Submission to CRTC for Interim VoIP Solution
August 2009

This document represents Andrew LLC’s proposal and views on a solution for Canada’s next generation emergency calling architecture. The proposal describes the vision and ultimate direction that emergency calling procedures are taking in various standards organizations and then looks at the migratory steps necessary in order to reach this final architecture. Andrew provides an overview of its location product offerings addressing this space along with indicative cost estimates of providing such a service. Finally the proposal suggests a mechanism of cost recovery for the location platform essential to all proposed NGN emergency architectures.

Please direct all queries and correspondence concerning this submission to:

James Winterbottom
Global Product Manager
Andrew GeoLENs
IP Location Product Portfolio
james.winterbottom@andrew.com
phone: +61-2-42-212938
Executive Summary
There is a specific end-game architecture that is most appropriate to support emergency services calling over the Internet. This architecture is exemplified by the NENA i3 and IETF/ECRIT definitions. It is applicable in the long term and beyond the point where legacy PSTN, circuit services constraints, and other considerations arising from current models and assumptions cease to apply.

Migration to the end-game will likely involve interim architectural steps with associated limitations. The NENA i2 model provides a basis for this evolution. The NENA i2 model may also be sensibly modified in the short term to deal with very short term constraints associated with device and established network functionality limitations.

Fundamental to all approaches, and as a concrete starting point, the location-enabling of access networks is a critical step. LIS functionality is a common requirement to all interim steps in the evolution. A description of the Andrew GeoLENS LIS portfolio is provided to illustrate the kind of infrastructure associated with LIS deployment. Investment in the location-enabling of broadband access is necessary and it is possible to make a coarse estimate of the initial cost of deployment. A non-competitive levy is one option to provide operators with a cost recovery mechanism which, in turn, would facilitate the earliest deployment of the necessary infrastructure.

Vision
The Internet breaks the traditional perceived view of telecommunication services where the service and access are provided by the same organization. The Internet allows services to be offered independently of the access network. This is clearly demonstrated in the growth of domestic broadband, where numerous ISPs compete for customer Internet access over DSL, cable and wireless technologies, and totally independent voice providers such as Vonage and Skype compete for voice services. Neither the access provider, nor the voice provider has any direct relationship other than sharing a common subscriber.

The separation of access and service provides consumers with more choices, allows service providers to operate without requiring them to own an access network, and allows access providers to concentrate on providing big fast pipes. It also allows subscribers to take their independent application identity (e.g. VoIP phone number) from one point of access to another and between access network operators seamlessly. However, the cost of this division is that responsibilities that typically fell to a single company before now need to be divided between the access and service providers to ensure that services continue to operate correctly.

1 In fact the traditional telecommunications service in the PSTN era was the provision of a switched circuit from any network attached device (typically a telephone) to any other address (aka a phone number) on the PSTN. The use of this service for voice communication was so predominant that the perception developed that this was actually the key network “service” as opposed to actually only being an “application” of the key service (establishing a circuit on demand). Even though the key service was used for other things (Fax, security system monitoring, data communications via modems etc) the predominant nature of the voice application led to an unnecessary perceived coupling between the role of the network operator as a switched circuit provider with the use of those circuits for the voice application. In the era of the Internet, similarly, the key “service” that network operators provide is the delivery of IP “packets” over the Internet in place of the establishment of circuits. The packet model of communication, coupled with increasingly high bandwidth and always-on modes of operation permits far broader applications for the service. Voice continues to be an application that the packet mode can support though it is far less dominant and, still, is not by its nature a “key service” of the network operator.
Location, traditionally a key responsibility of the PSTN/voice service provider, becomes more specifically a responsibility of the access provider. It is the access provider that has the physical connectivity relationship with the end-user, and so they are the provider in the best position to know where the user is. This fact is recognized in the NENA i2, i3 and IETF ECRIT next generation emergency calling architectures. These architectures all have a specific node in the access network for determining and providing the location of its users. This node is called the location information server, LIS.

The LIS is local to an access network and an access network provides Internet connectivity to users within a geographical area. This means that the access network, and by extension the LIS, has a local footprint in one or more emergency jurisdictions and this makes it relatively easy\(^2\) to establish trust relationships between the access and emergency providers. This is in contrast to a voice provider that may have no local footprint in the jurisdiction from which an emergency call is being made. In the IETF ECRIT architecture a calling device is responsible for discovering the LIS in the local access network, acquiring its location, discovering a routing service, Location to Service Translation (LoST) server, obtaining a route to the emergency service routing proxy (ESRP) and then initiating a call to the ESRP, possibly through their home VSP. The architecture however does not require the involvement of a home VSP, and by excluding the VSP the solution becomes less complex and more robust as all entities by necessity reside within the same jurisdictional boundary. The general flow is shown in Figure 1.

Eliminating the VSP from the equations provides the following tangible benefits:
1. reduces the number of nodes in call establishment

\(^2\) “Relatively easy” in comparison to establishing a trust relationship between a local emergency network agency and a VoIP application provider who may be located in a completely foreign jurisdiction and with no formal presence in the local jurisdiction.

Andrew Solutions
Proprietary and Confidential
2. keeps all nodes within the same jurisdictional boundary
3. reduces the time to establish a call
4. establishes a local source to verify the veracity of location information allowing easy
   identification or erroneous location information
5. a common emergency calling semantic that works with any device capable of connecting to
   the Internet, no special voice subscription service is required
6. easy to identify which access network a call is coming from, allowing the location of dropped
   or nuisance calls to be provided

Migration towards the Vision

For the end-game architecture to operate ubiquitously across all networks for all emergency calls, all the
equipment and networks in the chain must support a common set of features and signaling. Today, for a
number of reasons, this is not the case so a migration path from the current starting position to the end-
game position is necessary.

The North American National Emergency Number Association (NENA) has described two architectures
for Next Generation emergency call (NG-911), an end-game solution, i3, and a migratory solution, i2.

NENA i2

The NENA i2 solution is designed to deliver emergency calls from the Internet to legacy public safety
answering points (PSAPs) connected to the PSTN using TDM and CAMA trunks. The preferred approach
in i2 is for a VoIP device to obtain its location from a location information server (LIS) running in the local
access network and then include location information in-band when it makes an emergency call. The
location information may be a literal location which is an actual location such as a civic street address or
a geographic area around a particular latitude and longitude for example. Alternatively it may be a
location reference which is typical a URI which resolves to an IP address and allows the recipient of the
reference to query that IP address one or more times for the corresponding literal location value. While
the nominal approach is for the device to deliver the location information to the call server, there is
scope for the call server or other routing-node to request the location of the calling device given a
suitable location key, such an IP address or location URI. This approach also requires a sufficient
association or relationship between the VSP or agent and the LIS operator for the VSP or agent to
identify and be allowed access to the correct LIS.

When the device makes an emergency call it uses its nominated VoIP service provider (VSP). The call-
server at the VSP identifies that the call is an emergency call and sends any location information it has
(this may be a literal location or a location-key possibly in the form of the calling-device’s IP address) in a
routing request to a centralized routing function, called the VoIP Positioning Centre (VPC). The VPC uses
the location information to provide a routing key, specifying which emergency service gateway (ESGW)
from the Internet to the PSTN to use, and an emergency services query key (ESQK) that is used by the
PSAP to acquire the calling-device’s location from the VPC.

The role of the VPC is to provide routing information based on the location of a caller and, to provide
location information about a calling device to a PSAP. If the VPC is only provided a location key in the
routing request then the VPC must first identify the serving LIS, and then request the location of the
caller from that LIS. The recommended protocol for the VPC to use when requesting information from
the LIS is the IETF HELD protocol [1] via either a location URI dereference [2] or as a third-party request
using device identity extensions [3].
In order for the i2 solution to work the access network must provide a LIS, and the LIS must capable of determining the location of the device attached to the network. The location provided by the LIS must be good enough, in the first instance, so that the call can be routed to the correct PSAP, and accurate enough, later on, so that dispatched services are able to find the caller. When civic address information is provided by the LIS care must be taken to ensure that the location provided by the LIS will yield a valid PSAP route when used by the routing database in the VPC. Validation of the LIS civic location information is performed against a validation database (VDB) which is directly associated with the emergency service routing database (ERDB) used by the VPC.

![Figure 2 NENA i2 architecture](image)

**NENA i3 and ECRIT**

NENA i3 is very similar to NENA i2 from an access network perspective, most of the additional functionality in i3 occurs inside the ESInet. However, there is one key difference and that is with the routing function. In i2, the route is requested by the VSP but is determined by a centralized VPC with the help of an ERDB. In ECRIT and i3, the calling device or proxy is responsible for obtaining the route to the correct ESRP. This procedure is highlighted in the following diagram.
The device does route determination by discovering the location to service translation (LoST) server that services the local access network. The device signals its location along with the identity of the service (in this case, emergency service) it wants to the LoST server, and the LoST server provide a destination address to which the device should address its call. In the emergency context, this address is called the PSAP URI. The LoST protocol is defined by the IETF in RFC5222.

**Barriers to NENA Deployments**

Despite the ground-breaking done with the definition of the i2 and i3 architectures, the NENA preferred calling model of having the VoIP end point (VEP) acquire its location and sending it in-band with the call does face some hurdles in the short term.

**Existing CPE**

No SIP clients deployed today are emergency or location aware. This means that they don’t invoke special behavior when an emergency call is made. The preferred NENA calling model requires the device to recognize that an emergency call is being placed, fetch location from a LIS, and then include this location information with the outbound call setup. Unless the device understands that an emergency dial sequence requires special attention it cannot do this, and most computer-based soft-phone and analogue terminal adapters (ATAs) do not have this capability today. Softphone and ATA deployments number in the hundreds of thousands in Canada.

---

3 An experimental emergency client based on a modified Mozilla ZAP! Client is available on the Internet and is the portent of things to come.
Andrew Solutions
Proprietary and Confidential
Including a location in call set up requires the calling device to send multi-part bodies in the SIP message, one part for the call setup and voice coding information, and a second part containing the location information. Results reported by SIPit ([https://www.sipit.net/SIPitSummaries](https://www.sipit.net/SIPitSummaries)) over the last three years show a slow uptake of multi-part SIP client support. The upshot of this is that most VoIP clients deployed today are not yet capable of sending multi-part SIP bodies. This is required to send the location information and a lack of the capability renders the preferred calling model for i2 unworkable in the interim and until the necessary CPE upgrades or replacements occur.

It is impractical to expect or mandate that all deployed CPE be upgraded to support specialized emergency call capabilities within a limited timescale. Indeed, it is largely impossible to enforce, so a practical interim solution to address existing CPE deployments is required and it needs to be one which facilitates and does not impede evolution to the correct end-architecture. This can readily be accommodated by using the VPC third-party query mechanism described earlier. Andrew notes that the CISC-ESWG consensus report approved by the CRTC ([http://www.crtc.gc.ca/eng/archive/2006/dt2006-60.htm](http://www.crtc.gc.ca/eng/archive/2006/dt2006-60.htm)) adopts this approach and, as such, does represent a sensible interim step per the preceding argument.

**Acquiring Location Information**

With the exception of cellular networks, the presence of a location server in an access network is a rarity. However, all next generation emergency networks are dependent on suitably accurate location information being available to route a call and later dispatch the appropriate responders. Furthermore, as previously described, location is most effectively determined by the operator of the access network that is providing network attachment for the calling entity. In NENA i2, NENA i3, and ECRIT it is the location information server (LIS) that provides the location service.

Two main protocols have been proposed for acquiring location information from a LIS. The first uses DHCP options and likens location information to any other host configuration. The second is HELD, an application layer protocol specifically designed for location information acquisition and which is suitable for operation across a range of network topologies including through residential gateways. As stated in the previous section, VoIP CPE does not currently support location acquisition, so any interim solution will require a service to obtain location on behalf of the calling entity from the LIS in the serving access network. Selecting a protocol that is able to provide both the longer-term LCP capabilities and the interim third-party request mechanism is desirable so that the LIS only needs to support a single location acquisition protocol. This is possible using the HELD protocol.

**Session Border Controllers**

Another key hurdle for including the location in-band with the call setup is the presence in the network of session border controllers (SBCs). SBCs are employed by almost every VoIP provider as a safeguard for their call proxies and invariably exist for traffic in-bound to the call-proxy and also often exist on the out-bound routes. The role of the SBC is to remove SIP headers and bodies that may result in proxy failures. This means that without significant reconfiguration most VSPs would strip the location information from the call initiation message prior to processing the call, rendering the preferred i2 call model inoperable. Until relatively recently the products of one of the principal SBC vendors would drop headers not directly associated with basic call setup and would provide no facility to flag additional headers for pass-through treatment. While arguably such implementations break the SIP extensibility model the fact remains that these SBCs are deployed and working today and their possible inclusion in any call setup cannot be overlooked.
Security and Privacy

SIP messaging invoked through a VSP inherently includes subscriber identification information, either as a SIP address of record (Aor) or tel URI. Adding a literal location value to this identity information introduces significant privacy concerns, particularly if the data packets are passed through intermediary nodes prior to arriving at the VSP. For this reason the IETF recommends that transport security using TLS be used, and this directly implies the use of TCP. At the time of writing only one tier-1 carrier in the United States requires the use of TLS, and the vast majority of SBCs deployed are only configured to support SIP over UDP, and many older SBCs are incapable of TCP and TLS support.

In addition to caller privacy, it is highly desirable that the emergency providers can depend on the veracity of the location being provided. Emergency organizations require caller location information to be genuine, dependable and trustworthy. These requirements can be satisfied by ensuring that:

* The location information is current
* The location information is accurate at the time it is provided
* The location is attributable to the Target entity

To date this requirement is under-addressed in all the associated standards forums. A new document [9] in the IETF attempts to describe some of the issues around addressing these three key requirements that were implicitly provided as part of the conventional PSTN service delivery model.

The most commonly proposed solution for location veracity is the use of digital signatures, often referred to as location signing. However, simply signing a piece of information that represents a location provides at most one of the above required assurances. To meet all requirements then all 3 attributes of device identity, time and location must be included in the mix. Thus far the location dependability [10] HELD extension provides the closest solution to address the location veracity issues imposed by a VEP providing a literal location value for emergency call routing and dispatch.

Location URIs are also promoted as a solution to the location veracity issue. The rationale is that the LIS must authenticate itself to the PSAP when the URI is accessed, resulting in the PSAP having an assurance of the LIS identity. This approach does not however, provide any assurance that the entity calling the PSAP is the entity associated with the location URI, it merely asserts that the location URI is associated with a device serviced by a LIS. While location URIs do not address all of the veracity requirements their use does mitigate some of the vulnerabilities posed by the use of literal locations; the main one being that to exploit the above vulnerability the attacker must either have some device with a physical presence in the serviced access network, or have access to the data stream between the VEP and the VSP.

Limiting the exposure of the ESRP and the VEP to intermediaries goes a long way to reducing vulnerabilities in the calling model and significantly reducing location veracity concerns. This will ultimately be achieved as a property of the end-game solution presented at the start of this submission which is simply one more reason why this architecture does need to be the end goal.

A Deployable Interim Solution

The previous section detailed the barriers to deploying a NG emergency calling solution that requires the VEP to acquire its location and provide this information in-band at call initiation time. A deployable interim solution therefore will seek to overcome the hurdles previously described while still introducing the critical components ultimately necessary in the NENA i3 and end-game architectures. In all of these architectures there are two common elements, a location information server in the serving access.
network, and an emergency service routing proxy, or gateway, that directs calls to the local PSAP. Any interim solution should include at least these elements.

**Addressing the Hurdles**
Many of the barriers to deploying the preferred NENA i2 and i3 call flows stem from the VEP’s need to include location in-band with the call signaling. Removing this requirement eliminates the following barriers:

1. The need to upgrade all VEPs to:
   a. acquire location
   b. support sending multi-part bodies
   c. support TLS
2. The need to upgrade all older SBCs in the network to support:
   a. SIP multi-part bodies
   b. TLS connections.
3. The location veracity issues

Eliminating in-band location signaling eliminates some of the key barriers to immediate deployment however it also constrains the information available to enable routing, which was the key reason for including the location in the first instance. In the NENA i2 architecture, route selection is done by a central node called the VPC. While the general i2 call flows describe a literal location value being provided to the VPC for use in route determination, there is explicit support for a location key element. The location key needs to contain sufficient information to enable the VPC to determine the identity of the LIS serving the caller’s access network and for the LIS to determine the location of the specific device. For public networks an IP address is generally considered sufficient for these purposes, though how the issue of mapping from IP address to LIS address is resolved varies from implementation to implementation. There is a strong suggestion in the IETF that the LIS discovery through a residential gateway proposal in [3] could also be used by a VPC to map the VEP IP address to a LIS address. If this is true then configuration established as part of the interim solution can be reused without modification for later migratory solution and, indeed, the end-game architecture.

**Acquiring Location**
Location information is acquired from the location information server in the access network serving the caller. We have established that for an interim solution to work consistently from one VSP to the next, without call loss or wholesale network and CPE replacement, that the VEP cannot reliably obtain and provide location information for call routing and dispatch purposes. This places the responsibility on either the VSP or the VPC.

There are privacy issues with freely providing location information to anyone that asks. Consequently, before a LIS can provide location information for a target device it needs to be satisfied that the requesting entity is authorized to have this information. This is particularly true in the case of third-party requests which are necessary if the VEP does not include location in-band with the call. In the context of this submission, the LIS needs to know that the third-party request is coming from an entity that will only use location information for emergency purposes. This requires the LIS to trust the requesting entity.

Trust between entities is usually established in the Internet using cryptographic techniques, commonly via X.509 digital certificates. Digital certificates are used to assert identity and can subsequently be used to generate cipher keys suitable to ensure communication secrecy. Identity assertion can be achieved
through a direct relationship between the sender and receiver of a certificate, but is more commonly achieved by the sender and receiver of a certificate having a common trust anchor with some well respected third-party; that party being typically referred to as a Certificate Authority. The third-party essentially vouches for the identity of the certificate sender. Management of digital certificates presents some issues, the reliability and trustworthiness of certificates is directly tied to how well they are managed. A smaller number of certificates is easier to control than a larger number, so constraining the number of certificates improves their trustworthiness.

In an emergency services context, constraining the number of certificates directly impacts the number of entities that can request location from a LIS. However, this improves the privacy and maintains the integrity of the certificates. Each LIS requires a certificate as it needs to assert its identity and its authority in order to provide location information suitable for emergency services. This is largely inescapable. Security dilution is prevented by keeping the number of nodes in the call process that can request information from the LIS to a minimum. This logically leads to the conclusion that the VPC needs to have the trust relationship with the LIS, as these are few in number, rather than VSPs which are more numerous and may not be located in a jurisdiction with which a trust relationship can comfortably be established.

Dedicated network connections between a VPC and the LIS in each ISP may also be used. These connections may be established using virtual private network (VPN) tunnels instead of public connections. The advantage of this solution is that may reduce the overheads of certificate management and allow commercial off-the-shelf VPN hardware to be used. When using connections established in this manner the LIS trusts that all location requests originating from the VPN are authorized to obtain location information for the Target. It is a jurisdictional consideration as to whether it is more practical to maintain persistent concurrent VPN relationships between all VPC and LIS instances or whether authentication should occur dynamically and on demand.

Call initiation and routing
Call initiation in any interim solution will go through the caller’s VSP. The VSP will need to detect that the call is an emergency call and either request routing instruction directly from a VPC, or direct the call to a routing proxy. In the former case, the NENA i2 V2 interface is recommended and the location key can be the calling-device’s IP address. In the latter case the NENA V5 and V2 interfaces are used, and the calling-device’s IP address is similarly used as the location key to the VPC.

The VPC is able, given the right circumstances, to determine the serving LIS based on the IP address, retrieve location, select a route, and direct the call to the correct PSAP.

Conclusions
It is Andrew’s conclusion that any interim NG VoIP emergency calling solution that has to support existing VoIP deployments without extensive CPE and core network infrastructure changes will require the following:

1. LIS in the serving access networks able to handle trusted third-party requests from a VPC.
2. Emergency call detection and handling procedures in the VSP
3. VPC functions able to map caller IP address or other identifier to LIS address
4. VPC functions able to make trusted third-party requests to the LIS
5. Routing-proxy and ESGW functionality to deliver calls from the IP network to the PSAP.
6. A mechanism to deliver location associated with a call from the VPC to the PSAP.
This architecture and its functions are in alignment with the candidate proposal in the CISC-ESWG consensus report to the CRTC in May 2006 (http://www.crtc.gc.ca/public/cisc/es/ESRE0044%20.doc) and which was subsequently approved by the CRTC in September 2006 (http://www.crtc.gc.ca/eng/archive/2006/dt2006‐60.htm).

In addition to supporting immediate needs, for both wireline and wireless VoIP callers, this architecture with minimal changes adapts to support the end-game architecture even if the PSAP network remains on TDM or CAMA trunks, providing support for all emergency calls made within Canada. It is important to note that the i2 architecture, and variants based on it, is not mutually exclusive to the ECRIT/i3 architecture and, in fact, provides a logical interim step in the evolution to the latter but can also stay in place in parallel during an overlap period. That is, some emergency calls from legacy devices are effectively initiated at the VSP level with call associated information being delivered by the mechanism of the VPC while, at the same time, ECRIT-compliant devices are also able to initiate emergency calls via native LIS and LoST interaction capabilities. The same LIS infrastructure evolves to support both models transparently during this interim period of overlap and end-game migration to the point shown below.
In Figure 5 the VEP acquires its location and a location URI from the LIS using HELD. It is able to query a LoST server to obtain the ESRP (previously the routing-proxy) address and then direct a call to the ESRP including only the location URI. The access network is able to detect the destination of the IP traffic and so employ least cost routing techniques or a dedicated VPN to minimize the number of hops to the ESRP. By taking this approach and constraining location URI access to valid emergency entities SIP over UDP is a valid solution, avoiding the need upgrade the ESRP to support TLS. The location key sent to the VPC over the V2 interface becomes the location URI eliminating the need to perform LIS discovery using the VEP’s IP address.

Figure 5 Migration to End-Game legacy PSAP

Figure 6 Final migration IP-enabled PSAPs
Andrew’s LIS offerings

Andrew recognizes that it is fundamental to the feasibility of the NGN emergency services architectures that real commercial product is available to support the necessary network node functionality and is pleased to inform the CRTC that Andrew will make LIS product available in the Canadian market. Andrew has 2 main product offerings in the residential broadband location space, these are Internet service provider (ISP) LIS, and the Broadband Provider (BP) LIS. These are described in more detail in the following sections.

Internet service provider location information server (ISP LIS)

The Andrew GeoLEnS ISP LIS is designed to provide Internet service providers with the capabilities they need to meet subscriber expectations and jurisdictional obligations.

The GeoLEnS ISP LIS is a scalable platform that can accommodate small, medium and large Internet providers using various underlying technologies. Operators manage multiple access networks using different underlying technologies and the ISP LIS is flexible enough to support these on the same platform while maintaining logical network separation.

In deployments where the infrastructure provider does not make static location information directly available to the ISP, the ISP LIS is able to interface to a regional broadband provider LIS (RANP-LIS) using HELD [1] with associated network measurements [14]. In this case the GeoLEnS ISP LIS uses network parameters to determine which broadband provider LIS to contact, the resulting location is determined by the broadband provider LIS, but is made available to the users of applications by the ISP LIS.
In cases where an infrastructure provider makes static location information directly available to the ISP, the Internet provider can store these records directly in the GeoLENs ISP LIS. The GeoLENs ISP LIS supports a large number of static identifier to location mapping records that can be quickly loaded and changed as required.

In some environments there is a dynamic binding between the statically provisioned identifier, which maps to location, and the IP address of the device. In these configurations the GeoLENs ISP LIS resolves the dynamic binding by using AAA or DHCP data prior to determining the corresponding location of the device.
The GeoLEns ISP LIS uses the HELD protocol as the means to provide location information to requesting entities. It supports Target requests, third-party requests [3] and location requests made through a location URI [2]. Location information is returned as a PIDF-LO [11] and may contain civic [12] and/or geodetic location information. All location information provided by the GeoLEns ISP LIS complies with the rules and guidelines specified in RFC5491 [13].

**Broadband provider location information server (BP-LIS)**

The Andrew GeoLEns broadband provider (BP) LIS is designed to give infrastructure providers the capabilities they need to service their wholesale access customers’ and their own ISP location needs. The GeoLEns BP-LIS interoperates with the GeoLEns ISP LIS providing the end to end location solution for single and multi party provider broadband networks.

The BP-LIS is a scalable platform that can accommodate multiple network technologies. Operators manage networks using different underlying technologies and the BP-LIS is flexible enough to support these on the same platform while maintaining logical network separation.
For access providers that not only wholesale access but also provide their own ISP service the BP-LIS provides the option to integrate ISP-LIS functionality. In this configuration the system operates as a BP-ISP-LIS combination system, servicing both independent ISP and direct subscriber requests. System configuration ensures that query traffic for each ISP and end-subscriber traffic maintain logical and, where required, physical separation.

The BP-LIS is queried by an ISP-LIS using the HELD protocol [1] and supports a range of HELD identity extensions [3] and measurement types [14] to assist with location determination. Connectivity to the BP-LIS can be performed over TLS or VPN tunnel and both HELD over HTTP and HELD over BEEP [15] are supported.

The BP-LIS is able to communicate with a range of network nodes, including RADIUS, Diameter, and DHCP servers, in order to obtain dynamic network measurements relating to a device’s network...
attachment. This dynamic information is then correlated with static information which is provisioned into the BP-LIS from operator OSS systems. The correlation of the dynamic and static information and the application of any necessary arithmetic processing by the BP-LIS yields the location of the attached device.

The BP-LIS returns location information as a PIDF-LO [11] and may contain civic [12] and/or geodetic location information. All location information provided by the BP-LIS complies with the rules and guidelines specified in RFC5491 [13].

The BP-LIS is deployable as a high-availability, 5 9’s reliable, and NEBS compliant system providing a level of reliability suitable for emergency services. It is able to store 10s of millions of location records and provide service to multiple third party ISPs concurrently.

The above details of the GeoLEns LIS portfolio are provided as a positive indication to the CRTC that commercial product supporting the necessary node functionality for the i2 and ECRIT/i3 NGN-911 architectures is available. The additional detail is provided as an aid to understanding the manner in which operators may deploy these nodes and integrate them into the network.

Cost and Cost Recovery for Location Infrastructure
Consultation with various industry participants has indicated to Andrew that actual cost quantification is critical to progressing the decision making process in this important area of deliberation. In response to requests from industry participants and in the spirit of this need, to the best of its ability, and without any admission to binding agreement, Andrew provides the following conservative estimate of the cost of location enabling modern broadband networks.

The cost estimate covers the provision of LIS equipment with initial installation and necessary data grooming to location enable the access network. Other sources of costs across the industry will be in the recurring cost of operation, modifications to devices, call routing functions and those network elements and CPE which are required in the emergency network infrastructure. Andrew notes that these are areas outside its expertise and limits comment to the estimate cost of the deployment of LIS capability and consequent location enabling of the access.

Andrew estimates that the cost of location enabling a broadband network is in the order of $10 per subscriber. This value is indicative only and can be expected to be subject to the normal effects of economy of scale and other factors. To enable a network of one million residential addresses, for example, would cost in the order of $10 million dollars.

Cost Recovery
9-1-1 services are often funded by operators appending a levy to cellular customer bills. This levy is typically used to fund the emergency network infrastructure. Generally network operators are not provided a mechanism to recover the costs associated with their own infrastructure in support of 9-1-1. This situation can lead to a reluctance to invest and associated delays in deployment of this important infrastructure.

In NG-9-1-1 significant costs fall on the access providers to support the necessary location service elements. A lesser impost is required of the voice service providers and, ultimately, the ECRIT/i3 model can obviate any need for the VSP to provide network capabilities given emergency call procedures can be handled natively in the calling device with direct connectivity to the emergency service. Broadband
providers including infrastructure and ISP operators provide access to the Internet as their primary service but they may be required to provide location information to ensure that NG 9-1-1 infrastructure is universally available for all users.

Network operators may be able to recover the investment required to location enable their network by revenue derived from commercial subscriptions to the location service or by the sale of location-based applications that utilize the location service. However, this requires a degree of risk on the part of the operator and any reluctance with respect to those risk elements will naturally lead to a delay in the deployment of the necessary functionality. An alternative approach is to apply a cross-the-board levy to broadband Internet subscriptions in both the retail and wholesale markets that has the express purpose of funding the development of the network location infrastructure. Such a levy can address the cost-recovery issue while maintaining a level playing field since it would apply equally to all competitive providers. Consideration may also be given to making the cost-recovery levy temporary (for example, five years) with a view to chiefly addressing the non-recurring capital investment required to location enable the networks and permitting a window of opportunity for operators to otherwise develop a model to monetize the location capability to cover ongoing costs.

The previously stated estimate of the cost to location enable a network is $10 per subscriber. A 0.20c monthly levy would lead to initial cost recovery within a five year period with a higher levy resulting in a corresponding reduction of that cost recovery period.
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AoR</td>
<td>Address of Record. A SIP subscriber identifier</td>
</tr>
<tr>
<td>ATA</td>
<td>Analog Telephone Adapter</td>
</tr>
<tr>
<td>BEEP</td>
<td>Blocks Extensible Exchange Protocol</td>
</tr>
<tr>
<td>BP</td>
<td>Broadband Provider</td>
</tr>
<tr>
<td>B2BUA</td>
<td>Back to Back user Agent (UAS one side and UAC the other)</td>
</tr>
<tr>
<td>CAMA</td>
<td>Centralized Automatic Message Accounting</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer Premise Equipment</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>ERDB</td>
<td>Emergency Service Routing Database</td>
</tr>
<tr>
<td>ESGW</td>
<td>Emergency Services Gateway</td>
</tr>
<tr>
<td>ESQK</td>
<td>Emergency Services Query Key</td>
</tr>
<tr>
<td>ESRP</td>
<td>Emergency Services Routing Proxy</td>
</tr>
<tr>
<td>HELD</td>
<td>HTTP Enabled Location Delivery</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper-Text Transfer Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LIS</td>
<td>Location Information Server</td>
</tr>
<tr>
<td>LoST</td>
<td>Location to Service Translation</td>
</tr>
<tr>
<td>NENA</td>
<td>National Emergency Number Association</td>
</tr>
<tr>
<td>OSS</td>
<td>Operational and Support Systems</td>
</tr>
<tr>
<td>PIDF-LO</td>
<td>Presence Information Data Format – Location Object</td>
</tr>
<tr>
<td>PPP</td>
<td>Peer to Peer Protocol</td>
</tr>
<tr>
<td>PSAP</td>
<td>Public Safety Answering Point</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switch Telephone Network</td>
</tr>
<tr>
<td>RG</td>
<td>Residential Gateway</td>
</tr>
<tr>
<td>SBC</td>
<td>Session Border Controller</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplex</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
**UAC** User Agent Client (SIP end client)

**UAS** User Agent Server (SIP end Server)

**UDP** User Datagram Protocol

**URI** Universal Resource Identifier

**VDB** Validation Database

**VEP** VoIP End Point

**VoIP** Voice over IP

**VPC** VoIP Positioning Centre

**VPN** Virtual Private Network

**VSP** VoIP Service Provider

**WAN** Wide Area Network

**References**


[12] “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)”, RFC-5139, Thomson and Winterbottom


