *caseIdentity*/**`full`** subdirectory using the PCAP format as defined in Appendix A, and the Out-of-Band events shall be stored in the *caseIdentity*/**`oob`** subdirectory in XML format as defined in Appendix C. The *caseIdentity*/**limited** directory shall either remain empty, or not exist at all.

8. Interface “b” Requirements

The following requirements apply to Interface “b”:

R-710 The WISP shall expose a static IP address to the LEA across Interface “b” to the Internet to allow the LEA CF client to connect to the FSF and pull the authorized intercepts from the FSF.

O-20 The WISP and LEA may optionally arrange a VPN connection to implement Interface “b”, through which the static IP address of the FSF is accessible. Details of VPN technology and parameters used are beyond the scope of this standard, and need to be negotiated prior to beginning the intercept.

R-720 Interface “b” shall provide the highest availability, reliability and grade of service available in the WISP’s network.

Appendix A. *libpcap* Format

A.1 LIBPCAP VERSION

The file format used to store captured packets for Full Content intercepts is PCAP version 2.4[13], in current use by the libpcap[14] library version 1.0,[10] and included here for reference.

A.2 GLOBAL HEADER

This header starts the libpcap file and will be followed by the first packet header:

```
typedef struct pcap_hdr_s {
        guint32 magic_number;  /* magic number */
        guint16 version_major; /* major version number */
        guint16 version_minor; /* minor version number */
        gint32  thiszone;      /* GMT to local correction */
        guint32 sigfigs;       /* accuracy of timestamps */
        guint32 snaplen;       /* max length of captured packets, in octets */
        guint32 network;       /* data link type */
} pcap_hdr_t;
```

Figure 2 - pcap Global Header

- `magic_number`: used to detect the file format itself and the byte ordering. The writing application writes 0xa1b2c3d4 with its native byte ordering format into this field. The reading application will read either 0xa1b2c3d4 (identical) or 0xd4c3b2a1 (swapped). If the reading application reads the swapped 0xd4c3b2a1 value, it knows that all the following fields will have to be swapped too.
- `version_major`, `version_minor`: the version number of this file format (current version is 2.4)
- `thiszone`: the correction time in seconds between GMT (UTC) and the local timezone of the following packet header timestamps.

  Examples: If the timestamps are in GMT (UTC), `thiszone` is simply 0. If the timestamps are in Central European time (Amsterdam, Berlin, ...) which is GMT + 1:00, `thiszone` must be -3600. In practice, time stamps are always in GMT, so `thiszone` is always 0.
- `sigfigs`: in theory, the accuracy of time stamps in the capture; in practice, all tools set it to 0
- `snaplen`: the maximum size of each packet (typically 65535 or even more, but might be limited by the user), see: `incl_len` vs. `orig_len` below
- `network`: data link layer type (e.g. 1 for Ethernet, see wiretap/libpcap.c or libpcap's pcap-bpf.h for details), this can be various types like Token Ring, Fiber Distributed Data Interface (FDDI), etc.

[10]At the time of publication of this standard, the libpcap library version 1.0 had not officially been released, though version 2.4 of the libpcap format has been in use for some time.

A.3 Record (Packet) Header

Each captured packet starts with (any byte alignment possible):

```
typedef struct pcaprec_hdr_s {
        guint32 ts_sec;    /* timestamp seconds */
        guint32 ts_usec;   /* timestamp microseconds */
        guint32 incl_len;  /* number of octets of packet saved in file */
        guint32 orig_len;  /* actual length of packet */
} pcaprec_hdr_t;
```

Figure 3 - pcap Record Packet Header

- `ts_sec`: the date and time when this packet was captured. This value is in seconds since January 1, 1970 00:00:00 GMT; this is also known as a UN*X time_t. You can use the American National Standards Institute (ANSI) C time() function from time.h to get this value, but you might use a more optimized way to get this timestamp value. If this timestamp isn't based on GMT (UTC), use `thiszone` from the global header for adjustments.
- `ts_usec`: the microseconds when this packet was captured, as an offset to `ts_sec`.

  ⚠ Beware: this value shouldn't reach 1 second (1 000 000), in this case `ts_sec` must be increased instead!
- `incl_len`: the number of bytes actually saved in the file. This value should never become larger than `orig_len` or the `snaplen` value of the global header.
- `orig_len`: the length of the packet "on the wire" when it was captured. If `incl_len` and `orig_len` differ, the actually saved packet size was limited by `snaplen`.

A.4 Packet Data

The actual packet data will immediately follow the packet header as a data blob of `incl_len` bytes without a specific byte alignment.

A.5 Libpcap Copyright

Libpcap is distributed under the modified BSD license, and portions of this Appendix have been taken therefrom:

```
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

  1. Redistributions of source code must retain the above copyright
     notice, this list of conditions and the following disclaimer.
  2. Redistributions in binary form must reproduce the above copyright
     notice, this list of conditions and the following disclaimer in
     the documentation and/or other materials provided with the
     distribution.
  3. The names of the authors may not be used to endorse or promote
     products derived from this software without specific prior
     written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
```

Appendix B. Out-of-Band Event Mapping

This Appendix is an implementation guide providing a mapping of how events defined by address assignment protocols or other CALEA standards should be reported under this standard. Depending on protocols used, there may be numerous points at which the information requisite to creating OoB event messages can be collected, eg. a PPPoE session which ultimately authenticates to a RADIUS server could gather information at the PPP or RADIUS level, from the logs of either the PPP or RADIUS server, or syslogs generated by either server, or potentially snmp traps sent by either. Sometimes it is necessary to coordinate information gathered in numerous points. Duplicate OoB event messages should not be generated merely because the information is available in multiple places.

Protocols addressed include:

- DHCP
- RADIUS
- PPP (including encapsulated PPP (PPPoE, PPPoA) and tunneled PPP (PPTP, L2TP))

Standards addressed include:

- ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance for Internet Access and Services [11]
- CableLabs Cable Broadband Intercept 2.0 Specification [12]

B.1 Event mappings of Address Assignment Protocols

B.1.1 DHCP Event to WCS IPNA OoB Event mapping

DHCP Event	Purpose of DHCP Event	Out-of-Band Event
DHCPDISCOVER	Client broadcast to find available servers.	Access Attempt
DHCPOFFER	Server to client in response to DCHPDISCOVER with an offer of configuration parameters.	Access Attempt
DHCPREQUEST	Either a) or b) or c) a) Requesting offered parameters from one server and implicitly declining offers from all other servers. b) Confirming network address after a system reboots. c) Extending a lease on an IP address.	Access Attempt
DHCPACK	Committed configuration parameters.	Access Accepted
DHCPNAK	The committed IP address is invalid (e.g lease expired or wrong subnet).	Access Failed
DHCPDECLINE	Upon testing (e.g. arp or ping) the committed IP address is already in use.	Access Failed
DHCPRELEASE	Cancel remaining lease and return IP address.	Access Session End
DHCPINFORM	Request local parameters; client already has valid IP address.	Access Attempt

Table 1: DHCP Event Mapping

B.1.2 RADIUS Packet to WCS IPNA OoB Event mapping

RADIUS Packet	Direction	Code	Out-of-Band Event
Access-Request	RADIUS Client → Server	1	Access Attempt
Access-Accept	RADIUS Server → Client	2	Access Accepted
Accounting-Request	RADIUS Client → Server	4	Access Session Start*
Access-Reject	RADIUS Server → Client	3	Access Failed
Accounting-Request	RADIUS Client → Server	4	Access Session End

Table 2: Radius Packet Mapping

* The RADIUS Access-Accept message may include the IP address, in which case an Access Session Start is unneeded; otherwise an Access Session Start must supply the IP address, which is usually included in a RADIUS Accounting-Request.

B.1.3 PPP Event to WCS IPNA OoB Event mapping

PPP Event	Direction	Proto	Code	Out-of-Band Event
PAP Request	Client → Server	0xC023	0x1	Access Attempt*
CHAP Challenge	Client → Server	0xC223	0x1	Access Attempt*
EAP Request	Client → Server	0xC227	0x1	Access Attempt*
PAP Success	Server → Client	0xC023	0x2	Access Accepted
CHAP Success	Server → Client	0xC223	0x3	Access Accepted
EAP Success	Server → Client	0xC227	0x3	Access Accepted
PAP Failure	Server → Client	0xC023	0x3	Access Failed
CHAP Failure	Server → Client	0xC223	0x4	Access Failed
EAP Failure	Server → Client	0xC227	0x4	Access Failed
IPCP Configure-Ack	Server → Client	0x8021	0x2	Access Session Start*
LCP Terminate-Request	Client → Server	0xC021	0x5	Access Session End
LCP Terminate-Ack	Client → Server	0xC021	0x6	Access Session End
LCP Terminate-Request	Server → Client	0xC021	0x5	Access Session End
LCP Terminate-Ack	Server → Client	0xC021	0x6	Access Session End

Table 3: Radius Packet Mapping

* The username can be obtained from the PAP, CHAP and EAP Requests; the IP address can be obtained from the IPCP Configure-Ack message.

B.2 Event Mapping of other CALEA standards

B.2.1 Internet Access Services (IAS)

Table 4 shows the relationship between Internet Access and Services (IAS) events, as described in ATIS-1000013.2007 Section 5.2[11], and Out-of-Band Events under this standard.

IAS Event	Purpose of IAS Event	IPNA Event
Access Attempt[11]	The subject successfully provides an appropriate form of unique identifying information to an AAA server (or other equivalent functional entity).	Access Attempt
Access Accepted	The subject successfully provides some form of unique identifying information that is verified and validated by an AAA server.	Access Accepted
Access Failed	The subject provides incorrect identification or authentication information to the WISP domain and is rejected by an AAA server.	Access Failed
Access Session End	The subject initiates a disconnect request to the network or the subject's equipment experiences a loss of power.	Access Session End
Access Rejected	The subject's authentication or authorization to the network is successfully completed, but the subject's access attempt is rejected for other reasons.	Access Failed
Access Signaling Message Report	Sent in lieu of an Access Attempt, Access Accepted, Access Failed, Access Session End, or Access Rejected message for the same set of events.	N/A
Packet Data Session Start	The subject, or the subject's equipment, successfully completes the login process and an IP address is assigned to the subject's equipment.	Access Session Start
Packet Data Session Failed	The subject's login procedure to the network is successfully completed, but the intercept subject is denied access to the network.	Access Failed
Packet Data Session End	The subject's equipment ends a session with the network or the subject's equipment experiences disruption of connectivity for a sufficient time to cause termination of the subject's packet data session.	Access Session End

[11]The IPNA Access Attempt event consolidates both the IAS Access Attempt and Packet Data Session Start events; it is not necessary to create duplicate IPNA Access Attempt events where both an IAS Access Attempt and Packet Data Session Start event occur in succession.

IAS Event	Purpose of IAS Event	IPNA Event
Packet Data Session Already Established	Surveillance is begun on an intercept subject's communications while the intercept subject's packet data session is already established, regardless of whether the intercept subject is actively transmitting or receiving packets.	Access Accepted
Packet Data Header Reporting	Reports the header of each packet sent and received by the subject.	N/A
Packet Data Summary Report	A summary report triggered by the start of a packet stream, interim report of a packet stream, or end of a packet stream.	Packet Data Summary Report
Service Change	A registered account being used by an intercept subject has a service type or other service attribute(s) modified either by the WISP or a user which may impact an intercept subject's ability to access a public IP network.	Service Change
VPN Security Association Establishment	A VPN connection is established between a subject host and a destination host using an WISP VPN system as the subject's VPN endpoint.	VPN Security Association Establishment
VPN Security Association Release	A VPN connection that was established by an WISP domain system on behalf of the subject supporting protected IP communications with a remote IP address terminates.	VPN Security Association Release
Surveillance Activation	The WISP activates a surveillance for a subject for a particular LEA, based on the authorization submitted to the WISP by the LEA.	Surveillance Status Report
Surveillance Continuation	The WISP periodically reports the status of an ongoing, active surveillance to an LEA.	Surveillance Status Report
Surveillance Change	A change is made to the status of an active surveillance.	Surveillance Status Report
Surveillance Deactivation	The WISP deactivates a surveillance for an intercept subject for a particular LEA, based on the authorization submitted to the WISP by the LEA.	Surveillance Status Report

Table 4: IAS Event Mappings

B.2.2 Cable Broadband Intercept Specification (CBIS)

Table 5 shows the relationship between Cable Broadband Intercept Specification (CBIS)[12] events and Out-of-Band Events under this standard.

CBIS OoB Message	Purpose of the CBIS Message	IPNA Event
Access Attempt	Report when a network registration has been attempted.	Access Attempt
Access Accepted	Report successful authentication by the DHCP server (DHCP ACK).	Access Accepted
Access Failed	Report failure of network authentication (DHCP NACK).	Access Failed
Access Declined	Report when the subject sends a DHCP DECLINE message.	Access Failed
Access Session End	Report when the subject sends a DHCP RELEASE message.	Access Session End

Table 5: CBIS OoB Message Mappings

Appendix C. Event Parameters and XML Messages

This Appendix describes the out-of-band event message contents, defines the XML schema to describe the structure of those messages, and provides an example XML instance document for each message.

C.1 Event Parameters

C.1.1 Out-Of-Band Message Parameters Types and Descriptions

The data types referenced in the Out-of-Band Event Message Parameters table are defined using the basic XML schema types and user defined types described in Table 7.

Information Element	Data Type	Description
Access Method	**sequence**[12]	This element consists of three information elements: Access Type, Equipment ID, and MultiLink. The semantics of these elements are defined below. This parameter does not need reported more than once per Access Session.
Access Session Characteristics	**string**	Identifies characteristics of the intercept subject's Access Session (e.g., bandwidth limits, noteworthy network-level filtering). This parameter is WISP/network specific.
Access Session Identity	**string**	Uniquely identifies the intercept subject's network Access Session for a given surveillance.
Access Type	**string**	Specifies the type of equipment or network used to gain internet access (e.g., cable modem, dsl, fiber, wireless, etc.). This is the first information element within the Access Method element.
Case Identity	**FSSafeString**	Uniquely identifies the specific intercept of a Subject. This identity remains constant for the entire surveillance period. For example, this can be a phone number or an WISP's ticketing system identifier.
Changes Attempted	**string**	Identifies all added, deleted, or modified account/service information/attributes.
Change Result	**sequence**[12]	Identifies whether the service change request was accepted and implemented, was refused, or if an error occurred. If refused, identifies the reason. If an error occurred while the request was being processed, identifies the error and the result (e.g., no change made).
Encryption Algorithm	**string**	Identifies the encryption algorithm(s) (e.g., Triple Date Encryption Standard, Rivest Cipher 4, Message Digest 5, Secure Hash Algorithm) for a Local or Remote VPN Encryption element. Use readily identifiable values negotiated with the LEA prior to beginning the intercept.
Encryption Key	**string**	Provides the actual encryption key(s) used to encrypt packets traversing a VPN tunnel, paired with an Encryption Algorithm.
Equipment ID	**string**	Contains the MAC address or other identifier of the device used for accessing network resources, if available. This is the second information element within the Access Method.
Failure Reason	**string**	Provides the reason the Access Session was not accepted (e.g., receipt of DHCPNAK message, incorrect password, unavailable resource, access rejected by network).
Flow Signature	**sequence**[12]	Describes a set of the Source and Destination IP address, IP Protocol, and Source and Destination Ports if available[2] and applicable to the IP Protocol.
IAP Identifier	**FSSafeString**	Uniquely identifies an Intercept Access Point providing CmII, CmC or OoB event data.
IP Address	**IPAddress**	Provides the IP Address assigned throughout an Access Session.
IP Assignment Method	**string**	Indicates whether the value in IP Address is static, dynamic, or unknown.

[12]Wherever possible the <all> indicator is used rather than <sequence> to allow elements in any order.

Information Element	Data Type	Description
Lease Duration	**unsignedInt**	Defines the length of the IP address lease associated with the intercept subject's Access Method in units of seconds.
Local VPN Encryption Information	**sequence[12]**	Consists of an Encryption Algorithm and Encryption Key pair used by the Local VPN Endpoint to encrypt packets traversing the VPN tunnel. Multiple entries may be included in a VPN Security Association Establishment message if required.
Local VPN Endpoint IP Address	**IPAddress**	Identifies the IP address of the Local VPN Endpoint from the perspective of the VPN Security Association.
Location	**string**	Identifies the location of the subject's equipment, facility, or service when reasonably available and required by the Broadband Intercept Order. Must be the most specific location information available in the network, for example, one or more of street address, location name, network (MAC) address, location of access node/access point, etc. This parameter may be omitted if the Location has not changed from that most recently reported.
MultiLink	**boolean**	Indicates whether or not a multi-link login has occurred. This is the third information element within the Access Method.
Packet Count	**unsignedLong**	Count of the number of packets associated with a Flow Signature since the last Packet Data Summary Report.
Packet Signature	**sequence[12]**	Specifies the sequence of a Flow Signature and the corresponding Packet Count. There may be more than one Packet Signature element included in a Packet Data Summary Report.
Primary Account Subscriber Identity	**string**	Identifies the account number or other administrative identifier uniquely assigned to the primary account and the primary subscriber under whom the account is registered.
Remote VPN Encryption Information	**sequence[12]**	Consists of an Encryption Algorithm and Encryption Key pair used by the Remote VPN Endpoint to encrypt packets traversing the VPN tunnel, if applicable to the VPN architecture. Multiple entries may be included in a VPN Security Association Establishment message if required.
Remote VPN Endpoint IP Address	**IPAddress**	Identifies the IP address of the Remote VPN Endpoint from the perspective of the VPN Security Association.
Status	**sequence[12]**	Describes the status of a surveillance (i.e., active, inactive, error condition, or a simple "heartbeat"). The status has two components. The first component is one of the enumerated values indicating active, inactive, error or heartbeat. The second component is an optional text string to provide further explanation.
Subscriber Identity	**string**	Uniquely identifies the subscriber to the service. This is the alias used by the WISP to identify the intercept subject. For example, may include one or more of Service Account ID, user ID, MAC Address, IP Address.
Termination Reason	**string**	Provides the reason the Access Session was disconnected (e.g., inactivity period threshold exceeded, or normal logout), and indicating whether the termination was initiated by the subject or the WISP.
Time Stamp	**dateTime**	Identifies the date and time that the event triggering the message was detected, to at least milisecond precision.
VPN Security Association Identity	**integer**	Uniquely identifies the VPN Security Association within the session (eg. an IPsec spi). This identity remains constant throughout the VPN Security Association.
VPN Security Association Protocol	**sequence[12]**	Identifies the protocol(s) (e.g., IP Security Internet Key Exchange, Point-to-Point Tunneling Protocol, Layer 2 Tunneling Protocol, Generic Routing Encapsulation) and any associated information concerning the protocols (e.g., IPsec AH, or IPsec tunnel-mode ESP). Use readily identifiable values negotiated with the LEA prior to beginning the intercept.
VPN Termination Reason	**string**	Identifies the error condition or other reason for the ending of or failure to establish the VPN Security Association.

Table 6: Out-of-Band Event Message Parameters

Table 7 describes restrictions on the data types defined for message parameters, including the permitted values for these defined types. The schema provided in Appendix C.2.1 embodies these restrictions.

Defined Type	Base Type / Indicator	Permitted Values
IPAddress	**choice**	Either an IPv4 address in dotted-decimal notation or an IPv6 address in standard notation.
FSSafeString	**string**	String of characters intended to be safe for use in a filesystem name. Limited to 255 characters from the set: [a-z A-Z0-9-_:+=.-].

Table 7: XML Defined Types

C.1.2 Message Parameters

Parameters designated **M** are mandatory, **O** are optional, and **C** are conditional.

C.1.2.1 Access Attempt Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Location	C	Provide when required (see Table 6).
Access Method	O	Provide when known.

Table 8: Information for Access Attempt Message

C.1.2.2 Access Accepted Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Location	C	Provide when required (see Table 6).
Access Method	O	See R-370. / Provide when known.
Access Session Identity	O	See R-370.
Access Session Characteristics	O	
IP Address	O	See R-370.
IP Assignment Method	O	See R-370. / Provide when known.
Lease Duration	O	See R-370. / Provide when applicable.

Table 9: Information for Access Accepted Message

C.1.2.3 Access Failed Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Location	C	Provide when required (see Table 6).
IP Address	C	Provide when known.
IP Assignment Method	C	Provide when known.
Failure Reason	C	Provide when known.

Table 10: Information for Access Failed Message

C.1.2.4 Access Session End Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Access Session Identity	M	
IP Address	C	Provide when known.
Termination Reason	C	Provide when known.

Table 11: Information for Access Session End Message

C.1.2.5 Access Session Start Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Location	C	Provide when required (see Table 6).
Access Method	O	See R-370. / Provide when known.
Access Session Identity	M	
Access Session Characteristics	O	
IP Address	M	
IP Assignment Method	O	See R-370. / Provide when known.
Lease Duration	O	See R-370. / Provide when applicable.

Table 12: Information for Access Session Start Message

C.1.2.6 Packet Data Summary Report Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Packet Signature	M	Multiple Packet Signatures may be included.

Table 13: Information for Packet Data Summary Report Message

C.1.2.6 Service Change Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	M	
Primary Account Subscriber Identity	C	Provide when known.
Changes Attempted	M	
Change Result	M	

Table 14: Information for Service Change Message

C.1.2.7 Surveillance Status Report Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Access Session Identity	M	
Status	M	

Table 15: Information for Surveillance Status Report Message

C.1.2.8 VPN Security Association Establishment Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	C	Provide when known.
Access Session Identity	C	Provide when known.
IP Address	C	IP Address of the Access Session / Provide when known.
VPN Security Association Identity	M	
VPN Security Association Protocol	M	
Local VPN Endpoint IP Address	M	
Remote VPN Endpoint IP Address	M	
Local VPN Encryption Information	M	
Remote VPN Encryption Information	C	Provide when applicable to the VPN type.

Table 16: Information for VPN Security Association Establishment Message

C.1.2.9 VPN Security Association Release Message

Information Element	M/O/C	Comments / Restrictions
Case Identity	M	
IAP Identifier	M	
Time Stamp	M	
Subscriber Identity	C	Provide when known.
Access Session Identity	C	Provide when known.
VPN Security Association Identity	M	
VPN Termination Reason	M	

Table 17: Information for VPN Security Association Release Message

C.1.3 Out-Of-Band Message Filename Components

Out Of Band Event Message	Filename Component
Access Attempt	AccessAttempt
Access Accepted	AccessAccepted
Access Failed	AccessFailed
Access Session End	AccessSessionEnd
Access Session Start	AccessSessionStart
Service Change	ServiceChange
Surveillance Status Report	SurveillanceStatusReport
VPN Security Association Establishment	VPNSecurityAssociationEstablishment
VPN Security Association Release	VPNSecurityAssociationRelease

Table 18: Out-of-Band Message Filename Components

C.2 XML Messages

XML instance documents conforming to this standard must validate against the following XML Schema in Appendix C.2.1. A valid example XML instance document of each message type is given in Appendix C.2.2, using various formats for element values and namespace styles. The XML schema is available from the WISPA website at:

http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd

A .zip file containing the XML schema and the example instance documents is available from the WISPA website at:

http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.zip

C.2.1 XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="http://www.wispa.org/calea/WCS/"
    targetNamespace="http://www.wispa.org/calea/WCS/"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

    <xs:annotation>
        <xs:documentation>
```

```
        WISPA Calea Standard - IP Network Access (WISPA-CS-IPNA) 1.0
    </xs:documentation>
</xs:annotation>

<xs:element name="WCSMessage">
    <xs:annotation>
        <xs:documentation>
            WCSMessage is the root element of all WISPA-CS messages.
        </xs:documentation>
    </xs:annotation>

    <xs:complexType>
        <xs:choice>
            <xs:element ref="AccessAttempt" />
            <xs:element ref="AccessAccepted" />
            <xs:element ref="AccessFailed" />
            <xs:element ref="AccessSessionEnd" />
            <xs:element ref="AccessSessionStart" />
            <xs:element ref="PacketDataSummaryReport" />
            <xs:element ref="ServiceChange" />
            <xs:element ref="SurveillanceStatusReport" />
            <xs:element ref="VPNSecurityAssociationEstablish" />
            <xs:element ref="VPNSecurityAssociationRelease" />
        </xs:choice>

        <xs:attribute name="version" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="1.0" />
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="series" use="optional">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="IPNA" />
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
    </xs:complexType>
</xs:element>

<xs:element name="AccessAttempt">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="Location" type="xs:string"
                minOccurs="0" />
            <xs:element name="AccessMethod" type="AccessMethod"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="AccessAccepted">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
```

```
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="Location" type="xs:string"
                minOccurs="0" />
            <xs:element name="AccessMethod" type="AccessMethod"
                minOccurs="0" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" minOccurs="0" />
            <xs:element name="AccessSessionCharacteristics"
                type="xs:string" minOccurs="0" />
            <xs:element name="IPAddress" type="IPAddress"
                minOccurs="0" />
            <xs:element name="IPAssignmentMethod"
                type="IPAssignmentMethod" minOccurs="0" />
            <xs:element name="LeaseDuration" type="xs:unsignedInt"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="AccessFailed">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="Location" type="xs:string"
                minOccurs="0" />
            <xs:element name="IPAddress" type="IPAddress"
                minOccurs="0" />
            <xs:element name="IPAssignmentMethod"
                type="IPAssignmentMethod" minOccurs="0" />
            <xs:element name="FailureReason" type="xs:string"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="AccessSessionEnd">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" />
            <xs:element name="IPAddress" type="IPAddress"
                minOccurs="0" />
            <xs:element name="TerminationReason" type="xs:string"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="AccessSessionStart">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="Location" type="xs:string"
```

```
                minOccurs="0" />
            <xs:element name="AccessMethod" type="AccessMethod"
                minOccurs="0" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" />
            <xs:element name="AccessSessionCharacteristics"
                type="xs:string" minOccurs="0" />
            <xs:element name="IPAddress" type="IPAddress" />
            <xs:element name="IPAssignmentMethod"
                type="IPAssignmentMethod" minOccurs="0" />
            <xs:element name="LeaseDuration" type="xs:unsignedInt"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="PacketDataSummaryReport">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="PacketSignature"
                type="PacketSignature" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="ServiceChange">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string" />
            <xs:element name="PrimaryAccountSubscriberIdentity"
                type="xs:string" minOccurs="0" />
            <xs:element name="ChangesAttempted" type="xs:string" />
            <xs:element name="ChangeResult" type="ChangeResult" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="SurveillanceStatusReport">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" />
            <xs:element name="Status" type="Status" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:element name="VPNSecurityAssociationEstablish">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
```

```
            <xs:element name="SubscriberIdentity" type="xs:string"
                minOccurs="0" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" minOccurs="0" />
            <xs:element name="IPAddress" type="IPAddress"
                minOccurs="0" />
            <xs:element name="VPNSecurityAssociationIdentity"
                type="xs:integer" />
            <xs:element name="VPNSecurityAssociationProtocol">
                <xs:complexType>
                    <xs:all>
                        <xs:element name="Protocol"
                            type="xs:string" />
                        <xs:element name="AdditionalInformation"
                            type="xs:string" />
                    </xs:all>
                </xs:complexType>
            </xs:element>
            <xs:element name="LocalVPNEndpointIPAddress"
                type="IPAddress" />
            <xs:element name="RemoteVPNEndpointIPAddress"
                type="IPAddress" />
            <xs:element name="LocalVPNEncryptionInformation"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:all>
                        <xs:element name="EncryptionAlgorithm"
                            type="xs:string" />
                        <xs:element name="EncryptionKey"
                            type="xs:string" />
                    </xs:all>
                </xs:complexType>
            </xs:element>
            <xs:element name="RemoteVPNEncryptionInformation"
                maxOccurs="unbounded" minOccurs="0">
                <xs:complexType>
                    <xs:all>
                        <xs:element name="EncryptionAlgorithm"
                            type="xs:string" />
                        <xs:element name="EncryptionKey"
                            type="xs:string" />
                    </xs:all>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="VPNSecurityAssociationRelease">
    <xs:complexType>
        <xs:all>
            <xs:element name="CaseIdentity" type="FSSafeString" />
            <xs:element name="IAPIdentifier" type="FSSafeString" />
            <xs:element name="TimeStamp" type="xs:dateTime" />
            <xs:element name="SubscriberIdentity" type="xs:string"
                minOccurs="0" />
            <xs:element name="AccessSessionIdentity"
                type="xs:string" minOccurs="0" />
            <xs:element name="VPNSecurityAssociationIdentity"
                type="xs:integer" />
            <xs:element name="VPNTerminationReason"
                type="xs:string" />
        </xs:all>
```

```
        </xs:complexType>
    </xs:element>

    <xs:simpleType name="FSSafeString">
        <xs:annotation>
            <xs:documentation>
                A string of characters intended to be safe for use in a
                filesystem name.
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern value="([a-zA-Z0-9_:+=\.\-])+" />
            <xs:maxLength value="255"></xs:maxLength>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="IPAddress">
        <xs:choice>
            <xs:element name="IPv4Address" type="IPv4Address" />
            <xs:element name="IPv6Address" type="IPv6Address" />
        </xs:choice>
    </xs:complexType>

    <xs:simpleType name="IPv4Address">
        <xs:annotation>
            <xs:documentation>
                IPv4 address in dotted-decimal notation.
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern
                  value="((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])\.){3}(25[0-5]|2[0-4][0-
9]|1[0-9][0-9]|[1-9][0-9]|[0-9])" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="IPv6Address">
        <xs:annotation>
            <xs:documentation>
                IPv6 address in standard notation.
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern value="([0-9a-fA-F]{1,4}:){7}[0-9a-fA-F]{1,4}" />
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="AccessMethod">
        <xs:all>
            <xs:element name="AccessType" type="xs:string" />
            <xs:element name="EquipmentID" type="xs:string" />
            <xs:element name="MultiLink" type="xs:boolean" />
        </xs:all>
    </xs:complexType>

    <xs:simpleType name="IPAssignmentMethod">
        <xs:restriction base="xs:string">
            <xs:enumeration value="static" />
            <xs:enumeration value="dynamic" />
            <xs:enumeration value="unknown" />
        </xs:restriction>
    </xs:simpleType>
```

```
    <xs:complexType name="PacketSignature">
        <xs:all>
            <xs:element name="FlowSignature" type="FlowSignature" />
            <xs:element name="PacketCount" type="xs:unsignedLong">
                <xs:annotation>
                    <xs:documentation>
                        Count of Packets matching this Flow Signature
                        since the last Packet Data Summary Report.
                    </xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:all>
    </xs:complexType>

    <xs:complexType name="FlowSignature">
        <xs:all>
            <xs:element name="sourceAddress" type="IPAddress" />
            <xs:element name="destAddress" type="IPAddress" />
            <xs:element name="sourcePort" type="xs:unsignedInt"
                minOccurs="0" />
            <xs:element name="destPort" type="xs:unsignedInt"
                minOccurs="0" />
            <xs:element name="ipProtocol" type="xs:unsignedByte" />
        </xs:all>
    </xs:complexType>

    <xs:complexType name="ChangeResult">
        <xs:all>
            <xs:element name="Disposition">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="accepted" />
                        <xs:enumeration value="refused" />
                        <xs:enumeration value="error" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="AdditionalInformation" type="xs:string"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>

    <xs:complexType name="Status">
        <xs:all>
            <xs:element name="Status">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="active" />
                        <xs:enumeration value="inactive" />
                        <xs:enumeration value="error" />
                        <xs:enumeration value="heartbeat" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="AdditionalInformation" type="xs:string"
                minOccurs="0" />
        </xs:all>
    </xs:complexType>

</xs:schema>
```

C.2.2 XML Instance Documents

C.2.2.1 Access Accepted XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <AccessAccepted>
        <CaseIdentity>X555-2</CaseIdentity>
        <IAPIdentifier>IAP-1</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00Z</TimeStamp>
        <SubscriberIdentity>login@isp.com</SubscriberIdentity>
        <AccessMethod>
            <AccessType>DSL</AccessType>
            <EquipmentID />
            <MultiLink>false</MultiLink>
        </AccessMethod>
        <AccessSessionIdentity>225588</AccessSessionIdentity>
        <AccessSessionCharacteristics>
            256k up / 256k down
        </AccessSessionCharacteristics>
        <IPAddress>
            <IPv4Address>192.168.100.123</IPv4Address>
        </IPAddress>
        <IPAssignmentMethod>dynamic</IPAssignmentMethod>
        <LeaseDuration>21600</LeaseDuration>
    </AccessAccepted>
</WCSMessage>
```

C.2.2.2 Access Attempt XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCS:WCSMessage series="IPNA" version="1.0"
    xmlns:WCS="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <WCS:AccessAttempt>
        <WCS:CaseIdentity>Case12345</WCS:CaseIdentity>
        <WCS:IAPIdentifier>CMII_Radius_IAP</WCS:IAPIdentifier>
        <WCS:TimeStamp>2001-12-31T12:00:00.345002-06:00</WCS:TimeStamp>
        <WCS:SubscriberIdentity>user@ispdomain.com</WCS:SubscriberIdentity>
        <WCS:Location>123 Main St., SomeCity, AA, 12345</WCS:Location>
        <WCS:AccessMethod>
            <WCS:AccessType>Wireless</WCS:AccessType>
            <WCS:EquipmentID>00:11:22:aa:bb:cc</WCS:EquipmentID>
            <WCS:MultiLink>false</WCS:MultiLink>
        </WCS:AccessMethod>
    </WCS:AccessAttempt>
</WCS:WCSMessage>
```

C.2.2.3 Access Failed XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
```

```
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <AccessFailed>
        <CaseIdentity>Case-999</CaseIdentity>
        <IAPIdentifier>radius.wisp.com</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00.035</TimeStamp>
        <SubscriberIdentity>user@wisp.com</SubscriberIdentity>
        <Location>SomeTown, USA</Location>
        <FailureReason>Authentication Failed: Bad Password</FailureReason>
    </AccessFailed>
</WCSMessage>
```

C.2.2.4 Access Session End XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <AccessSessionEnd>
        <CaseIdentity>CALEA-TAP-0003</CaseIdentity>
        <IAPIdentifier>IAP-CmII-dhcp.isp.com</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00.3-11:00</TimeStamp>
        <SubscriberIdentity>00:22:33:01:23:45</SubscriberIdentity>
        <AccessSessionIdentity>580</AccessSessionIdentity>
        <IPAddress>
            <IPv4Address>10.20.25.48</IPv4Address>
        </IPAddress>
        <TerminationReason>DHCP RELEASE</TerminationReason>
    </AccessSessionEnd>
</WCSMessage>
```

C.2.2.5 Access Session Start XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <AccessSessionStart>
        <CaseIdentity>CALEA-TAP-0005</CaseIdentity>
        <IAPIdentifier>IAP1</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00.08Z</TimeStamp>
        <SubscriberIdentity>01:23:45:11:22:01</SubscriberIdentity>
        <AccessSessionIdentity>1000</AccessSessionIdentity>
        <IPAddress>
            <IPv4Address>172.16.17.18</IPv4Address>
        </IPAddress>
        <AccessMethod>
            <AccessType>Wireless</AccessType>
            <EquipmentID>01:23:45:11:22:01</EquipmentID>
            <MultiLink>false</MultiLink>
        </AccessMethod>
        <IPAssignmentMethod>dynamic</IPAssignmentMethod>
        <LeaseDuration>10000</LeaseDuration>
    </AccessSessionStart>
</WCSMessage>
```

C.2.2.6 Packet Data Summary Report XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <PacketDataSummaryReport>
        <CaseIdentity>233-4T2-11</CaseIdentity>
        <IAPIdentifier>tap-3.wisp.org</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00</TimeStamp>
        <SubscriberIdentity>192.0.2.123</SubscriberIdentity>
        <PacketSignature>
            <FlowSignature>
                <sourceAddress>
                    <IPv4Address>192.0.2.123</IPv4Address>
                </sourceAddress>
                <destAddress>
                    <IPv4Address>198.81.129.100</IPv4Address>
                </destAddress>
                <ipProtocol>6</ipProtocol>
                <sourcePort>32008</sourcePort>
                <destPort>80</destPort>
            </FlowSignature>
            <PacketCount>18</PacketCount>
        </PacketSignature>
        <PacketSignature>
            <FlowSignature>
                <sourceAddress>
                    <IPv4Address>198.81.129.100</IPv4Address>
                </sourceAddress>
                <destAddress>
                    <IPv4Address>192.0.2.123</IPv4Address>
                </destAddress>
                <ipProtocol>6</ipProtocol>
                <sourcePort>80</sourcePort>
                <destPort>32008</destPort>
            </FlowSignature>
            <PacketCount>36</PacketCount>
        </PacketSignature>
        <PacketSignature>
            <FlowSignature>
                <!-- tcp packet fragments (no port numbers) -->
                <sourceAddress>
                    <IPv4Address>198.81.129.100</IPv4Address>
                </sourceAddress>
                <destAddress>
                    <IPv4Address>192.0.2.123</IPv4Address>
                </destAddress>
                <ipProtocol>6</ipProtocol>
            </FlowSignature>
            <PacketCount>26</PacketCount>
        </PacketSignature>
    </PacketDataSummaryReport>
</WCSMessage>
```

C.2.2.7 SERVICE CHANGE XML INSTANCE DOCUMENT

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <ServiceChange>
```

```
        <CaseIdentity>WCS-CaseID-40</CaseIdentity>
        <IAPIdentifier>admin.isp.org</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00.123004</TimeStamp>
        <SubscriberIdentity>john.doe</SubscriberIdentity>
        <PrimaryAccountSubscriberIdentity>
            11525
        </PrimaryAccountSubscriberIdentity>
        <ChangesAttempted>Upgrade Service to 512k</ChangesAttempted>
        <ChangeResult>
            <Disposition>refused</Disposition>
            <AdditionalInformation>
                Credit Card Declined
            </AdditionalInformation>
        </ChangeResult>
    </ServiceChange>
</WCSMessage>
```

C.2.2.8 Surveillance Status Report XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPA-CS:WCSMessage series="IPNA" version="1.0"
    xmlns="http://some.other.namespace/example"
    xmlns:WISPA-CS="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <WISPA-CS:SurveillanceStatusReport>
        <WISPA-CS:CaseIdentity>Case-555</WISPA-CS:CaseIdentity>
        <WISPA-CS:IAPIdentifier>iap3.isp.org</WISPA-CS:IAPIdentifier>
        <WISPA-CS:TimeStamp>2001-12-31T12:00:00.23-06:00</WISPA-CS:TimeStamp>
        <WISPA-CS:AccessSessionIdentity>
            12345
        </WISPA-CS:AccessSessionIdentity>
        <WISPA-CS:Status>
            <WISPA-CS:Status>heartbeat</WISPA-CS:Status>
        </WISPA-CS:Status>
    </WISPA-CS:SurveillanceStatusReport>
</WISPA-CS:WCSMessage>
```

C.2.2.9 VPN Security Association Establishment XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<WCSMessage series="IPNA" version="1.0"
    xmlns="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <VPNSecurityAssociationEstablish>
        <CaseIdentity>123456</CaseIdentity>
        <IAPIdentifier>vpn-concentrator.isp.com</IAPIdentifier>
        <TimeStamp>2001-12-31T12:00:00.22Z</TimeStamp>
        <SubscriberIdentity>01:03:44:02:32:21</SubscriberIdentity>
        <IPAddress>
            <IPv4Address>192.168.200.50</IPv4Address>
        </IPAddress>
        <VPNSecurityAssociationIdentity>
            253935531
        </VPNSecurityAssociationIdentity>
        <VPNSecurityAssociationProtocol>
            <Protocol>IPsec</Protocol>
            <AdditionalInformation>
                IPsec ESP/Tunnel
            </AdditionalInformation>
```

```
        </VPNSecurityAssociationProtocol>
        <LocalVPNEndpointIPAddress>
            <IPv4Address>192.168.100.100</IPv4Address>
        </LocalVPNEndpointIPAddress>
        <RemoteVPNEndpointIPAddress>
            <IPv4Address>192.168.200.50</IPv4Address>
        </RemoteVPNEndpointIPAddress>
        <LocalVPNEncryptionInformation>
            <EncryptionAlgorithm>3des-cbc</EncryptionAlgorithm>
            <EncryptionKey>
                c1ddba65 83debd62 3f6683c1 20e747ac 933d203f 4777a7ce
            </EncryptionKey>
        </LocalVPNEncryptionInformation>
        <LocalVPNEncryptionInformation>
            <EncryptionAlgorithm>hmac-md5</EncryptionAlgorithm>
            <EncryptionKey>
                3f957db9 9adddc8c 44e5739d 3f53ca0e
            </EncryptionKey>
        </LocalVPNEncryptionInformation>
    </VPNSecurityAssociationEstablish>
</WCSMessage>
```

C.2.2.10 VPN Security Association Release XML Instance Document

```
<?xml version="1.0" encoding="UTF-8"?>
<IPNA:WCSMessage series="IPNA" version="1.0"
    xmlns:IPNA="http://www.wispa.org/calea/WCS/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.wispa.org/calea/WCS/
                http://www.wispa.org/calea/WCS/WISPA-CS-IPNA-1.0.xsd">
    <IPNA:VPNSecurityAssociationRelease>
        <IPNA:CaseIdentity>123</IPNA:CaseIdentity>
        <IPNA:IAPIdentifier>IAP-5</IPNA:IAPIdentifier>
        <IPNA:TimeStamp>2001-12-31T12:00:00.5</IPNA:TimeStamp>
        <IPNA:AccessSessionIdentity>63502</IPNA:AccessSessionIdentity>
        <IPNA:VPNSecurityAssociationIdentity>
            253935531
        </IPNA:VPNSecurityAssociationIdentity>
        <IPNA:VPNTerminationReason>
            Expired SA purged from SA Database
        </IPNA:VPNTerminationReason>
    </IPNA:VPNSecurityAssociationRelease>
</IPNA:WCSMessage>
```

Appendix D. References

[1]. 47 C.F.R. § 1.20000. Purpose.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20000.htm

[2]. 47 C.F.R. § 1.20001. Scope.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20001.htm

[3]. 47 C.F.R. § 1.20002. Definitions.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20002.htm

[4]. 47 C.F.R. § 1.20003. Policies and procedures for employee supervision and control.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20003.htm

[5]. 47 C.F.R. § 1.20004. Maintaining secure and accurate records.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20004.htm

[6]. 47 C.F.R. § 1.20005. Submission of policies and procedures and Commission review.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20005.htm

[7]. 47 C.F.R. § 1.20006. Assistance capability requirements.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20006.htm

[8]. 47 C.F.R. § 1.20007. Additional assistance capability requirements for wireline, cellular, and PCS telecommunications carriers.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20007.htm

[9]. 47 C.F.R. § 1.20008. Penalties.: http://edocket.access.gpo.gov/cfr_2006/octqtr/47cfr1.20008.htm

[10]. FCC Order, Aug 9th, 2005. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A1.doc

[11]. Lawfully Authorized Electronic Surveillance For Internet Access and Services (ATIS-1000013.2007): https://www.atis.org/docstore/product.aspx?id=22665

[12]. CableLabs® Cable Broadband Intercept Specification Summary: http://www.cablemodem.com/specifications/cbis.html

[13]. The libpcap file format: http://wiki.wireshark.org/Development/LibpcapFileFormat

[14]. The pcap library: http://www.tcpdump.org/

[15]. SSH File Transfer Protocol, Version 4: http://tools.ietf.org/html/draft-ietf-secsh-filexfer-04

[16]. CALEA: http://www.askcalea.net/docs/calea.pdf