NICS Guidance for Position Location Information (PLI)

Purpose

This document proposes preferred methods and mechanisms for delivering real-time Position Location Information (PLI) to the NICS system. The focus of the guidance is for vehicle, personal, and air PLI for the purpose of enhancing situational awareness for disaster response scenarios - both within NICS and for redistribution to other organizations.

High Level Goals Summary

- Data format
  - Easy to implement
  - Well known & commonly used standard (or standards)
  - Schema commonly used within the NICS community
- Data content
  - Delivery of fundamental information, not decoration (icons for example)
  - Fundamental information includes
    - Identity
    - Time
    - Position, (velocity , …)
  - Allow ability to ***optionally*** include other information that is tightly bound to the fundamental information
    - Security classification or distribution sensitivity information
    - Other metadata related to the fundamental data quality or technical aspects of collection
      - Location accuracy information
      - For cell generated PLI, handset signal strength
- Latency
  - PLI information should be delivered with as little latency as possible, in the context of other system constraints in order to be able to satisfy a wider variety of downstream requirements.
  - Individual PLI updates from each source should be delivered to NICS as directly as possible on a per-update basis. Accumulating updates and periodically sending them as a set introduces mean latency equal to half the update set interval.
- Security
  - Provide encryption, authentication, and authorization functionality as needed to support handling sensitive information (LEA for example)
  - Separate security processing considerations from general PLI data handling

- Support for multi-layer security processing

PLI Considerations

Types

- Personal PLI from smart phones and other mobile devices with GPS and comm capabilities (SPOT units, DeLorme units, etc).
- Vehicle PLI originating from units like the Riverside MDC ToughBooks.
- Air PLI originating either from portable units like MDC Toughbooks, or other technologies
- Miscellaneous sources such as voice/sms information with GPS or address information, which can be transformed or adapted to populate a PLI message.

Data Formats

JSON

JSON (JavaScript Object Notation) is a text-based open standard designed for human-readable data interchange that is widely supported, and has been used by NICS for PLI message publish/subscribe distribution - for land/sea/air applications – both in CalFire/Riverside, GoMEX response, FEMA exercises, and other first responder events.

We highly recommend that for the purpose of transmitting basic, low-latency PLI information that no styling formation be included in the messages – such as icon references, etc. We also recommend that important information that is not defined in this document be included in the optional "extended" field using name/value pairs.

Some notes follow:

- An object identifier "id" is mandatory. This must be unique for each object. We propose using a W3C standard for identifiers (***info***) that will enable unique domain specific identifiers to retain control of semantics for the domain.
  - An **info** identifier contains elements "info:" followed by an issuing authority; followed by a slash ("/"); followed by the specification and version; followed by a ":"; followed by a unique identifier for the PLI device, including the organization. .
  - An example of an info token could be something along the lines of "`info:us.ma.mit.ll.nics/pli.json.v1:us.ca.calfire.rru/e4`"
    - The element '`us.ma.mit.ll.nics`' specifies a domain name authority which controls the formatting/organization of the following identification information.
    - '`pli.json.v1`' specifies the format specification and version.
    - '`us.ca.calfire.rru`' specifies the unique identifier for the organization (CAL FIRE in this case).
    - '`e4`' is the unit identifier relevant to the enterprise (CAL FIRE, in this case).

- An example of a JSON PLI message is shown below. All fields are required, but not all values are required. Mandatory parts are colored as green, optional elements are encoded as orange.

```
{
    "id":"info:us.ma.mit.ll.nics/pli.json.v1:us.ca.calfire.rru/e4",
    "name":"E4 Android Smartphone",
    "description":"Search and Rescue Worker, on foot",
    "point":"-117.71235,32.41245",
    "course":"231",
    "speed":"3",
    "extended":
    {
        "Organization":"MITLL",
        "Incident":"Test",
        "Role":"IncidentCommander"
    },
    "timestamp":"2013-01-28T19:47:53Z",
    "version":"0.0.1"
}
```

  - Note that **id**, t**imestamp**, and p**oint** elements are mandatory.
  - Time is represented as UTC using W3C specification and position is lat/lon/altitude (WGS84) in units of degrees.
  - A **name** element is optional, but is often useful to have for quick looks at the data, particularly if the organizational unit uses an **id** encoding that does not reveal human readable information.
  - A **description** element is optional. It may be useful in certain situations to like sending geo-coded status, or other textual information.
  - Additional information elements like incident, role, etc. can be added as "extended" name/value pair fields, as shown in the example.

Other Formats

Other NICS supported formats include Cursor On Target (CoT), KML/GML Placemarks, EDXL-DE, among others.

Transport & Security

Background

NICS can be utilized for different homeland protection missions, each with different security requirements. Different mission areas are likely to use different technologies for security and data transport. Additionally, there are dependencies between security models and technologies. Consequently, we expect that at the very least the NICS data ingest and production functionality will have to be nimble with respect to different transport and security requirements.

We understand that security requirements are often relatively modest for the Disaster Response Community, at least as compared to that of LEA and DoD systems. Some minimal requirements from DHS involve encryption of information using the AES-256 algorithm. We also think that some client/server authentication mechanisms be in place, and that we try to use (at least initially) simple and ubiquitous transport technology that has no operating system dependencies.

Transport

NICS has service elements available to that can ingest service based on various protocols – such as UDP, and https.

- For secure asynchronous delivery of data to NICS, PLI should be sent to a NICS ingest service that utilizes https/AES256 encryption.
- The ingest https service additionally provides service authentication (via Entrust) to the client to insure that the PLI will not be hijacked or accessible to man-in-the-middle attaches.
- Https is a simple, ubiquitous, and non-proprietary technology.
- The interface can be configured so that it has good performance and lossless data transfer.
- The client may send multiple (concatenated) messages to the server in a single request.
- If guaranteed delivery of PLI nor security is an issue (sometimes the case for initial testing), it may be preferable to send Placemarks to via UDP. Use of this connectionless protocol can simplify things for both the client and the service.

Evolution

We expect to be dealing with more stringent security requirements and different transports for NICS in the near future. Those requirements will necessitate having to stand up mechanisms for certificate based authentication and authorization mechanisms for clients, servers, and users. As these capabilities come online there will be an opportunity to upgrade the PLI service model.