INSTITUTE FOR DEFENSE ANALYSES

# Department of Defense Public Safety and Emergency Management Communications: Interoperability Data Requirements


Serena Chan, *Project Leader*

Brian A. Haugh
Francisco L. Loaiza-Lemos
Steven P. Wartik



March 21, 2017

Approved for public release; distribution is unlimited.

IDA Document
D-8416

Log: H 2017-000202

Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

*The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.*

**About This Publication**

**This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task ET-5-4155, "DoD First Responder Communications Interoperability," for the offices of the ODNI PM-ISE and DoD CIO C4&IIC. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.**

**Acknowledgments**
**Reginald N. Meeson**

**For more information:**

**Serena Chan, Project Leader**
**schan@ida.org, 703-933-6563**

**Margaret E. Myers, Director, Information Technology and Systems Division**
**mmyers@ida.org, 703-578-2782**

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-8416

# Department of Defense Public Safety and Emergency Management Communications: Interoperability Data Requirements

Serena Chan, *Project Leader*

Brian A. Haugh
Francisco L. Loaiza-Lemos
Steven P. Wartik

# Executive Summary

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO).

The objective of this project is to assess the current state of communications interoperability between DoD public safety and emergency management (PS/EM) entities and United States (U.S.) civilian PS/EM entities, and how that is likely to change as the next generation of public safety information systems is implemented across the nation. This white paper addresses one aspect of this project—assessing the *data requirements* for information exchanges involving DoD PS/EM entities and U.S. civilian PS/EM entities.

IDA's investigations into systems, data standards, and exchanges for DoD and U.S. civilian PS/EM communications have revealed the dominance of the Common Alerting Protocol (CAP) standard from the Organization for the Advancement of Structured Information Standards (OASIS) in public safety warnings and notifications. A related white paper[1] prepared for this project, which surveys civilian and DoD mass warning and notification systems, identifies many systems using the CAP standard for formulating alert messages. CAP and other OASIS standards comprising the Emergency Data Exchange Language (EDXL) are incorporated into the Emergency Management (EM) Domain of the National Information Exchange Model (NIEM) so that a NIEM information exchange can contain a CAP-compliant alert message.

Given CAP's dominance in mass warning and notification systems, CAP data elements must be an essential part of any compilation of data requirements for DoD and U.S. civilian PS/EM communications. The EDXL-DE (Distribution Element) standard should be essential because it captures metadata about specific emergency communications, such as alerts using CAP. Support for the EDXL-HAVE (Hospital AVailability Exchange) standard should be required because incidents with many casualties will require emergency management entities to be notified of available hospital services and patient beds. The EDXL-RM (Resource Message) supports a complementary set of messages involving requests for, responses from, or reports on available emergency management resources, including personnel and vehicles.

---

[1] Institute for Defense Analyses, *A Survey of Mass Warning and Notification Systems,* IDA Document D-8388, March 21, 2017.

The National Emergency Number Association (NENA) has developed data sharing standards to support information sharing related to 9-1-1 calls. NENA's Next Generation 9-1-1 standards are essential data requirements for future DoD and U.S. civilian public safety 9-1-1 systems, although not necessarily for PS/EM personnel who use those systems. The IDA team analyzed NENA's data standards on automated data exchanges between 9-1-1 system components which provide data requirements for 9-1-1 systems but not for data exchanges directly to PS/EM entities. The new 2017 joint standard from NENA and the Association of Public-Safety Communications Officials (APCO) International for an Emergency Incident Data Document (EIDD) is designed to capture emergency incident data that could be shared directly with PS/EM entities. As such, the EIDD provides a set of data elements that need to be supported in next-generation information exchanges among DoD and U.S. civilian PS/EM entities.

The NIEM EM Domain data elements support "emergency-related services (including preparations and responses by emergency management entities), information sharing, and activities such as homeland security and resource communications management."[2] As such, the vast majority of the data elements developed within the EM Domain namespace will have direct relevance to information sharing with and between PS/EM entities.

Other data requirements come from the Computer Aided Dispatch (CAD) systems used by Public Safety Answering Points (PSAPs) to assist in initiating calls for service, dispatching, and maintaining the status of responding resources in the field. There are numerous vendors of such CAD systems, which may use different internal data elements. However, the APCO codes[3] and new NENA/APCO EIDD standard[4] offer promise for greater standardization in this area.

The Keystone middleware's use of a common lingua franca based on widely used data standards, such as NIEM and CAP, facilitates interoperability among diverse alerting and emergency management systems. The Keystone and Unified Incident Command and Decision Support (UICDS) service definitions serve to identify many of the data elements needed for the interoperation of such systems and their communications with PS/EM entities.

IDA's investigations into data requirements for information exchanges between DoD and U.S. civilian PS/EM entities identified a set of data standards that need to be considered for use in future DoD and U.S. civilian PS/EM communications systems, such as FirstNet. The IDA team will use these standards in developing a semantic model (an ontology) of core PS/EM communications data requirements to facilitate semantic interoperability and enable automated reasoning with such data. Additionally, the IDA team will conduct an analysis of overlap amongst these standards, to be reported in a subsequent white paper.

---

2 As described on the NIEM EM Domain webpage: https://www.niem.gov/communities/emergency-management

3 APCO International, *ANS1.116.1-2015 Public Safety Communications Common Status Codes For Data Exchange.* https://www.apcointl.org/doc/911-resources/apco-standards/601-11161-2015-status-codes/file.html

4 *APCO/NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD),* January 2017.

# Contents

## Table of Figures

# Table of Tables

# 1. Introduction

## A. Background

### 1. Issues

Department of Defense (DoD) public safety and emergency management (PS/EM) entities and U.S. civilian PS/EM entities have time-critical needs to communicate effectively in order to coordinate responses to public safety incidents. Some DoD military bases in the United States depend upon civilian firefighting and Emergency Medical Services (EMS) for response to incidents on base. Public Safety Answering Points (PSAPs) serving DoD bases may need to dispatch requests to civilian public safety responders when they do not have the requisite organic services on base or if they are overwhelmed. On the other hand, civilian field responders may need to request and coordinate with military emergency management entities, especially with the National Guard, when confronted with situations requiring defense support to civil authorities (DSCA) and humanitarian assistance and disaster relief (HADR). Many different lines of communication are available for such coordination, including Computer Aided Dispatch (CAD) from PSAPs, and shared websites, such as WebEOC and the All Partners Access Network (APAN). However, better understanding of these communications capabilities and requirements is needed, especially as we move into the next generation of public safety information systems, such as FirstNet[1] and Next Generation 9-1-1.[2] We need to better understand what the existing communication systems are, how interoperable they are, and what public safety information-sharing requirements they serve. Such an improved understanding can provide a foundation for migrating to next-generation systems that can exceed current capabilities and meet future needs.

Two major offices within the Executive Branch of the Federal Government have responsibilities and authorities appropriate for promoting effective next-generation communications between DoD PS/EM entities and civilian PS/EM entities. The Office of the Program Manager, Information Sharing Environment (PM-ISE) works with the law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs communities to improve the management, discovery, and sharing of information related to counterterrorism, homeland security, and weapons of mass destruction. The Office of the PM-ISE facilitates the development of responsible information sharing by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best

[1] Emergency management Network Authority (FirstNet), 2017. http://www.firstnet.gov/

[2] National Emergency Number Association (NENA), NG9-1-1 Project, 2017. http://www.nena.org/?NG911_Project

practices. In collaboration with the PM-ISE, the DoD Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC) is working with all levels of government and the private and nonprofit sectors on the following activities: improving the information-sharing environment for the National Public Safety Communications Enterprise (NPSCE); adopting the National Information Exchange Model (NIEM) for government-wide information sharing; and supporting the development of additional information infrastructure components, such as models and the rigorous specification of their semantics needed to improve the quality of proposed solutions.[3] Given their overlapping responsibilities, these two offices are collaborating to assess the status and direction of DoD and civilian PS/EM communications.

## 2. Project

To address the issues described, the Offices of the PM-ISE and the DCIO (C4&IIC) asked the Institute for Defense Analyses (IDA) to perform analyses to assess the current state of interoperability between DoD PS/EM entities and U.S. civilian PS/EM entities, and how that is likely to change as the next generation of public safety information systems is implemented across the nation (e.g., Next Generation 9-1-1 and FirstNet). In support of these analyses, the IDA team collected information on the types of data required for representative DoD−civilian emergency management communications. Commonalities among these data elements will be analyzed and their concepts formalized using a formal semantic model. Then, the feasibility of using NIEM to support information exchanges using these concepts will be assessed. This white paper addresses one aspect of this project: assessing the types of data required to support information exchanges between DoD and U.S. civilian PS/EM entities.

## 3. The National Information Exchange Model

The need for common vocabularies and information-sharing formats to enable sharing and correlating information between DoD and U.S. civilian PS/EM entities has been well recognized across the government, including federal, state, local, tribal, and territorial (SLTT) levels of government. A documented best practice for such information sharing is the use of NIEM.[4] Thus, it is natural to look to using NIEM as a common information model to facilitate communications between DoD and U.S. civilian PS/EM entities.

---

[3] Institute for Defense Analyses, *DoD First Responder Communications Interoperability*, IDA Project Description ET-5-4155, June, 2016.

[4] Standards Coordinating Council, *Fusion Center Best Practices Include Information Sharing and Access Standards*, 2016. http://www.standardscoordination.org/content/fusion-center-best-practices-include-information-sharing-and-access-standards.
Federal CIO Council, *Agency Information Exchange Functional Standards Evaluation*, 2010. https://cio.gov/wp-content/uploads/downloads/2012/09/3.12.1-NIEM-Assessment-Report_Final_Master.pdf

NIEM was developed initially by collaborative efforts between the Department of Justice (DOJ) and the Department of Homeland Security (DHS) to provide a set of common, well-defined data elements for sharing information related to law enforcement and homeland security. All 50 states and the majority of federal agencies are now using (at varying levels of maturity) or considering using NIEM.[5] DoD has adopted a NIEM First strategy, which requires that the NIEM standards-based approach be considered first when developing information exchanges based on the eXtensible Markup Language (XML).[6] NIEM has been widely adopted in the Public Safety sector for activities, such as Suspicious Activity Reporting (SAR), at the SLTT and the federal levels of government.

NIEM provides both a standard data model and a standard process for developing specific information exchanges. As illustrated in Figure 1-1, the NIEM data model consists of a common core of reusable data elements extended by specialized domain models, such as *Emergency Management* (EM). The EM domain model has been designed to support exchanges for PS/EM communications in emergency situations. The NIEM process also provides a methodology for supplementing existing models with additional data elements or even establishing new domains as needed. In any case, the fully formalized use of NIEM involves development of Information Exchange Package Documentations (IEPDs) to describe the formats and intended interpretations of specific types of exchanges of information. IEPDs leveraging the EM domain have been developed and used for standardizing some PS/EM communications. NIEM domains can be expanded to meet any additional data requirements identified for PS/EM communications.

---

5 https://www.niem.gov/aboutniem/Pages/history.aspx

6 Department of Defense, *Adoption of the National Information Exchange Model within the Department of Defense*, DoD CIO Memorandum, March 28, 2013. http://dodcio.defense.gov/Portals/0/Documents/2013-03-28%20Adoption%20of%20the%20NIEM%20within%20the%20DoD.pdf

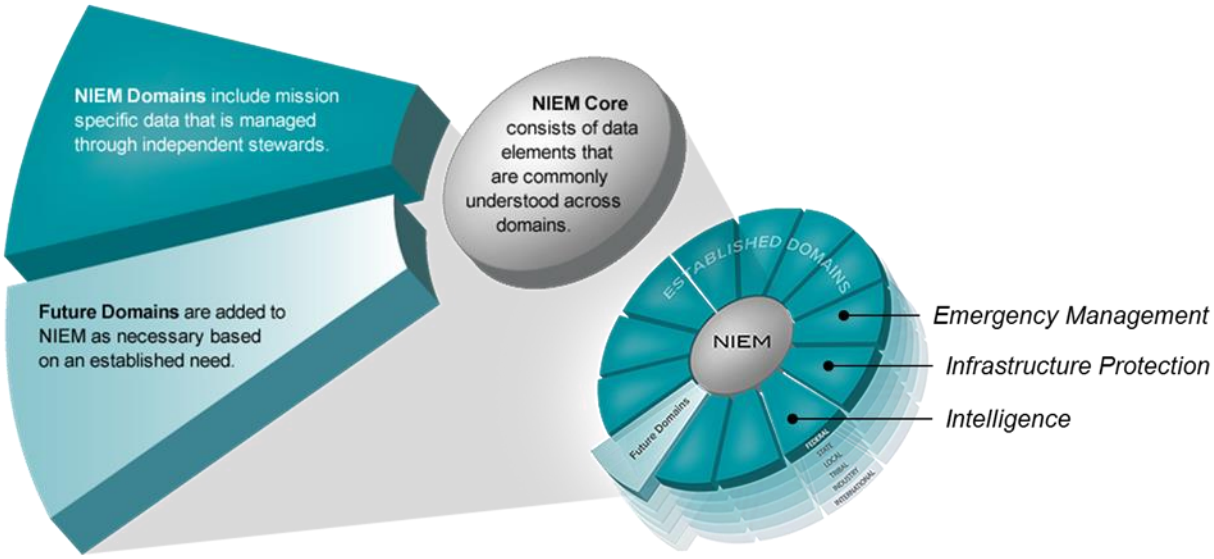


**Figure 1-1. NIEM Core and Example Domains[7]**

## B. Approach

The IDA team took a multi-faceted approach to identifying data requirements for communications between DoD and U.S. civilian PS/EM entities. Initial plans called for identifying a subset of representative DoD–civilian PS/EM information exchanges and extracting their data elements as example requirements. However, it proved difficult to acquire a reasonable number of examples of such specific exchanges. To supplement the limited number of specific exchanges identified, those data standards that have been designed to support emergency notifications and management were investigated as sources of data requirements.

Relevant data standards, such as the NIEM EM Domain and the Common Alerting Protocol (CAP), were investigated for their scope and usage. Specific examples of exchange specifications based on these standards were sought. Outreach to the facilitator of the NIEM EM Domain identified a specific NIEM IEPD for Interconnected Emergency Operation Centers (iEOC) developed by DHS, which leverages some NIEM domains and external standards. Outreach to the NIEM Program Management Office (PMO) established contacts with others using NIEM, including those working with the NIEM MilOps Domain under DoD stewardship.

Separate outreach to the DoD CIO Office Deputy for Architecture and Information Sharing established further contacts within DoD, including the National Guard Bureau, which shared details of their current and planned systems and tools for PS/EM information sharing. A related activity under this project identified and investigated major mass warning and notification systems

[7] Adapted from the NIEM website to illustrate several relevant domains. https://www.niem.gov/technical/Pages/The-Model.aspx

employed by the civilian sector and DoD to alert individuals.[8] These systems were then further investigated to determine, insofar as possible, what data standards or data models they are using. One of the systems investigated—Keystone—was found to incorporate NIEM-compliant exchange schemas as a lingua franca to share emergency incident data between systems using different data standards. In addition, an informal survey on current systems, data, and practices in this domain was distributed to DoD personnel known to be engaged with civilian PS/EM entities. This survey returned some information on PS/EM communications systems used by DoD, which were further investigated for their data requirements.

## C. Overview

Section 2 begins with an initial focus on the data requirements already identified within NIEM as most relevant to PS/EM communications, which are grouped together in the NIEM Emergency Management (EM) Domain. It provides an overview of the NIEM EM Domain, including listings of the many categories of data types and data elements defined specifically for this domain. It does not enumerate every data type or element since those details are readily available online from the NIEM EM Domain website.

Section 3 reviews the Emergency Data Exchange Language (EDXL). This composite standard from the Organization for the Advancement of Structured Information Standards (OASIS) is obviously targeted at supporting emergency situation data exchanges and is widely used by public alerting and notification systems. Much of the EDXL standard is also incorporated into the NIEM EM Domain as an external standard. This paper briefly reviews each of the principal EDXL component standards using their object model or reference model diagrams to provide an overview of their supported data content. Because the CAP component of EDXL has seen nearly universal support by public alerting and notification systems, this paper includes an appendix that delineates its data elements. All of these data elements can be considered essential requirements of any system supporting DoD-civilian PS/EM data communications. Detailed documentation of this and the other EDXL standards is readily available from the OASIS website.

Section 4 presents an overview of data elements required by CAD systems used by 9-1-1 PSAPs. The presentation abstracts from the CAD systems documentation the specific data elements needed to identify the WHO, WHAT, WHERE, and WHEN of the incident data of a 9-1-1 call. This is followed, in Section 5, by an overview of the National Emergency Number Association (NENA) data requirements, which provide detailed data structures for sharing 9-1-1 data amongst 9-1-1 communications system components. NENA's standards development activities have produced collections of XML schemas for communicating messages to, from, and among professionals and systems involved in 9-1-1 communications. The body of this paper provides an overview of the types of data required by the many NENA schemas. Detailed

---

[8] Institute for Defense Analyses, *A Survey of Mass Warning and Notification Systems,* IDA Document D-8388, March 21, 2017.

descriptions of the elements in the XML Schema Definitions (XSDs) of these schemas are provided in Appendix B for ease of reference.

Section 6 provides an overview of the Emergency Incident Data Document (EIDD) standard developed and issued jointly by the Association of Public-Safety Communications Officials (APCO) International and NENA, and just approved in 2017 as a standard of the American National Standards Institute (ANSI). This standard is designed to support data exchanges about emergency incidents between a wide variety of next-generation public safety systems, including CAD systems and the mobile systems of PS/EM entities.

Section 7 provides an overview of the Keystone and Unified Incident Command and Decision Support (UICDS) middleware, which has been designed to support incident information sharing between PS/EM entities and incident responders, who may be operating on diverse systems using different data formats. It observes how Keystone's use of a common lingua franca based on widely used data standards, such as NIEM and OASIS EDXL, facilitates interoperability among diverse alerting and emergency management systems. The Keystone and UICDS service definitions serve to identify many of the data elements needed for the interoperation of such systems and their communications with PS/EM entities.

Section 8 concludes this paper with a brief summary of the standards reviewed and their relevance to PS/EM communications.

# 2. NIEM Emergency Management Domain

## A. NIEM Emergency Management Domain Overview

The NIEM Emergency Management (EM) Domain was developed to support information sharing related to emergency preparation, response, and management. Its goals include fostering information sharing that improves the abilities of users to prepare for, respond to, and recover from emergency situations. It is intended to promote interoperability between mission-based organizations focused on these goals at the federal, state, and local levels.[9] As such, it is very well aligned with the information sharing interests of PS/EM entities. The NIEM EM Domain Facilitator has estimated that 99% of the NIEM EM domain-specific data constructs support public safety and emergency management information sharing.[10] An overview of the prevalence of key terms used in the NIEM EM Domain is provided by the word cloud from its flyer shown in Figure 2-1.


**Figure 2-1. Emergency Management Domain Word Cloud**

---

9 NIEM Emergency Management (EM) Domain, *NIEM EM Domain Flyer*, downloaded January 2017 from: https://wss.apan.org/s/NIEMPMO/EM/Shared%20Documents/NIEM%20EM%20Domain%20Flyer.pdf

10 The Department of Homeland Security's (DHS) Science and Technology (S&T) First Responders Group (FRG) manages the NIEM EM Domain. The Director of DHS S&T FRG serves as the NIEM EM Domain Chair. The NIEM EM Domain Facilitator works for the Domain Chair to facilitate the management of the NIEM EM Domain. See the NIEM EM Domain home page for more information: https://www.niem.gov/communities/emergency-management.

The NIEM 3.2 EM Schema package[11] includes many related schemas from NIEM and external standards in order to reuse relevant existing standards and maximize information interoperability across multiple communities. The following indented hierarchy listing illustrates the structure of the schema folders in the NIEM 3.2 EM Schema package:

adapters

edxl-cap, edxl-de, edxl-have, geospatial

app-info

codes

ansi_d20, apco_event, atf, canada_post, cbrncl, census_commodity, census_uscounty, core_misc, dea_ctlsub, dod_jcs-purb2.0, doI_soc, dot_hazmat, edxl_have, edxl_rm, fbi_ncic, fbi_ndex, fbi_ucr, fips_5-2, fips_6-4, fips_10-4, hl7, iso_693-3, iso_3166-1, iso_4217, it_codes, mmucc, nga_datum, nga_genc, nlets, occs_facility, pmise_soar, unece_rec20, usps_states, xCard

conformanceTargets

domains

biometrics, cbrn, cyfs, emergencyManagement, immigration, infrasturctureProtection, intelligence, internationalTrade, jxdm, maritime, screening

external

cap, de, have, ogc, xml

localTerminology

niem-core

proxy

structures

Although all of these schemas are included in full in the NIEM 3.2 EM Schema package, only select types and elements from them are utilized by the NIEM EM domain exchange schema (emergencyManagement.xsd). The NIEM EM Domain Facilitator has identified the following code sets that are required by the NIEM EM Domain:

codes/iso_639-3/4.0/iso_639-3.xsd

codes/edxl_rm/4.0/edxl_rm.xsd

codes/edxl_have/4.0/have-codes.xsd

codes/apco_event/4.0/apco_event.xsd

---

[11] The NIEM 3.2 EM Schema appears to include all of NIEM 3.2. It can be downloaded from the NIEM Emergency Management Domain homepage on the All Partners Access Network (APAN) website at: https://wss.apan.org/s/NIEMPMO/EM/Shared%20Documents/NIEM%203.2%20EM%20Schema%2001252016%20(2).zip

The NIEM EM Domain Facilitator identified other attributes from the following schemas as required to support the elements used in the NIEM EM domain exchange schema:

adapters/edxl-cap/4.0/edxl-cap.xsd

internationalTrade/4.0/internationalTrade.xsd

niem-core/4.0/niem-core.xsd

screening/4.0/screening.xsd

jxdm/6.0/jxdm.xsd

biometrics/4.0/biom.xsd

However, IEPDs based on the NIEM EM domain may make use of elements/types (constructs) from any of the NIEM schemas (or others) if warranted for the type of information exchange specified by such an IEPD.

## B. NIEM Core

Given our focus on PS/EM communications requirements, only those NIEM Core types and elements that are used by the NIEM EM domain XSD (emergencyManagement.xsd) should be requirements from this domain for such communications. These NIEM Core constructs have been singled out by the Emergency Management Community of Interest as meeting their needs for information sharing. Other NIEM Core constructs may be useful in some PS/EM contexts, but they should not be required by practitioners in this domain.

## C. NIEM EM Namespace Data Types

The unique contributions of the NIEM EM Domain are specified using its NIEM EM namespace in the NIEM EM XSD (emergencyManagement.xsd). These contributions consist of definitions of types and of elements. The types can be grouped into categories based on the initial terms in their names, thanks to the NIEM naming and design rules that require a hierarchical structure in NIEM names. For example, we include the data types *AlarmEventType* and *AlarmPermitType* in the category of *Alarm* types. A listing of these categories provides an overview of the scope of the types of information covered by the NIEM EM Domain. Table 2-1 lists the general category names of the types defined in the NIEM EM XSD along with the number of types defined for each category.[12] For the *Alert* data type category, we separate out a subcategory *AlertEventDetails* because there is a substantial number (11) of types whose names begin with this prefix.

[12] Note that for simplicity, we count all NIEM EM types, although these include pairs of simple and plain types, which specify the same content; plain types allow additional attributes, while simple types do not.

**Table 2-1. NIEM EM Namespace Data Type Categories**

| Data Type Category | Number | Data Type Category | Number |
|---|---|---|---|
| AccessType | 1 | LiabilityType | 1 |
| Alarm | 6 | LicenseCertificationRegistrationType | 1 |
| Alert | 16 total | LocationAugmentationType | 1 |
| AlertEventDetails | 11 | Logical…Type | 2 |
| ApprovalStatusCode | 2 | Message | 6 |
| AvailabilityStatusCode | 2 | MissionInformationType | 1 |
| Badge | 2 | NISTSP800733PIVCardDataType | 1 |
| BarcodeCode | 3 | Notification | 12 |
| CheckInOut | 5 | OperationalStatus | 3 |
| CommentAugmentationType | 1 | Organization | 3 |
| ContactRoleCode | 3 | OwnerInformationType | 1 |
| Credential | 10 | PIVAssuranceLevelCode | 2 |
| CriteriaCategoryCode | 2 | PeerReviewType | 1 |
| DataLinkType | 1 | PermitType | 1 |
| Deployment | 4 | Person | 5 |
| EAssuranceLevelCode | 2 | PhysicalAccessLevelCode | 2 |
| EMMessage | 5 | PhysicalFitness | 3 |
| EMS | 2 | PointToPointLocationTrackingType | 1 |
| EOCRosterType | 1 | ProhibitiveDeploymentConditionType | 1 |
| EducationType | 1 | RecallCategoryCode | 2 |
| ElectronicAccessRight | 2 | RecommendationType | 2 |
| ElectronicAddressCategoryCodeType | 1 | RequestResourceInformationType | 1 |
| EmergencyDepartmentStatusType | 1 | Resource | 3 |
| EmergencySupportFunction | 2 | RosterType | 1 |
| ExerciseCategoryCode | 2 | ServiceCall | 4 |
| ExperienceType | 1 | Skill | 3 |
| ExplicitRecipientAddressType | 1 | StagingType | 1 |
| FIPS201ConformanceCode | 2 | TeamType | 1 |
| FirstResponder | 4 | TrainingType | 1 |
| GeneralNotificationType | 1 | TriagePatientCountType | 1 |
| Incident | 5 | Unit | 3 |
| Inquiry | 5 | UpdateRecordType | 1 |

| Data Type Category | Number | Data Type Category | Number |
|---|---|---|---|
| InsuranceAugmentationType | 1 | ValueType | 1 |
| JobTitleOrRoleType | 1 | WaiverType | 1 |
| LCRCategoryCode | 2 | | |

This listing reveals a focus in the NIEM EM Domain on alerts and notifications, which have the most XML types defined amongst the categories. It also shows substantial numbers of types defined for alarms, credentials, first responders, messages, EM messages, persons, deployments, and service calls.

## D. NIEM EM Namespace Data Elements

The NIEM EM Domain defines a large number of specific data elements, which typically represent properties of entities in this domain. Table 2-2 lists the general category names of groups of NIEM EM Domain data elements defined in the NIEM EM XSD, along with the number of elements defined within each category.[13] As with the NIEM EM Domain data types, the element categories are named with the shared initial terms in the element names.

**Table 2-2. NIEM EM Namespace Data Element Categories**

| Data Element Category | Number | Data Element Category | Number |
|---|---|---|---|
| Access | 3 | JobTitle | 5 |
| AdditionalCapacity | 2 | JurisdictionName | 1 |
| AdultGeneralServiceCoverageStatusCode | 1 | KeyHistoryObject | 1 |
| AgencySymbol | 1 | LCR | 4 |
| Alarm | 44 total | LaborDeliveryServiceCoverageStatusCode | 1 |
| AlarmEvent | 19 | LastExerciseTime | 1 |
| Alert | 33 total | Liability | 5 |
| AlertEventDetails | 18 | LicenseCertificationRegistration | 2 |
| AnesthesiaServiceCoverageStatusCode | 1 | Location | 3 |
| ApprovalStatusCode | 1 | Logical | 5 |
| Arrival | 2 | MemberOnlineIndicator | 1 |
| Author | 3 | Message | 10 |
| Availability | 3 | MetricCommentText | 1 |
| Badge | 11 | MinChildResourceClassQuantity | 1 |

[13] Note that for simplicity we count all NIEM EM elements, although some of them are abstract and will not appear in an actual XML message document.

| Data Element Category | Number | Data Element Category | Number |
|---|---|---|---|
| Barcode | 5 | Mission | 4 |
| BaselineQuantity | 1 | NISTSP800733PIVCardData | 2 |
| BinaryChecksumDigestID | 1 | NavigationInstructionsText | 1 |
| BurnServiceCoverageStatusCode | 1 | Notification | 24 |
| CallCategoryText | 6 | NotifierAugmentationPoint | 1 |
| CallerCategoryText | 1 | NotifierRole | 2 |
| Card | 3 | OperationalStatus | 3 |
| Cardholder | 4 | Organization | 10 |
| CardioThoracicServiceCoverageStatusCode | 1 | OriginatingMessageID | 1 |
| CardiologyServiceCoverageStatusCode | 1 | Owner | 4 |
| Category | 2 | OwningOrganization | 1 |
| CeilingMeasure | 1 | PIVAssuranceLevelCode | 1 |
| Cell | 2 | ParentIncident | 1 |
| CertificationIssuedIndicator | 1 | ParentOrganizationID | 1 |
| Certifications | 1 | PeerReview | 6 |
| CheckInOutCode | 7 | Permit | 4 |
| ChildIncident | 1 | Person | 12 |
| Commercial | 2 | PhysicalAccessLevelCode | 1 |
| Comparison | 2 | PhysicalFitness | 3 |
| Contact | 4 | PointToPointLocationTracking | 2 |
| Contributor | 1 | PrecedingMessageID | 1 |
| CoordinateDateTime | 1 | PrintedText | 1 |
| Course | 2 | ProhibitiveDeploymentCondition | 3 |
| CredentialClass | 16 | ProvidingOrganizationName | 1 |
| Credential  24 total | | Publication | 2 |
| Credentials | 1 | Qualification | 4 |
| Data | 7 total | Recall | 2 |
| DataLastVerifiedCommentText | 3 | Recommendation | 6 |
| DataLink | 4 | ReferenceInformation | 1 |
| DeclineReasonCode | 1 | RegistrationJurisdictionName | 1 |
| DegreeIssuingDate | 1 | ReimplantationServiceCoverageStatusCode | 1 |
| DeliveryMethodText | 1 | RelatedIncident | 1 |
| DepartureDateTime | 1 | ReportToLocation | 1 |

| Data Element Category | Number | Data Element Category | Number |
|---|---|---|---|
| Deployment | 16 | ReportingInstructionsText | 1 |
| DisasterDeclarationText | 1 | Request | 3 |
| DiscoveryObject | 1 | Resource | 32 |
| Doctor | 2 | ResponseLevelText | 1 |
| EAssuranceLevelCode | 1 | RestrictionCategoryText | 1 |
| EMMessage | 5 | RetiredX509CertificateForKeyManagement | 1 |
| EMS | 11 total | RoleDescriptionText | 1 |
| EMSOffload | 5 | Roster | 2 |
| EMSTraffic | 4 | RouteLocation | 1 |
| EOCPlanCode | 5 | RoutingInstructionsText | 1 |
| Education | 5 | SearchText | 1 |
| Electronic | 2 | SecurityObject | 1 |
| Emergency | 5 | ServiceCall | 7 |
| Exercise | 5 | SignatureAuthorityName | |
| Experience | 3 | Skill | 6 |
| ExplicitRecipient | 4 | SpinalServiceCoverageStatusCode | 1 |
| FIPS201ConformanceCode | 1 | StaffingCode | 1 |
| FireSeverityLevelText | 1 | Staging | 4 |
| FireboxName | 1 | Station | 1 |
| FirstResponder | 6 | Team | 5 |
| GeneralNotification | 2 | TemporaryIDIndicator | 1 |
| HandServiceCoverageStatusCode | 1 | Training | 3 |
| HomeDispatch | 1 | Triage | 5 |
| HomeUnit | 1 | URI | 1 |
| IDCategoryCode | 1 | UncertaintyDistanceText | 1 |
| Incident | 8 | Unit | 7 |
| IncludeHigherCapabilityResourceIndicator | 1 | Update | 3 |
| InfectiousDiseasesServiceCoverageStatusCode | 1 | Value | 4 |
| Inquiry | 4 | VolunteerIndicator | 1 |
| Insurance | 4 | Waiver | 4 |
| InventoryRefreshDateTime | 1 | X509CertificateFor | 4 |
| InvoiceImage | 1 | | |

## E. Other NIEM Domains

The NIEM 3.2 EM Schema package includes all of the other NIEM domain schemas, as listed above in Section 2.A. However, the NIEM EM XSD cites only select elements and types from these domains. Thus, not all of the content of all of these domains is required for PS/EM communications using the NIEM EM domain. The NIEM EM Domain Facilitator has identified the following NIEM domains as containing elements or types that are used in the EM Domain schema: Justice, International Trade, Screening, and Biometrics.

## F. External Standards

The NIEM 3.2 EM Schema package includes a wide range of external standards between the XSDs in its *external* folder and those in its *codes* and *adapters* folders, as listed above. These include standards from OASIS (EDXL), APCO, and the International Organization for Standardization (ISO). However, only the following external code schemas were identified as being used by the EM Domain schema:

codes/iso_639-3/4.0/iso_639-3.xsd

codes/edxl_rm/4.0/edxl_rm.xsd

codes/edxl_have/4.0/have-codes.xsd

codes/apco_event/4.0/apco_event.xsd

Other parts of external standards, which are included in the NIEM 3.2 EM packages, may be used in IEPDs based on the NIEM EM Domain.

# 3. Emergency Data Exchange Language

The Emergency Data Exchange Language (EDXL) specification developed by OASIS, is a composite standard made up of a group of related standards for information sharing messages based on XML. Other emergency management standards (e.g., NIEM EM) and systems use EDXL and its component standards, especially CAP, to define messages for information sharing. Here, we briefly review the scope of the component EDXL standards, whose details are readily accessible from OASIS.[14]

## A. EDXL-Distribution Element

The EDXL-Distribution Element (EDXL-DE) provides a type of container for sending emergency-related messages, such as alerts or resource messages. The basic structure and content of an instance of an EDXL-DE is illustrated by its object model in Figure 3-1. This shows the core data elements of an EDXL distribution containing a unique identifier and general metadata about the message sender, recipient, and intended distribution. These core data elements can then be augmented with zero to many instances of target areas and content objects. A target area can be specified via a geospatial circle, a polygon, or various location codes. Each content object can have a description, keywords, incident metadata, content originator, and consumer roles, as well as other metadata. A single content instance, which may be XML content or other mime type content, is included in each content object.

The EDXL-DE is designed to define a metadata container around content formulated using the other EDXL standards or other content types, such as text, image, audio, and video types.

[14] For links to the EDXL standards, see the OASIS Emergency Management Technical Committee website at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

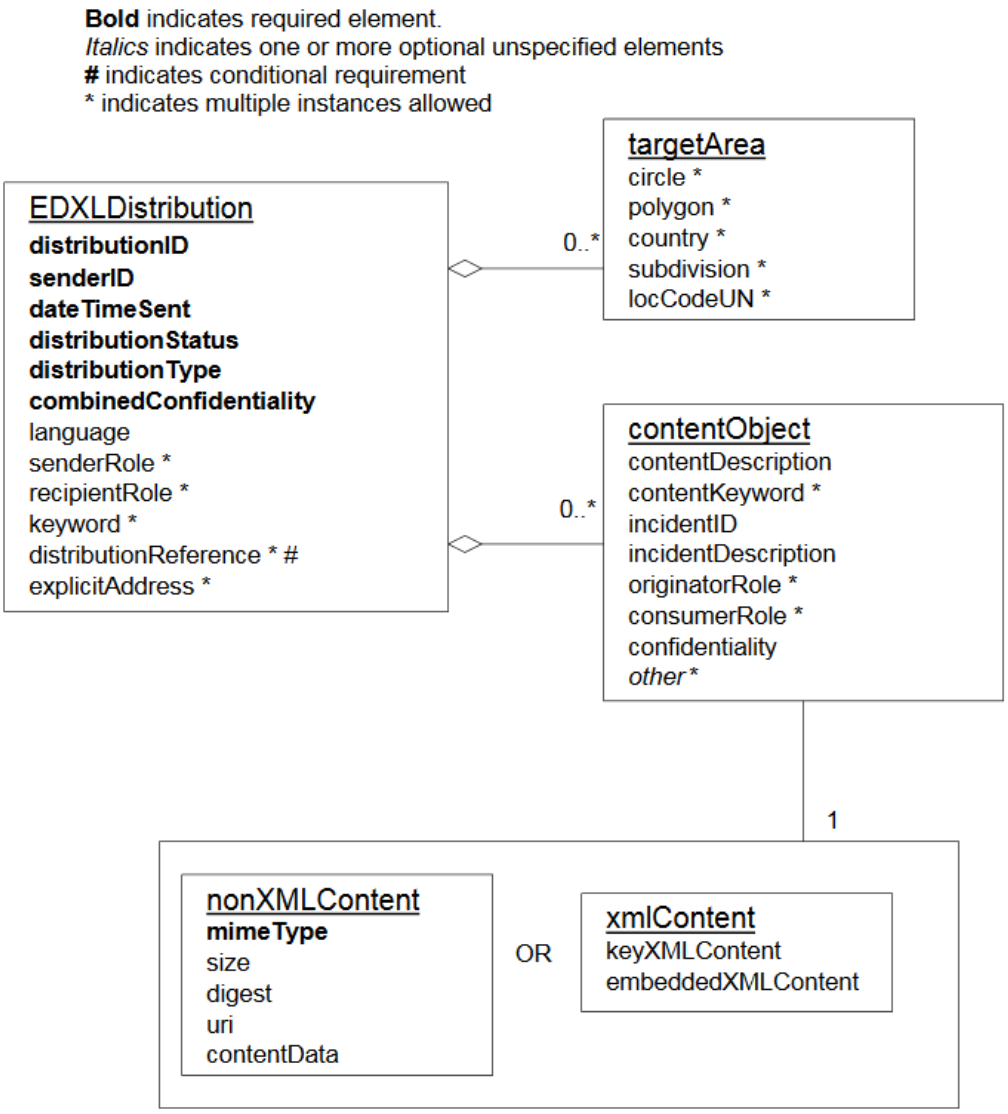


**Figure 3-1. EDXL Distribution Element Object Model**[15]

## B. EDXL-Resource Messaging

The EDXL-Resource Message (EDXL-RM) specification defines 16 separate and specific message types supporting the major communication requirements for allocation of resources across the emergency incident life-cycle. This includes preparedness, pre-staging of resources, initial and ongoing response, recovery, and demobilization/release of resources.[16]

---

[15] OASIS, *Emergency Data Exchange Language (EDXL) Distribution Element, v. 1.0* OASIS Standard EDXL-DE v1.0, 1 May 2006, p. 10.

[16] OASIS, *Emergency Data Exchange Language Resource Messaging (EDXL-RM) 1.0*, November 2008. Available at: http://docs.oasis-open.org/emergency/edxl-rm/v1.0/os/EDXL-RM-v1.0-OS.pdf

The principal entities and their relationships in EDXL-RM are illustrated in the Resource Messaging – Abstract Reference Model shown in Figure 3-2. This model shows the three main types of resource message – *Request*, *Response*, and *Report*. It shows how each resource message contains resource data. It can identify the parties that own the resource, the funding that is used to acquire or apply the resource, and the assignments and schedules for managing the resource.

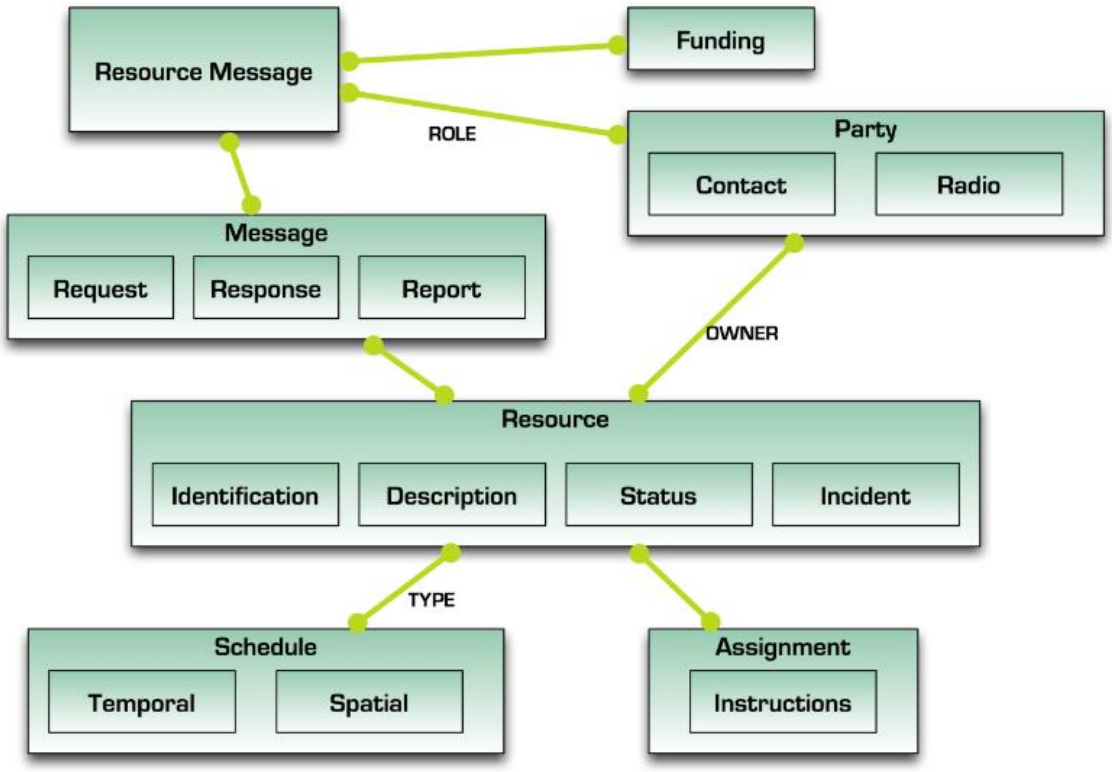


**Figure 3-2. Resource Messaging – Abstract Reference Model[17]**

## C. EDXL-Hospital AVailability Exchange

The EDXL-Hospital AVailability Exchange (EDXL-HAVE) is designed to support the exchange of information about available hospital services and resources, such as available hospital beds and burn units. This type of information can be critical for effective routing of victims of incidents by EMS. Like many EDXL messages, those using EDXL-HAVE are more likely to go to Emergency Operations Centers (EOCs) or dispatching operations than directly to field responders. The emergency management infrastructure requires such information for effective dispatching and coordination of incident responders themselves. An overview of the data requirements for EDXL-HAVE messages is provided by the EDXL-HAVE document object model shown in Figure 3-3.

[17] Ibid. p. 16.

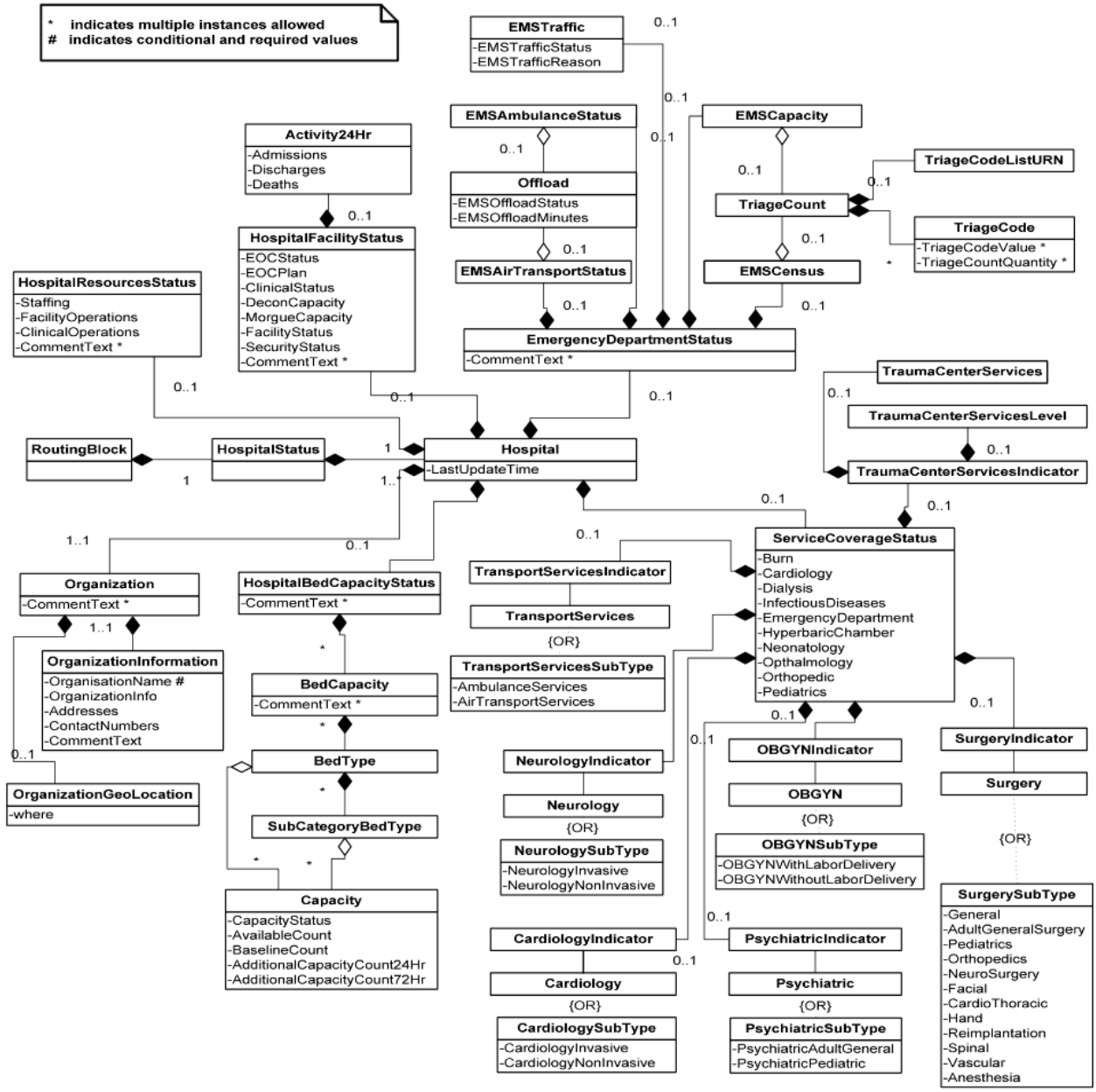


**Figure 3-3. EDXL-HAVE Document Object Model[18]**

The EDXL-HAVE document object model clearly shows the *Hospital* entity at the center of all the component entities that characterize different aspects of it and its available services and resources. The types of information carried by the sub-elements of *Hospital* are indicated by their names: *Organization*, *EmergencyDepartmentStatus*, *HospitalBedCapacityStatus*, *ServiceCoverageStatus*, *HospitalFacilityStatus*, *HospitalResourcesStatus*, and *LastUpdateTime*.

---

[18] *Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE)* Version 1.0 OASIS Standard, November 1, 2008, p. 10.

Further sub-elements of these are shown that capture properties of these elements, although not all their details are illustrated. See the extensive EDXL OASIS documentation for the complete data dictionary on this and other EDXL standards.[19]

## D. Common Alerting Protocol

The Common Alerting Protocol (CAP) was developed to provide a standard for sending and receiving alerts and notifications. CAP's history began in November 2000, when the National Science and Technology Council issued a report recommending that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems."[20] CAP version 1.0 was released in 2004. Changes based on user feedback were incorporated into version 1.1, which was released in 2005. The current version, 1.2, was released in 2008. CAP was then incorporated into the broader EDXL standard since it is obviously appropriate for providing alerts in emergency situations.

CAP is non-proprietary. It is platform-independent—it can be used to send messages from, route messages through, and deliver messages to, any digital device. Its objective is to eliminate the need for custom software interfaces devoted to warning sources and dissemination systems.

A CAP message is an XML document. Figure 3-4 shows its structure. The document contains an alert. An alert contains elements to identify itself; to supply metadata on the sender, the time the message was sent, the status (actual, exercise, etc.), the type (alert, update, etc.), and the scope (public, restricted, or private); and to provide the alert's information contents (info). The information content comprises textual descriptions, suitable for display on devices (these descriptions may be brief, suitable for receipt as text messages, or arbitrarily long); dates and times on when events related to the alert are slated to begin (or have begun) and end, and when the alert is to expire; and parameters intended for use by automated systems processing the message. The information also contains any number of two categories of elements: *area* and *resource*.

*Area* elements describe the geographical area in which an event occurs. An area can be given as a circle or polygon, or by using an application-specific coding system. It may be two- or three-dimensional. A *resource* is an entity of interest in describing an event. Typically, it is a file containing an image, audio, video, or some other content that cannot be represented as text. A *resource* can be a URL, if the receiving device is expected to have access to the Internet. Alternately, a *resource* can be embedded in the content of an alert message using base-64 encoding.

---

[19] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

[20] Working Group on Natural Disaster Information Systems Subcommittee on Natural Disaster Reduction, National Science and Technology Council Committee on Environment and Natural Resources, Nov. 2000, *Effective Disaster Warnings*. http://www.sdr.gov/docs/NDIS_rev_Oct27.pdf.

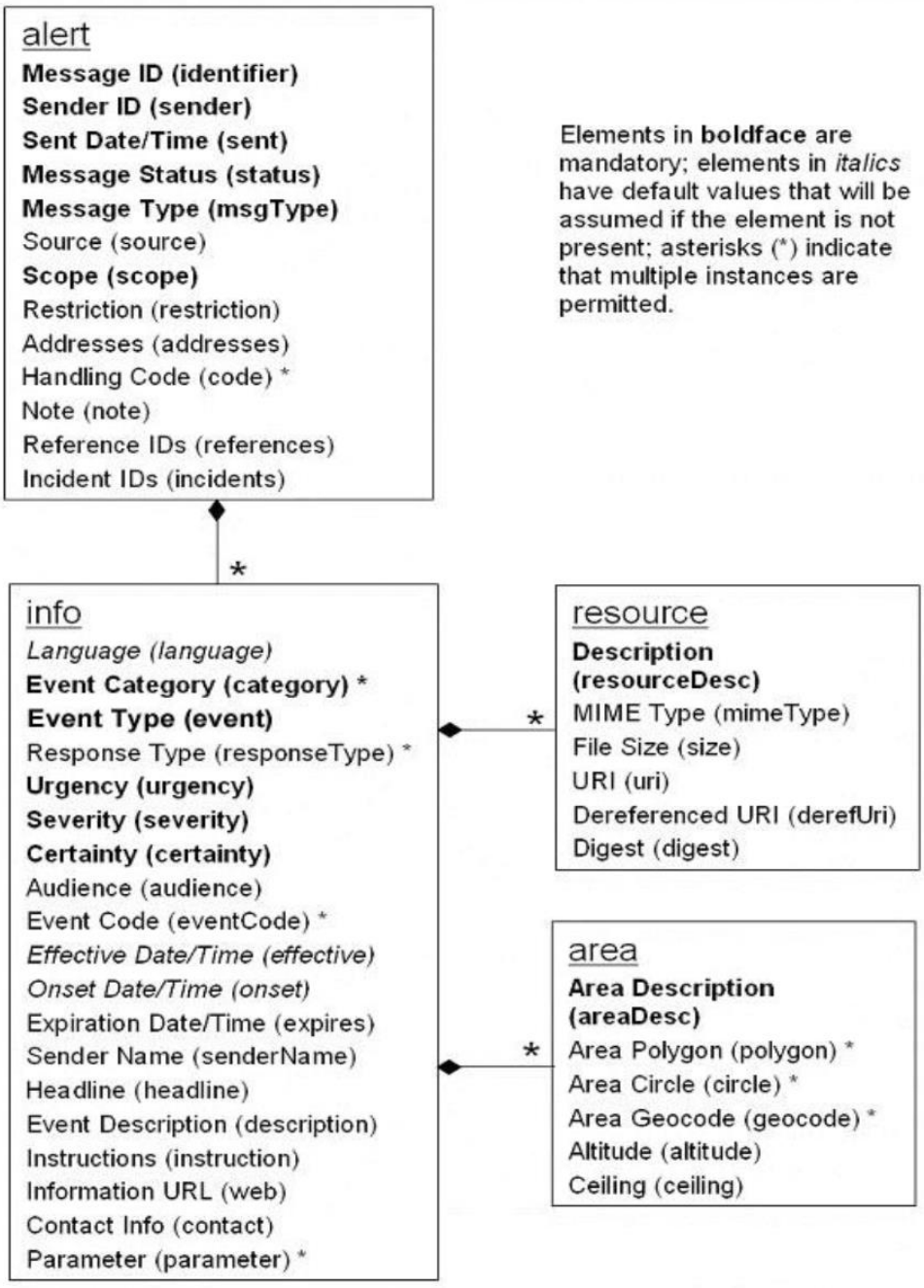


**Figure 3-4. CAP Alert Message Structure[21]**

[21] OASIS, *Common Alerting Protocol Version 1.2* OASIS Standard, July 1, 2010, p. 12. This version of the CAP document object model does not reflect one of the recently submitted changes, and it is still in the process of being updated by OASIS.

# 4. Computer-Aided Dispatch

This section provides an overview of Computer Aided Dispatch (CAD) data requirements. The CAD data requirements are derived from multiple documents that cover the general utilization of CAD systems instead of more formal documents, such as XML schemas associated with the valid messages that are exchanged, as is the case with the NENA data requirements presented in Section 5. Figure 4-1 highlights the fact that the information requirements covered by CAD systems encompass both the requirements that can be characterized as strictly for exchange between the PS/EM headquarters and the field responder units that deliver the services at the location where the incident is reported (the WHAT, WHERE, WHEN) and the requirements arising from the additional functionality of the CAD systems, such as the ability to generate map overlays for situational awareness, automatically converting street addresses into latitude and longitude data, integrating vehicle location and street maps to monitor response progress, and optimizing route generation to avoid traffic congestion spots and reduce travel time.

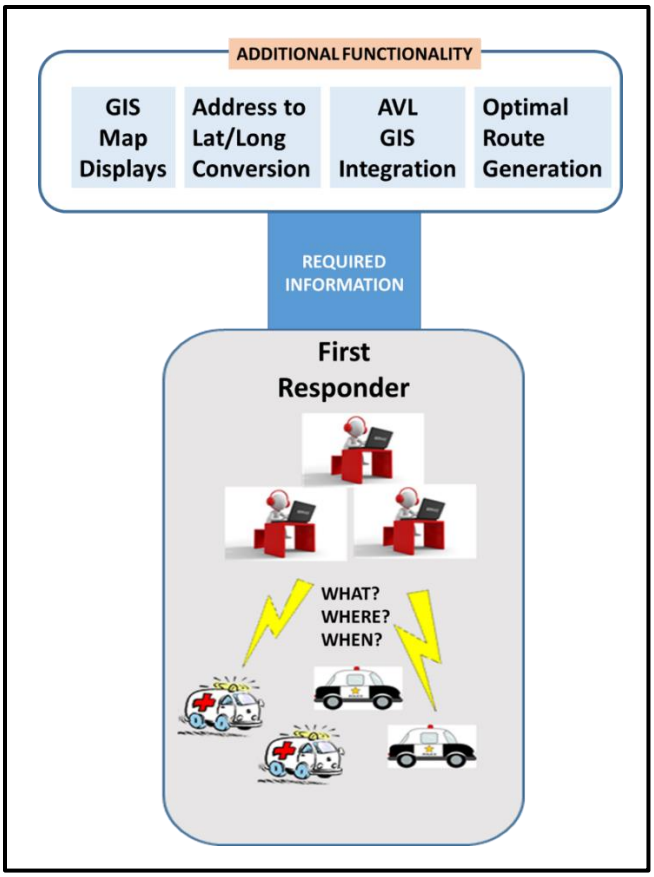


**Figure 4-1. Information Types Associated with CAD Systems**

The data requirements in Table 4-1 and Table 4-2 are described in tabular form. Each table contains three columns defined as follows:

- Element: A label for the element. The value in the column is human-readable text. It is not necessarily the value used by a specific CAD system, but the exemplar is meant to express the common semantics of the element.
- Type: The data type of the element. Because the data requirements are derived from descriptions of what a CAD message may contain, and the messages shown in the documents are essentially text, most of the data elements used in the exchanges are character strings.
- Description: A textual narrative describing the nature and purpose of the element.

Because the data elements have not been derived from an information model, or an XML schema specification, there is no way to ascertain at this stage in all cases whether an element is required or optional, or its cardinality.

## A. CAD Data Elements for Exchanges

General data requirements for CAD system exchanges between the emergency management headquarters and the units that deliver services are listed in Table 4-1.

**Table 4-1. CAD Data Elements for Exchanges**

| Element | Type | Description |
|---|---|---|
| **Location** | Text | The alpha-numeric character string that corresponds to the street address associated with the event. |
| **Reporting Party (RP)** | Text | The alpha-numeric character string that corresponds to the individual making the statement, together with street address and telephone number. |
| **Incident Type** | Text | The alpha-numeric string that corresponds to the kind of event being reported. In some cases, the CAD system may use codes rather than the full string, e.g., BURG rather than Burglary. For interoperability purposes, one should seriously consider standardizing these values. CAD system providers would be free to customize the display values, but the actual machine-to-machine values should be the standardized codes. |
| **Incident Description** | Text | A textual narrative that amplifies the nature of the event being reported, which may provide additional context concerning potential risks to the field responders, e.g., the number of people involved in the burglary, whether they appear to be armed, etc. |

## B. CAD Data Elements to Support System Functionality

As noted earlier, CAD systems also employ a number of additional data elements to provide specific functionality, but these elements are not necessarily exchanged between the emergency

dispatch station and the field responder vehicles (e.g., patrol cars, ambulances, etc.). For example, a state-of-the-art CAD system will contain a module that converts street addresses into either latitude and longitude values or a set of Universal Transverse Mercator coordinates that can be used to identify the closest service vehicle. These elements are not part of the exchange, but are used by the CAD system operators to generate new messages or to direct other messages to specific responder units (i.e., those closest to the incident and available). Several generic types of data elements, which are required to support such CAD system functionality, are identified in Table 4-2.

**Table 4-2. CAD Data Elements for System Functionality**

| Element | Type | Description |
|---|---|---|
| **Incident Identifier** | Integer | The numeric value that is assigned to a reported event and which serves to uniquely identify the event. |
| **Count of Units Available** | Integer | The numeric value that represents how many units are available as potential field responders for the event – it may be computer-generated by the CAD system based on the value entered by the call-taker for the Location data element, which then computes the proximity of the field responders to the event. |
| **Count of Units Not Available** | Integer | The numeric value that represents how many units are not available – it may be computer-generated by the CAD system based on the value entered by the call-taker for the Location data element, and whether the unit is already engaged in another incident and therefore cannot be tasked to respond to the event reported. |
| **Automatic Vehicle Location (AVL)/ Global Positioning System (GPS)/ Events Activated Tracking Systems (EATS)** | Decimal | The latitude and longitude values generated by GPS devices mounted on the vehicles, which are polled at specified intervals. In modern CAD systems, the data fed by AVL is then post-processed to compute proximity of the units to the reported event. EATS may not be specifically needed to provide a response to an incident, but it may be added to the mix as a security measure to ensure availability of high-value equipment in combination with anti-theft protection. The interoperability challenge here is to get all participants to use the same datum or coordinate system as the baseline and to standardize the conversion between the various alternatives. |
| **Beat/Zone Map Code** | Text | The alpha-numeric character string assigned to a zone within a map grid or map overlay that can be used to locate the reported event. This appears to be an older approach whose main advantage may be the simplification of other calculations related to event proximity. |
| **Geographic Information System (GIS)/AVL Integration Metadata** | Text | This is a complex set of individual data elements that capture metadata associated with streets that incident responders may need to use to reach the location of the event reported. They include Left/Right Turn Allowed at each intersection, Turn Difficulty Score to rate how easily certain types of vehicle (e.g., hook and ladder trucks) can turn at a given intersection, One-Way/Two-Way Traffic Flag for each segment in the street grid, Heavy Traffic Score to signal whether the route should avoid the segment due to congestion. Standardization of the algorithms used to compute optimal routes would facilitate the adoption of the GIS/AVL integration solutions. |

## C. Related Data Standards

In addition to the general data requirements identified for CAD systems, a number of other data standards are designed to support communications between them and 9-1-1 public safety systems. The data standards developed by NENA are used in communicating automatic location information from telecommunications provider 9-1-1 systems to CAD systems. Overviews of these standards are provided in Section 5. The NENA data standards described in Section 5 appear to apply only to internal communications between functional elements of 9-1-1 systems and CAD systems. As such, they are not focused on direct information exchanges with PS/EM personnel, although they are essential to getting 9-1-1 automatic location information to CAD systems that share the information with field responders.

In addition to the NENA data standards for internal communications of 9-1-1 systems, NENA has engaged with APCO International in developing a data standard for exchanging emergency incident data. The resulting Emergency Incident Data Document (EIDD) standard supports the exchange of emergency incident data between CAD systems, and ultimately to PS/EM entities on mobile systems. See Section 6 of this report for an overview of this EIDD standard.

# 5. National Emergency Number Association Exchanges

The National Emergency Number Association (NENA) is an organization dedicated to "[improving] 9-1-1 through research, standards development, training, education, outreach, and advocacy."[22] One outcome of NENA's standards development activities has been the production of XML schemas for communicating messages to, from, and among professionals and systems involved in 9-1-1 communications. The current set of NENA schemas (version 4.3.1) was published on January 22, 2012.[23]

NENA was created in 1982, long before the widespread use of wireless communications devices, before XML, and before the digital transmission of telephone-initiated information over the Internet. Its standards are continuously evolving in response to new technologies and consumer trends (e.g., the use of social media to report emergencies). NENA is currently producing XML schemas for next-generation 9-1-1 communications.

NENA standards describe many concepts applicable to both civilian and military PS/EM situations. These standards tend to focus more on system-level concerns than operational-level matters. For example, NENA's Automatic Location Information (ALI) standard describes information to be transmitted automatically during a 9-1-1 call to help a PSAP operator pinpoint the caller's location; NENA also specifies how to use a service that translates a geolocation into a street address, or vice versa. Both these actions can be initiated without human involvement. The PSAP operator sees only the results.

Civilian and military PS/EM entities may need to exchange information during emergency events. In 2015, the Secretary of Defense issued a memorandum ordering cooperation with local law enforcement offices.[24] U.S. Northern Command (NORTHCOM) executed a pilot program in which a civilian 9-1-1 operator notifies the North America Aerospace Defense Command (NORAD) – USNORTHCOM Current Operations Center (N2C2) in certain emergency circumstances, such as one in which a caller states that he or she wants to take violent action

---

22 http://www.nena.org/?page=Mission

23 http://www.nena.org/?page=XML_Schemas

24 DoD, "Force Protection Efforts Following the Chattanooga Attacks," Secretary of Defense Memo, OSD 010319-15CMDO13583-15, October 2, 2015. See https://meetings.nga.org/files/live/sites/meetings/files/resources/CoG/151002DoDMemoSecurityMilitaryInstallations.pdf

towards military personnel.[25] Conversely, a military base will want to notify civilian emergency management personnel in the event of an on-base chemical, biological, radiological, nuclear (CBRN) event that cannot be contained. Because over 98% of PSAPs implement at least some NENA capabilities,[26] military systems that communicate with PSAPs need to handle NENA-conformant data elements.

This section provides an overview of National Emergency Number Association (NENA) data requirements. It is divided into sections corresponding to the categories of schemas in the current NENA distribution. Each section contains one or more subsections. Each subsection focuses on a single schema (although that schema often references, through import or inclusion, other schemas). These subsections describe the types of data required by their schemas. Detailed descriptions of the elements in the XSDs of these schemas are provided in Appendix B for ease of reference. These elements may be part of an XML document transmitting NENA-related information. The structure of these sets of elements is as follows:

Automatic Location Information (ALI)

ALI Information – street address, geolocation

Master Street Address Guide (MSAG) – database with locations by telephone numbers

Service Order (SO) – location at which the service is to occur

ALI Query Service (AQS) – new protocols between a PSAP and the Next Generation Emergency Services Network (NGESN)

Geographic Information System (GIS) – ways to describe geographic features

Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)

Presence Information Data Format (PIDF) – ability and willingness of an entity to communicate

Emergency Routing Database (ERDB) – database of Emergency Service Zones

VoIP Positioning Center to/from Emergency Services Routing (V2)

Location Information Server to/from VoIP Positioning Center (V3)

Validation Database Interface (V7) – for validating addresses

VoIP Positioning Center to/from Emergency Routing Databases (V8)

Request/Response on Database for Location of the Sender (V9)

NextGen (i3) – Next-generation 9-1-1 Communications Standards (NG9-1-1)

Data With Call – data provided with call

---

[25] USNORTHCOM J34 Homeland Defense and Protection Division, *Draft U.S. Northern Command Enterprise Mass Warning and Notification (EMWN) Concept of Operations (CONOPS)*, November 2016.

[26] http://www.nena.org/?page=911Statistics

Discrepancy Reporting – maintain and query discrepancy reports

Emergency Call Routing Function (ECRF) Messages

Logging Services

Policy Store

Spatial Information Function (SIF)

## A. Automatic Location Information

NENA has several schemas that describe standards for messages involving automatic location information. Automatic Location Information refers to the information transmitted based on information generated by an Automatic Location Identification (ALI) system.[27] Such a system automatically transmits a caller's address whenever the caller calls 9-1-1 (or any other compatible emergency responder service). The location may be transmitted as a postal address, especially if the call is made from a land line (telephone companies maintain databases of addresses that ALI systems can access), or as a geolocation of a cellular device.

The primary schema, described in the first subsection, deals specifically with ALI. Other schemas provide support. Only one, described in Section 5.A.2, contains high-level concepts. The others are type libraries and are considered too low level to be discussed in this paper.

### 1. Automatic Location Information Main Schema

A message containing ALI includes components describing the location of a call. Location may be given as a street address, according to the Master Street Address Guide (MSAG), discussed in Section 5.A.2; as a geolocation; as a cell site; or as a combination of these elements.

ALI may also include information on agencies near the location, on the caller and the calling number, on the 9-1-1 network through which a call is being routed, and on the sources used to collect the data in an ALI message.

### 2. Master Street Address Guide

The Master Street Address Guide (MSAG) is a database populated with locations keyed by telephone numbers. A record includes a street name, along with sufficient identifying information to disambiguate that street from other similar or identically named streets. It further includes house numbers, although these are not necessarily given as single numbers but as ranges.

---

[27] See https://www.techopedia.com/definition/2925/automatic-location-identification-ali. Both Automatic Location Identification and Automatic Location Information use the acronym ALI. In the context of NENA, ALI refers to Automatic Location Information.

## B. Service Order

A NENA service order (SO) record describes the location at which the service is to occur. Location is given as a street address, geolocation, or cell tower site. It is also given in terms of the customer receiving the service. Information on the customer includes the customer's name and telephone number, as well as the nature of the telephone call and descriptions of the kind of service requested.

## C. ALI Query Service

The ALI Query Service (AQS) specifies new protocols between a PSAP and the Next Generation Emergency Services Network (NGESN). It overcomes certain ALI limitations.[28] The specification includes Web Service Description Language (WSDL) descriptions of the query operations AQS supports.

The ALI Query Service is provided as a Standard Preview Release. This means it is still a draft standard that remains a work in progress and is subject to change.

The ALI Query Service's elements are defined in a single XML schema that lays out the syntaxes of an AQS query and the response to that query. The schema also provides for an advisory message. The query may be an advisory request, in which case the response will be an advisory.

## D. Geographic Information System

A Geographic Information System (GIS) is a computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a street address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It also can be used to graphically display coordinates on a map, i.e., latitude/longitude from a wireless 9-1-1 call.

NENA provides a single schema related to Geographic Information Systems—the NENA GISsfProfile. It is an extension to the Geographical Markup Language (GML) XML schema. It provides ways to describe geographic features that are pertinent to 9-1-1-related messages.

## E. Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)

NENA has released evolving versions of standards. One, released in 2006, is known as the Interim VoIP Architecture for Enhanced 9-1-1 Services; it is also known as i2. NENA's i3 services represent next-generation services; these are covered in section 5.K, below.

---

[28] ALI schema limitations include a data limit of 511 characters. For more details, see *NENA ALI Query Service Standard,* Sections 1 and 2.1. This document is included in the NENA schemas distribution, in file aqs/doc/DocSet/ NENA AQS Draft 1.3.docx

### 1. Presence Information Data Format

Presence information describes the ability and willingness of an entity to communicate. NENA supports Internet Engineering Task Force RFC 4481, *Timed Presence Extensions to the Presence Information Data Format (PIDF) to Indicate Status Information for Past and Future Time Intervals.* [29]

### 2. Emergency Routing Database

The Emergency Routing Database (ERDB) is a database of Emergency Service Zones in a service area, along with routing information among those zones. Zones are defined in terms of geographic boundaries. The NENA ERDB XML schema specifies messages that may be used to communicate and update those boundaries.

## F. VoIP Positioning Center to/from Emergency Services Routing (V2)

The V2 schema defines messages sent across the V2 interface to a VoIP Positioning Center (VPC). These messages are for Emergency Services Routing (ESR). The V2 schema defines request and response messages. A request specifies the source, target, and caller. A response includes the request information, along with routing information.

## G. Location Information Server to/from VoIP Positioning Center (V3)

The V3 schema defines messages sent across the V3 interface between a Location Information Server (LIS) and a VoIP Positioning Center (VPC). It is deprecated, so it is not further described in this document.

## H. Validation Database Interface (V7)

The V7 schema defines messages sent across the V7 interface to a Validation Database (VDB). These messages concern address validation. A service may request address validation by street address. In response, it receives information on addresses matching that request.

## I. VoIP Positioning Center to/from Emergency Routing Databases (V8)

The V8 schema defines messages that are sent across the V8 interface to a VPC. These messages concern Emergency Routing Databases (ERDBs). A request may be made to receive routing information from an ERDB, based on geographic coordinates, civic location, or both. The response message contains routing information from the ERDB.

---

[29] https://tools.ietf.org/html/rfc4481

## J. Request/Response on Database for Location of the Sender (V9)

The V9 schema defines messages that are sent across the V9 interface to determine which Validation Database (VDB) or Emergency Routing Database (ERDB) to query. A system may send an identity request message, and it will receive an identity response message in reply. The identity request message specifies whether to query VDB or ERDB locations and the location of the sender. The response message contains addresses (as URIs) of VDBs or ERDBs appropriate to the sender's location.

## K. NextGen (i3)

NextGen is, as the name implies, NENA's effort to promote next-generation 9-1-1 communications standards, often referred to as NG9-1-1. It has several high-level schemas (collectively known as i3), covered in the following subsections that encapsulate query-response communications (request-response, in NENA parlance). The NENA distribution also includes Web Services Description Language (WSDL) specifications of the requests and responses.

The NextGen area also contains schemas with elements used in the high-level schemas. These schemas provide the details of acceptable addresses, geolocations, and the like. It seems sufficient to note that NextGen requires address and geolocation data elements without deep exploration of their precise syntax (at least for now). These common schemas are not described below.

### 1. Data With Call

The Data With Call schema specifies the data that is associated with a 9-1-1 call. This data includes information on the device making the call, the URL of the caller (if known), and whether the call is from a business or residence. Information about the caller is provided in the standard vCard format.[30]

### 2. Discrepancy Reporting

The Discrepancy Reporting schema defines messages to maintain and query discrepancy reports. There must be a discrepancy report (DR) function to notify agencies and services (including Border Control Function (BCF), Emergency Services Routing Proxy (ESRP), ECRF, Policy Store, and Location Validation Function (LVF)) when any discrepancy is found. The discrepancy reporting audience is anyone who is using the data and finds a problem. Discrepancy reporting data elements in NENA are structured into two query-response formats. One deals with querying discrepancies and receiving reports in response. The other deals with requesting reports on discrepancy resolutions.

---

[30] IETF RFC 6350, *vCard Format Specification.* Available at https://tools.ietf.org/html/rfc6350

### 3. Emergency Call Routing Function Messages

The Emergency Call Routing Function (ECRF) must report 9-1-1 service area gaps and overlaps larger than a provisioned threshold. Gaps or overlaps exceeding standard threshold parameters defined in NENA 08-003[31] must result in a notification from an ECRF. To do so, the ECRF makes uses of the GapOverlap event. All 9-1-1 authorities who provide source GIS data to an ECRF must subscribe to its GapOverlap event. The event notifies both agencies when it receives data that shows a gap or overlap larger than the threshold. The notification includes the layer(s) where the gap/overlap occurs, whether it is a gap or an overlap, and a polygon that represents the gap or overlap area.

### 4. Emergency Services Routing Proxy Messages

The Emergency Services Routing Proxy (ESRP) assists in routing 9-1-1 messages. The ESRP schema defines messages used by the ESRP. These messages have to do with registering an entity as a dequeuing entity, along with the ESRP managing the queue.

### 5. Logging Services

NENA includes a logging capability to keep track of 9-1-1 messages and events. Each log entry includes a timestamp, information about the agency that logged an event, and technical details of the 9-1-1 call. The Logging Services schema defines messages for logging services.

### 6. Policy Store

NENA maintains a common policy store from which policies can be retrieved. The Policy Store XML schema defines messages to add, maintain, and query policies. Policies are transmitted as Base 64-encoded strings. Policies may be arbitrarily long. To send or receive a large policy, messages can split the policy into "chunks" of a maximum size negotiated by the sender and receiver, then transmit multiple messages, each with a single chunk.

### 7. Spatial Information Function

The Spatial Information Function (SIF) is the base database for NG9-1-1. Nearly all location-related data is ultimately derived from the SIF. If a datum is somehow associated with location, the base data will reside in the SIF.

SIF-related messages are request-response pairs. A system may submit a request to convert from a presence (see Section 5.E.1) specified as a geolocation to a presence specified as a civic address, or vice-versa. A system may also submit a request to convert between MSAG and

---

[31] *NENA Detailed Functional and Interface Specification for the NENA i3 Solution—Stage 3* (i3), 08-003, Version 1, June 14, 2011. (Version 2 DRAFT NENA-STA-010, June 9, 2015 pending).

presence formats. MSAG, an older format than PIDF, is being used less in next-generation systems.[32]

[32] See *Understanding NENA's i3 Architecture Standard for NG9-1-1.* Available at http://www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/08-003_Detailed_Functional_and_Interface_Specification_for_the_NENA_i3_Solution.pdf

# 6. Emergency Incident Data Document

The Association of Public-Safety Communications Officials (APCO) International and NENA have jointly developed and issued a data standard to support exchanging emergency incident-related information, identified as *APCO/NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD).*[33] This standard is designed to support data exchanges about emergency incidents between a wide variety of next-generation public safety systems, including Customer Premise Equipment (CPE), CAD systems, Records Management Systems (RMS), and the mobile systems of public safety and emergency responders. The EIDD standard supports sharing incident information updates and emergency-responder status reports, as well as the initial incident information content of a 9-1-1 call.

This EIDD has been formulated as a NIEM-compliant IEPD.[34] The EIDD exchange schema, which specifies the format of an EIDD-compliant message, is contained in the EmergencyIncidentDataDocument.xsd file. It declares just one data element (*EmergencyIncidentDataDocument*) and imports the schema EIDD.xsd to define it. EIDD.xsd defines the structure of a message in terms of required and optional data elements, and it imports other required NIEM schemas and external schemas. The principal NIEM schemas used by EIDD are the NIEM Core, select associated code lists, and the NIEM Justice Domain. Most of the imported external schemas are standards from the Internet Engineering Task Force (IETF) defining data elements for emergency calls.

An overview of the structure of the information content supported by an EIDD-compliant XML message is provided by the illustration in Figure 6-1. The EIDD Header captures general metadata about the document, including required data for a unique ID and the agent and agency that created the document. The Split/Merge Information components identify how a given incident may be merged with another or split into multiple incidents. The Link Information component supports tracking links between related, although separate, incidents. Incident Information includes incident type code as well as an incident type textual description, along with data on status, timestamps, reporting agent, involved persons and vehicles, priorities, beat/dispatch group,

[33] Extensive documentation of the EIDD standard, including its data dictionary can found in its master document at: https://www.apcointl.org/doc/911-resources/apco-standards/694-apco-nena-2-105-1-2017-ng9-1-1-emergency-incident-data-document-eidd/file.html

[34] The complete package of NIEM-compliant schemas for the EIDD can be downloaded from: https://www.apcointl.org/doc/911-resources/apco-standards/697-iepd-for-ng9-1-1-emergency-incident-data-document.html

and disposition information. Call Information is an optional component that can capture information for multiple callers, including radio calls, for the same incident.

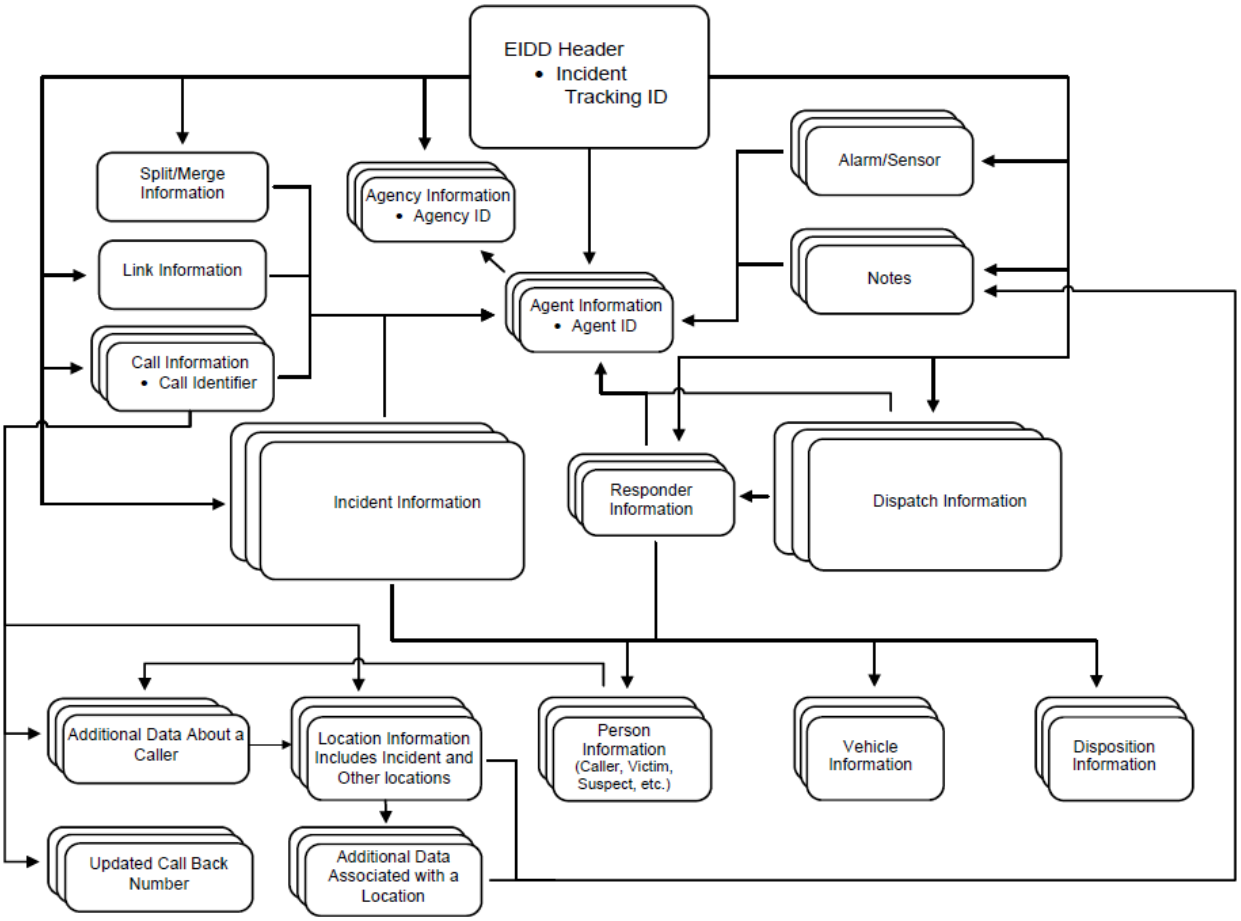


**Figure 6-1. Logical Organization of EIDD Data Components[35]**

The Dispatch Information component identifies the agency and the agent who completed a dispatch operation, as well as information about the emergency responders dispatched to the incident. The Disposition Information component supports optional standardized disposition codes (e.g., for false alarms, closed incidents) that can be assigned to an incident. The Person Information component supports specifying the role of a person in an incident along with detailed data about the person, using attributes taken from the NIEM Core Person entity. The Vehicle Information component supports specifying the relationship of a vehicle to an incident, along with detailed data about the vehicle, using attributes taken from the NIEM Core Vehicle entity. The Location Information component includes a code for location type, along with numerous data elements for representing locations in different ways, including geodetic, civic, and descriptive text elements.

---

[35] *APCO/NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD),* p. 16.

The Emergency Resource component supports identification of a responder for an incident. Responders in this element can be persons, vehicles, or organizational units. The composition of organizational units is also supported by this component. Other EIDD components and data elements are thoroughly documented in its master document, cited above.

# 7. Keystone/UICDS Exchanges

## A. Keystone Architecture

Keystone is middleware[36] designed to support incident information sharing amongst PS/EM personnel, who may be operating on diverse systems using different data formats. It adapts and extends, for DoD applications, an information-sharing system previously developed by DHS called the Unified Incident Command and Decision Support (UICDS) System. Keystone, like UICDS, uses "adapters" (a type of Application Program Interface (API)) to translate data into and out of a common internal NIEM-compliant format. Once ingested into a Keystone Core, messages can then be transformed into formats compatible with any other system for which a Keystone adapter has been developed. Keystone adapters are available for a wide variety of existing emergency management and mass warning and notification systems, including the following:[37]

- *AtHoc Alerts* – commercial bi-directional mass notification system operational in three Services, the Joint Staff, the National Guard, and many Federal agencies and universities.
- *Command, Control, Communications, Computers and Intelligence Suite (C4I Suite)* – a SharePoint and web-based application used for situational awareness of Navy installations.
- *ICD-0101B (prototype)* – providing sensor data input to Keystone for the U.S. Army.
- *Installation Protection Integration Platform (IP2)* – emergency response and information management system used by Department of Defense components.
- Non-Secure Internet Protocol Router–Situational Awareness Geospatial Enterprise (NIPR-SAGE) – used by USNORTHCOM and its mission partners.
- *WebEOC* – commercial web-based incident/event management system used by federal, state, county, and city entities.

All of the cited Keystone adapters have been used in the Mission Assurance, Threat Alert, Disaster Resiliency, and Response (MATADRR) initiative for enhanced information sharing by

[36] Middleware, such as this, is software that operates between other software systems, accessed from them via APIs.

[37] For more information on these systems, see: *A Survey of Mass Warning and Notification Systems,* IDA Document D-8388, March 21, 2017.

USNORTHCOM.[38] The Keystone architecture used in the MATADRR initiative, shown in Figure 7-1, illustrates the use of multiple communicating Keystone Cores to partition a space of partners engaged in common information-sharing missions. Keystone adapters can reside on the Mule Enterprise Service Bus (ESB) shown, which provides support for messaging reliability, security, performance, and translation to and from standard formats, such as CAP and NIEM. New adapters can easily be added using the Keystone Software Development Kit (SDK).[39]

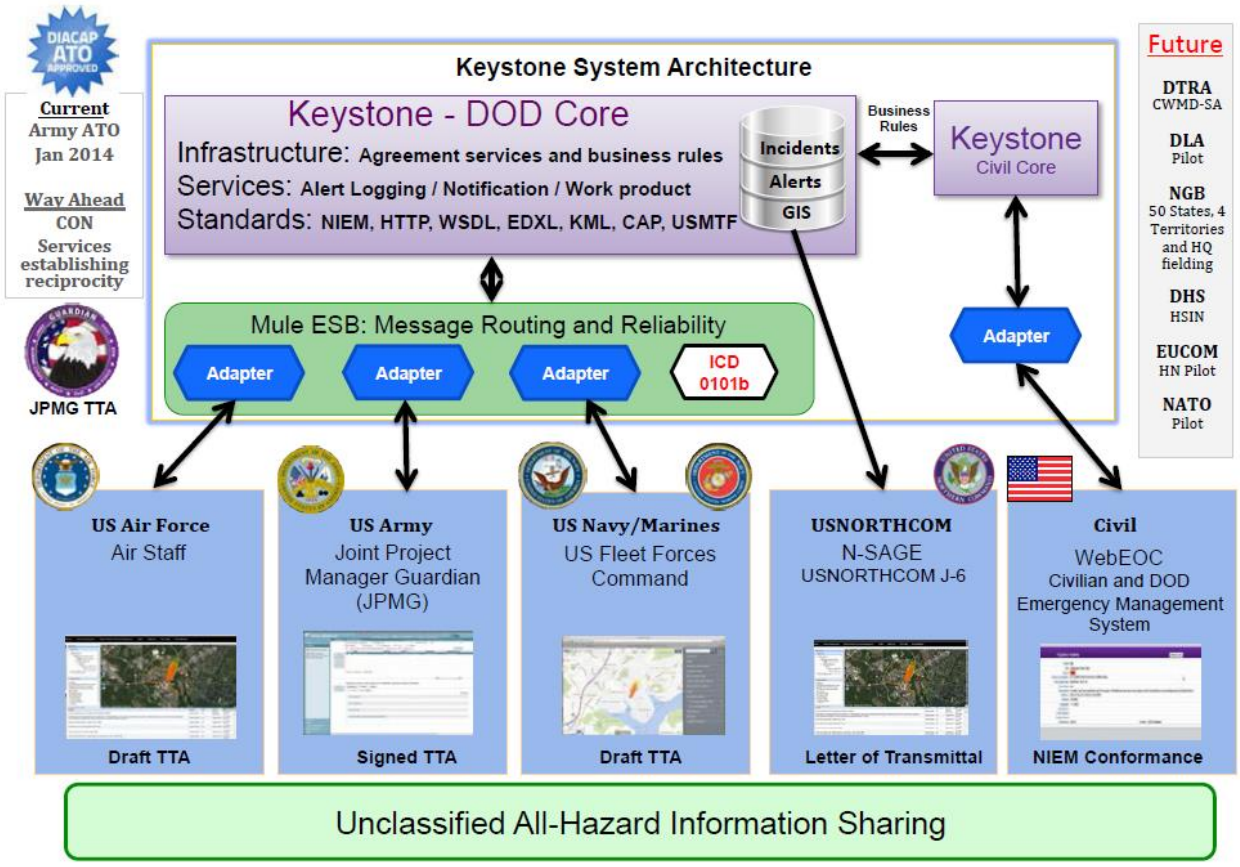


**Figure 7-1. Keystone Architecture for MATADRR Initiative**

The illustration shows two Keystone Cores, one for DoD and one for civilian partners. This division supports control over information sharing between cores by a set of business rule policies. Access to shared information can be controlled, not only by which Core a participant accesses, but also by user ID, software systems, incident type, proximity (radius of latitude and longitude of the system), certainty, urgency, base location, and severity of an incident. Sources providing

---

[38] Space and Naval Warfare Systems Center Pacific, *Mission Assurance, Threat Alert, Disaster Resiliency and Response (MATADRR) Product Reference Guide*, June 2014. Downloaded from: www.dtic.mil/get-tr-doc/pdf?AD=ADA608435

[39] Ibid., p. 5.

information through Keystone have control over sharing of their information using policies formulated with these criteria.

In addition to its use in the MATADRR initiative, Keystone has been used in a major U.S. European Command (USEUCOM) pilot activity,[40] and it is being evaluated and prototyped for use by the South Carolina National Guard and the National Guard Bureau.

Keystone's use of a common lingua franca, based on established data standards, facilitates interoperability with any emergency management or notification system through the development of a single suitable adapter. Without such a common representation, each new type of system in a network would need interfaces developed for all other systems in the network, resulting in an N-squared problem, wherein N systems would require $N^2$ number of interfaces. Keystone's XML exchange schemas provide excellent examples of data elements drawn from established standards, such as NIEM and the OASIS EDXL, which can be considered essential for a wide range of communications amongst PS/EM entities.

## B. Keystone Data Standards

Keystone inherits most of its XSD data exchange specifications from UICDS. These specifications are defined as services using the Web Service Definition Language (WSDL), an XML format for describing services that operate on messages exchanged between endpoints. [41] These services, in turn, use data elements defined using XSDs, many of whose data elements are adopted directly from existing data standards. Keystone services are divided into two classes: Infrastructure Services and Emergency Management Services. The Infrastructure Services support the management of information sharing between Keystone cores. The Emergency Management Services, listed in Table 7-1, deal directly with information content about incidents, including alerts, commands, tasking, and resource management. These are the services that contain data elements with content that is most directly relevant to PS/EM entities.

---

[40] Space and Naval Warfare Systems Center Pacific, *EUCOM Keystone: Connecting Across Services Enabling Timely Horizontal & Vertical Integration, Product Reference Guide, Revision 1*, September 2015. Downloaded from: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA627445

[41] See https://www.w3.org/2002/ws/desc/.

**Table 7-1. Keystone (UICDS) Emergency Management Services[42]**

| Service | Description |
|---|---|
| **AlertServiceEndpoint** | The Alert service allows UICDS compatible clients to create, cancel and get CAP alert work products that conform to the CAP version 1.1 specification. |
| **BroadcastServiceEndpoint** | The Broadcast Service provides a mechanism to send messages to a set of selected UICDS resource instances or eXtensible Messaging and Presence Protocol (XMPP) users. |
| **IAPServiceEndpoint** | The Incident Action Plan (IAP) Service allows UICDS compatible clients to manage an IAP and the related Incident Command Structures (ICS) form work products that are associated with a UICDS incident. |
| **IncidentCommandServiceEndpoint** | The UICDS Incident Command Service allows clients to create and modify command structures for incidents (including both ICS and Multi-Agency Coordination Systems (MACS)) and associate resources to organizational roles within these structures. |
| **IncidentManagementServiceEndpoint** | The Incident Management Service allows clients to manage UICDS incidents. |
| **LEITSCServiceEndpoint** | The UICDS Law Enforcement Information Technology Standards Council (LEITSC) Service allows clients to create, update, close, and archive UICDS incidents based on LEITSC Detailed Call For Service messages. |
| **MapServiceEndpoint** | The UICDS Map Service provides a means for interacting with an UICDS core to manage map related resources. |
| **ResourceManagementServiceEndpoint** | The Resource Management Service provides UICDS clients with services to exchange EDXL-RM messages with other UICDS clients and send EDXL-RM messages to XMPP users. |
| **SensorServiceEndpoint** | The UICDS Sensor Service allows clients to manage Open Geospatial Consortium Sensor Observation Specification (OGC-SOS) GetObservation and Observation work products. |
| **TaskingServiceEndpoint** | The Tasking Service allows a client to create, update, query and delete a list of tasks for a resource. |

Each of the Service definitions has precisely defined required and optional data elements, which are not described in detail here. A couple of examples illustrate the general structure and type of data contents.

[42] This table is taken directly from the SAIC html documentation on UICDS (com.saic.uicds.core.em.endpoint), provided to IDA by the U.S. Army Armament Research, Development and Engineering Center (ARDEC) through the DoD PS/EM Communications Working Group.

## 1. Alert Service Endpoint

The Keystone (UICDS) Alert Service supports the exchange of alerts that are compliant with the OASIS CAP standard. The XML structure of an Alert Request is shown in Figure 7-2. This shows how an alert may optionally be associated with an incident, identified by its *incidentId*. The rest of an alert request specification consists of the standard CAP definition of an alert, as described above in Section 3.D. This illustrates the use of the CAP standard by Keystone, which facilitates its interoperability with the numerous alerting and notification systems that use CAP.

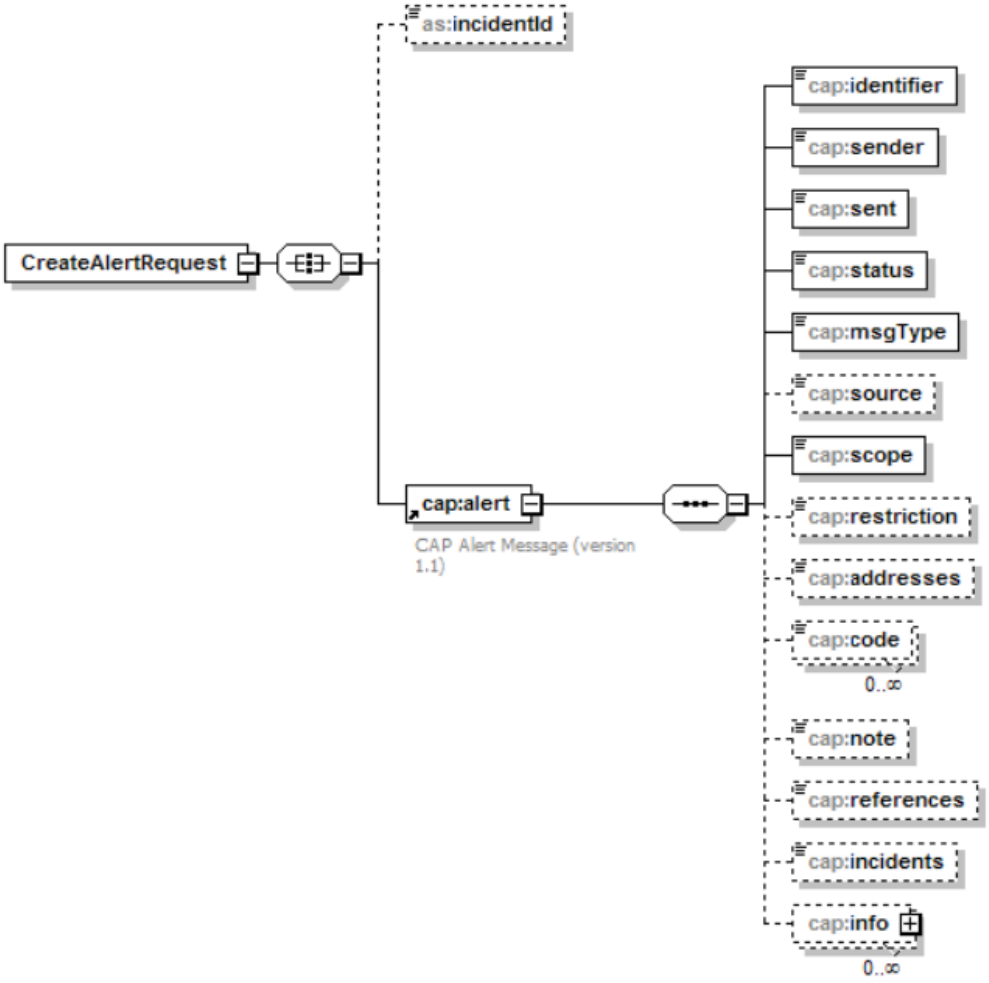


**Figure 7-2. Keystone Alert Service XML Structure[43]**

[43] This illustration is taken directly from the SAIC html documentation on UICDS for the class AlertServiceEndpoint, provided to IDA by ARDEC through the DoD PS/EM Communications Working Group

## 2. Incident Management Service Endpoint

The Keystone (UICDS) Incident Management Service illustrates the use of NIEM Core elements by Keystone. It defines a UICDS incident type in terms of the NIEM Core incident type, whose data elements are illustrated in the shaded portion of Figure 7-3. This figure shows the top level of the NIEM Core data elements used by UICDS that are taken from NIEM Core incident type definition. It includes some NIEM Core activity elements, since a NIEM incident is a kind of activity. The UICDS documentation imposes some business rules constraining the values of *nc:IncidentLocation* elements, as well as requirements for some of the other NIEM Core incident type elements.

The business rules for Incident Management Services allow the *ActivityCategoryText* data element to use local incident typing conventions or to use event types from the Universal Core (UCore) Taxonomy. However, the Universal Core, previously developed by the DoD as a standard for XML-based information sharing, has been superseded by the MilOps Domain of NIEM since the DoD CIO identified NIEM as the preferred XML standard to be considered first for DoD XML-based information sharing. Thus, this part of the Keystone documentation warrants updating to reflect this change in standards policy. More generally, all of the NIEM components of Keystone might see some benefit from updating to a more recent version of NIEM (e.g., the current V3.2).

The Incident Management Service uses a data element defined by the *UICDSIncidentType* in its set of methods used to create an incident, update incident information, share an incident with others, and close and archive an incident.

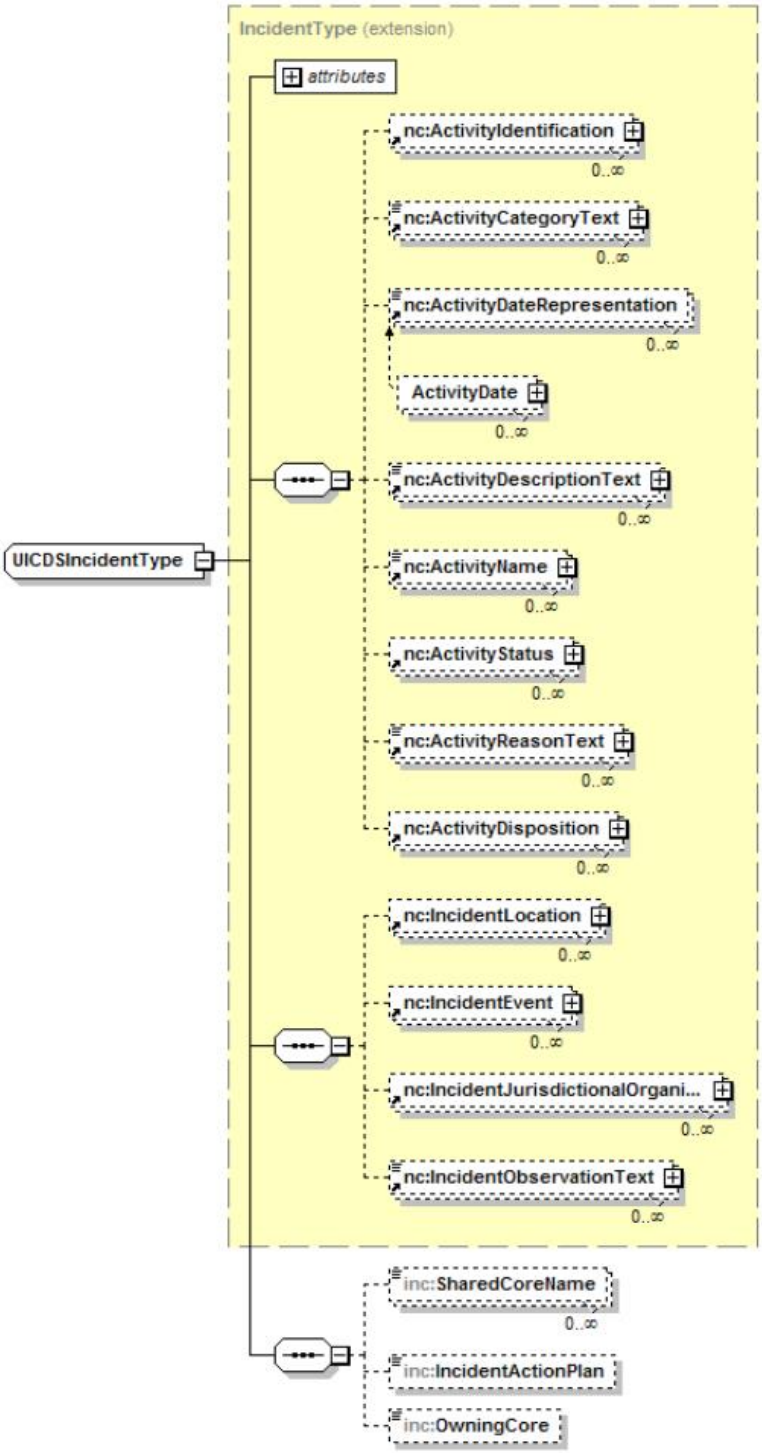


**Figure 7-3. Keystone (UICDS) Incident Management Service XML Structure[44]**

[44] This illustration is taken directly from the SAIC html documentation on UICDS for the class IncidentManagementServiceEndpoint, provided to IDA by ARDEC through the DoD PS/EM Communications Working Group

## C. Keystone (UICDS) Relevance

The information-sharing services and data elements defined for Keystone (UICDS) are relevant to the data requirements for PS/EM communications in at least a couple of different ways. First, they establish a framework for sharing information amongst PS/EM entities across multiple, otherwise incompatible, systems. This creates a bridge between disparate information systems that may be deployed at multiple levels of PS/EM entities, including federal, state, local, tribal, and territorial (FSLTT) responders and their emergency management teams and centers. We cannot reasonably expect all these different entities at different levels of government to standardize on a single set of commercial or government products for sharing emergency incident information. Yet there is an undeniable need for these entities to coordinate in emergency situations. Middleware, such as Keystone and UICDS, offers the promise of cost-effective data communications between entities at all levels of government to address public safety needs effectively.

Second, Keystone itself also includes modifications to the original UICDS code to better meet the needs of the DoD. Keystone extended core-to-core sharing business rules to intra-core sharing rules. It includes several new adapters to support interoperation with NORTHCOM SAGE and the Navy C4I Suite, along with enhancing the WebEOC adapter, and it has an enhanced and validated security architecture. These changes enable operation across DoD systems, while retaining capabilities for interoperation with civilian systems, greatly facilitating communications between these sectors.

Going beyond just providing a middleware translation service, Keystone and UICDS have provided a common lingua franca based largely on existing widely adopted standards, such as the OASIS CAP standard, the NIEM Core, and the LEITSC Call For Service standards. This use of common data standards by the Keystone (UICDS) cores greatly facilitates translations between alerting and emergency management systems, which use these standards. Considering the many information-sharing services that it supports for alerting and emergency management systems, Keystone provides an excellent basis for identifying the data elements needed to support those information services between emergency operations centers, dispatchers, and public safety and emergency responders.

Going forward, Keystone may benefit from considering the use of other emerging standards, such as the APCO/NENA EIDD standard and the NIEM EM Domain. Many of the current Keystone (UICDS) data elements that remain defined within a unique UICDS namespace may benefit from replacement with data elements defined in the more recently developed EIDD and EM Domain standards. Analysis of overlaps between such standards is planned for a subsequent IDA white paper.

# 8. Conclusions

IDA's investigations into systems and data standards for DoD and civilian PS/EM communications revealed the dominance of the OASIS CAP standard in systems supporting public safety warnings and notifications. The related white paper[45] surveying civilian and DoD mass warning and notification systems prepared for this project identifies the following systems using the CAP standard for formulating alert messages:

- Alert!,
- AtHoc,
- Installation Protection Integration Platform (IP2),
- Integrated Public Alert and Warning System (IPAWS),
- Keystone,
- XChangeCore.

In addition, several other systems (Rave Mobile Safety[46] and WebEOC), some of whose data standards are proprietary, have demonstrated interoperability with these systems. Thus, their internal standards either incorporate CAP data elements or are compatible with them. CAP and other EDXL standards are also incorporated into the NIEM EM Domain, so a NIEM information exchange can contain a CAP-compliant alert message.

Given its dominance in mass warning and notification systems, CAP data elements should be an essential part of any compilation of data requirements for DoD and civilian PS/EM communications. The data elements of the EDXL-DE standard should be essential since they are widely used to capture metadata about specific emergency communications, such as alerts using CAP. Support for the data elements of EDXL-HAVE should be required since incidents with many casualties will require PS/EM entities to be notified of available hospital services and beds for victims. The EDXL-RM Resource Message supports a complementary set of messages involving requests for, responses to, and reports on available emergency management resources, including personnel and vehicles.

Most of the NENA standards that IDA analyzed are not directly concerned with information exchanges with PS/EM personnel. Instead, these standards are more likely to be used in the

---

[45] Institute for Defense Analyses, *A Survey of Mass Warning and Notification Systems*, IDA Document D-8388, March 21, 2017.

[46] https://www.ravemobilesafety.com/products/

emergency communications systems supporting these personnel. For example, the standard for *Automatic Location Information* (ALI) describes data elements for different ways to pinpoint the location of an event; systems that use this standard automatically transmit (or receive) location information during a 9-1-1 call, without the person who initiates the call taking explicit action or even being aware that the information is being transmitted. These data elements, commonly used in emergency communications systems, can be considered essential data requirements for the systems, although not necessarily for communications directly with PS/EM entities. PS/EM personnel require location information, but not necessarily in the format specified for 9-1-1 systems. Other sets of standards defining location and caller information are designed to support messages to end users.

Other examples of NENA standards are the Master *Street Address Guide* (MSAG), a specification of the format of information in a national database that can be used to standardize civic addresses, and the *Geographic Information System* (GIS), an extension to the widely used Geography Markup Language model,[47] which incorporates extra concepts relevant to emergency management, such as cell phone towers. NENA also has defined a set of next-generation data models. These models are intended to be used in Internet-based communications, where some or all of the information may be provided by machines rather than humans. Elements in these models are important data requirements for future emergency communications systems. Example next-generation standards include *Discrepancy Reporting* (DR), *Logging* (Log), and *Data with Call*, for transmitting information on the device making a 9-1-1 call. However, these too are focused on system-to-system communications and should not be required for messages exchanged among PS/EM personnel.

In addition to the NENA data standards for the internal communications of 9-1-1 systems, NENA has engaged with APCO International in developing a data standard for exchanging emergency incident data. This Emergency Incident Data Document (EIDD) standard supports the exchange of emergency incident data between CAD systems, and ultimately with PS/EM personnel on mobile systems. This standard is an excellent source of data requirements for PS/EM messaging since it is focused on the information about emergency incidents that is most relevant to them. The EIDD standard is formulated as a NIEM IEPD and leverages the NIEM Core, its associated codes, and other standards, including the APCO Public Safety Communications Common Status Codes for Data Exchange.[48] All of the data elements used from these leveraged standards should be required for DoD-civilian PS/EM messaging.

The NIEM EM Domain data elements support "emergency-related services (including preparing first responders and responding to disasters), information sharing, and activities such as

---

[47] See http://www.opengeospatial.org/standards/gml

[48] This standard-APCO ANS 1.116.1-2015-can be downloaded from the APCO website at: https://www.apcointl.org/doc/911-resources/apco-standards/601-11161-2015-status-codes/file.html

homeland security and resource communications management."[49] As such, we understand that the vast majority of the data elements developed specifically for the EM Domain namespace will have direct relevance to information sharing with and between PS/EM entities. The NIEM EM Domain Facilitator Team has identified those data elements from other domains and code lists that are most essential for emergency management communications. All of these should be required data elements for DoD-civilian PS/EM communications.

Another source of data requirements comes from the Computer Aided Dispatch (CAD) systems used by Public Safety Answering Points (PSAPs) that assist in initiating calls for service, dispatching, and maintaining the status of responding resources in the field. There are numerous vendors of such CAD systems, which may use different internal data elements. However, some efforts have been made to standardize, including the APCO standard status codes for describing the status of emergency units [50] and the new APCO/NENA EIDD standard for exchanging emergency incident information by agencies and regions that implement NG9-1-1 and Internet Protocol (IP)-based emergency communications systems.[51] These standards need to be reviewed for overlap and consistency with the other standards reviewed in this report. Overlap between the EIDD and EDXL standards is readily apparent, although the specifics remain to be documented.

The use of common data standards, such as the NIEM Core and the OASIS CAP, by the Keystone and UICDS cores greatly facilitates translations across alerting and emergency management systems, which use these standards. Considering the many information-sharing services that Keystone and UICDS support for alerting and emergency management systems, they provide an excellent basis for identifying the data elements needed to support those information services among emergency operations centers, dispatchers, and PS/EM responders.

IDA's investigations into data requirements for information exchanges between DoD and U.S. civilian PS/EM entities identified a set of data standards that need to be considered for use in future DoD and U.S. civilian PS/EM communications systems, such as NG9-1-1 and FirstNet. IDA will use these standards in developing a semantic model (an ontology) of core data requirements to facilitate semantic interoperability and enable automated reasoning with such data. And, IDA will analyze overlaps amongst these standards, to be reported in a subsequent white paper.

---

[49] As described on the niem.gov webpage for the EM Domain: https://www.niem.gov/communities/emergency-management

[50] Association of Public-Safety Communications Officials (APCO) International, *ANS1.116.1-2015 Public Safety Communications Common Status Codes For Data Exchange*. https://www.apcointl.org/doc/911-resources/apco-standards/601-11161-2015-status-codes/file.html

[51] APCO/NENA, *APCO NENA 2.105.1-2017 NG9-1-1 Emergency Incident Data Document (EIDD)*. Available from: https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/APCO_NENA_2.105.1-2017_EIDD_.pdf

# Acronyms and Abbreviations

| | |
|---|---|
| ACN | Automatic Crash/Collision Notification |
| ALI | Automatic Location Information |
| ANI | Automatic Number Identification |
| ANSI | American National Standards Institute |
| APAN | All Partners Access Network |
| APCO | Association of Public-Safety Communications Officials |
| API | Application Program Interface |
| ARDEC | Armament Research, Development and Engineering Center |
| AQS | ALI Query Service |
| AVL | Automatic Vehicle Location |
| BCF | Border Control Function |
| C4&IIC | Command, Control, Communications and Computers and Information Infrastructure Capabilities |
| C4I Suite | Command, Control, Communications, Computers and Intelligence Suite |
| CAD | Computer Aided Dispatch |
| CAP | Common Alerting Protocol |
| CBRN | Chemical, Biological, Radiological, Nuclear |
| CLLI | Common Language Location Identifier |
| CIO | Chief Information Officer |
| CONOPS | Concept of Operations |
| CPE | Customer Premise Equipment |
| DCIO | Deputy Chief Information Officer |
| DE | Data Element |
| DHS | Department of Homeland Security |
| DoD | Department of Defense |

| | |
|---|---|
| DOJ | Department of Justice |
| DR | Discrepancy Report |
| DSCA | Defense Support to Civil Authorities |
| EATS | Events Activated Tracking Systems |
| ECRF | Emergency Call Routing Function |
| EDXL | Emergency Data Exchange Language |
| EDXL-DE | Emergency Data Exchange Language-Distribution Element |
| EDXL-HAVE | Emergency Data Exchange Language-Hospital AVailability Exchange |
| EDXL-RM | Emergency Data Exchange Language-Resource Messaging |
| EIDD | Emergency Incident Data Document |
| ELIN | Emergency Location ID Number |
| EM | Emergency Management |
| EMS | Emergency Medical Services |
| EMWN | Enterprise Mass Warning and Notification |
| EOC | Emergency Operations Center |
| ERDB | Emergency Routing Database |
| ESB | Enterprise Service Bus |
| ESN | Emergency Service Number |
| ESRP | Emergency Services Routing Proxy |
| ESZ | Emergency Service Zone |
| FirstNet | Emergency management Network Authority |
| FSLTT | Federal, State, Local, Tribal, and Territorial |
| GIS | Geographic Information System |
| GML | Geographical Markup Language |
| GPS | Global Positioning System |
| HADR | Humanitarian Assistance and Disaster Relief |
| HAVE | Hospital AVailability Exchange |
| IAP | Incident Action Plan |
| ICS | Incident Command Structures |

| | |
|---|---|
| IDA | Institute for Defense Analyses |
| iEOC | Interconnected Emergency Operation Centers |
| IEPD | Information Exchange Package Documentation |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| LEC | Local Exchange Carrier |
| LEITSC | Law Enforcement Information Technology Standards Council |
| LIE | Location Information Element |
| LIS | Location Information Server |
| LVF | Location Validation Function |
| MACS | Multi-Agency Coordination Systems |
| MATADRR | Mission Assurance, Threat Alert, Disaster Resiliency, and Response |
| MilOps | Military Operations |
| MSAG | Master Street Address Guide |
| OGC-SOS | Open Geospatial Consortium Sensor Observation Specification |
| WMWN | Mass Warning and Notification |
| N2C2 | NORAD–USNORTHCOM Current Operations Center |
| NENA | National Emergency Number Association |
| NGESN | Next Generation Emergency Services Network |
| NIEM | National Information Exchange Model |
| NIPR-SAGE | Non-Secure Internet Protocol Router–Situational Awareness Geospatial Enterprise |
| NORAD | North America Aerospace Defense Command |
| NPSCE | National Public Safety Communications Enterprise |
| OASIS | Organization for the Advancement of Structured Information Standards |
| PIDF | Presence Information Data Format |
| PM-ISE | Program Manager, Information Sharing Environment |
| PMO | Program Management Office |
| PS | Public Safety |

| | |
|---|---|
| PS/EM | Public Safety and Emergency Management |
| PSAP | Public Safety Answering Point |
| RMS | Records Management Systems |
| RP | Reporting Party |
| SAR | Suspicious Activity Reporting |
| SDK | Software Development Kit |
| SIF | Spatial Information Function |
| SLTT | State, Local, Tribal, and Territorial |
| SO | Service Order |
| UICDS | Unified Incident Command and Decision Support |
| US | United States |
| USEUCOM | United States European Command |
| USNORTHCOM | United States Northern Command |
| VDB | Validation Database |
| VoIP | Voice over Internet Protocol |
| VPC | VoIP Positioning Center |
| WSDL | Web Service Description Language |
| XML | eXtensible Markup Language |
| XMPP | eXtensible Messaging and Presence Protocol |
| XSD | XML Schema Definition |

# Appendix A. CAP Data Elements Detail

Table A-1 lists the data elements in a Common Alerting Protocol (CAP) message. The table has three columns, the meaning of which are as follows:

- Element: A label for the element. The value in the column is human-readable text. It is not necessarily the value used as a tag name in a CAP XML message.
- Type: The data type of the element. Column values are human-readable words and phrases that suggest an XSD data type. Because all content in an XML message is ultimately a string, the column describes syntactic constraints on an element's value. For example, "date-time" indicates that a string must conform to the form YYYY-MM-DDThh:mm:ssXzh:zm. (This is a CAP requirement that further constrains the syntax of an XSD date-time type.)
- Description: A textual description of the element.

The table emphasizes readability, not XSD fealty. The XML details corresponding to element labels and types in this table are easy to determine from the CAP standard.

The table does not indicate which elements are required, which are optional, and which may appear multiple times. It enumerates only the elements that may appear in an XML document conforming to the CAP standard.

**Table A-1. Common Alerting Protocol Data Elements**

| Element | Type | Description |
|---|---|---|
| Message ID | string | Uniquely identifies an alert message. |
| Sender ID | string | Uniquely identifies a message originator. |
| Sent Date/Time | date-time | Date and time of message origination. |
| Message Status | enumeration | Indicates appropriate handling of the alert message (actual, exercise, test, etc.). |
| Message Type | enumeration | Indicates message nature (new alert, alert update, acknowledgement, etc.). |
| Source | string | Names the operator or device sending an alert message. |
| Scope | enumeration | Specifies intended distribution scope (public, restricted, private). |
| Restriction | string | Used only for alerts whose scope is restricted; describes the restriction. |

| Element | Type | Description |
|---|---|---|
| Addresses | string | Lists intended recipient addresses of an alert message; each address is given as an identifier or address. Required for private-scoped messages, optional otherwise. |
| Handling Code | string | A user-defined code whose format and meaning are not prescribed by CAP. |
| Note | string | Text describing the alert message's purpose or significance; primarily intended for messages whose status is Exercise or whose type is Error. |
| References | string | References to previous CAP messages; each reference is a (sender, identifier, sent date/time) triple. |
| Incidents | string | IDs of incidents to which this alert message refers; the standard does not describe how these identifiers are formatted. |
| Language | ISO 3066-formatted string | The language in which the informational portion of an alert message is being transmitted (an alert can have multiple such portions). |
| Event Category | enumeration | Describes the incident's nature (geophysical, meteorological, etc.). |
| Event | string | Describes the type of the incident. |
| Response Type | enumeration | Describes the recommended response to the incident (shelter, evacuate, monitor, etc.). |
| Urgency | enumeration | Describes the urgency of an incident (immediate, future, past, etc.). *N.B.* Urgency, severity, and certainty together "distinguish less emphatic from more emphatic messages." |
| Severity | enumeration | Describes the severity of an incident (extreme, moderate, etc.). |
| Certainty | enumeration | Describes the certainty that an incident has occurred, is ongoing, or will occur (observed, likely, unlikely, etc.). |
| Audience | string | Describes the intended audience of an alert message. |
| Event Code | XML | A system-specific code, in the form of a (name, value) pair, whose nature is not otherwise prescribed by CAP. |
| Effective Date/Time | date-time | States the effective time of the information in an alert message. |
| Onset Date/Time | date-time | States the expected time of the beginning of an incident. |
| Expiration Date/Time | date-time | States the time at which information in an alert message expires. |
| Sender Name | string | Provides a human-readable name of the agency or authority issuing an alert. |
| Headline | string | Provides a brief human-readable summary of an alert; 160 characters is a reasonable maximum length. |
| Event Description | string | Provides an extended human-readable description of the incident that occasions an alert message. |

| Element | Type | Description |
|---|---|---|
| Instruction | string | Provides an extended human-readable statement of recommended actions to be taken by recipients of an alert message. |
| Information | URL | Gives a link to an Internet-accessible object with additional information about an alert message. |
| Contact Information | string | Provides contact for follow-up and confirmation of an alert message. |
| Parameter | XML | Specifies system-specific parameters that can be associated with an alert. Each parameter is a (name, value) pair; CAP does not further prescribe its format. |
| Resource Description | string | Gives human-readable text describing a resource provided as part of an alert message. |
| MIME Type | RFC 2046-formatted string | Specifies the MIME type of a resource in an alert message. |
| File Size | integer | States the size of a resource, in bytes. |
| URI | URI | Provides the location of a resource. |
| Dereferenced URI | Base 64-encoded data | A resource embedded into an alert message; used if the URI isn't a URL but rather a relative reference to the resource. |
| Digest | SHA-1 hash | Gives the SHA1 hash value of a resource, facilitating confirmation that the resource was transmitted uncorrupted. |
| Area Description | string | A human-readable textual description of an area affected by an incident described in an alert message. |
| Area Polygon | string | Specifies the area affected by an incident as list of points defining a polygon. |
| Area Circle | string | Specifies the area affected by an incident as a point specifying a circle's center and a number specifying a circle's radius, in kilometers. |
| Area Geocode | XML | Specifies geographically-based codes, in the form of (name, value) pairs, delineating the area of an incident in an alert message; CAP does not further define the manner in which the codes define the area. |
| Altitude | decimal | Specifies the height of an area above mean sea level, in feet. |
| Ceiling | decimal | Specifies the maximum height of an area above mean sea level, in feet; if provided along with altitude (both are optional), defines a volume. |

# Appendix B. NENA Data Element Details

## A. Automatic Location Information

NENA has several schemas that describe standards for messages involving automatic location information. Automatic Location Information (ALI) refers to the information transmitted based on information generated by an Automatic Location Identification system.[1] Such a system automatically transmits a caller's address whenever the caller calls 9-1-1 (or any other compatible emergency responder service). The location may be transmitted as a postal address, especially if the call is made from a land line (telephone companies maintain databases of addresses that Automatic Location Identification systems can access), or as a geolocation of a cellular device.

The primary schema, described in the first subsection, deals specifically with ALI. The other schemas provide support.

### 1. Automatic Location Information Main Schema

A message containing Automatic Location Information includes components describing the location of a call. Location may be given as a street address, according to the Master Street Address Guide (MSAG), discussed in Section 5.A.2; as a geolocation; as a cell site; or as a combination of these elements.

ALI may also include information on agencies near the location, on the caller and the calling number, on the 9-1-1 network through which a call is being routed, and on the sources used to collect the data in an ALI message.

Table B-1 contains the data elements for ALI defined in the ALI schema.

**Table B-1. Automatic Location Information Data Elements**

| Element | Type | Description |
|---|---|---|
| Agencies | (complex) | Categorized as police, fire, EMS, ESN, other. May also include specific agency names, and more specific type labels. One or more of the following elements may appear. Best practice is to always include ESN. |
| Police | (complex) | Agency name and telephone number. |
| Fire | (complex) | Agency name and telephone number. |

[1] See https://www.techopedia.com/definition/2925/automatic-location-identification-ali. Both Automatic Location Identification and Automatic Location Information use the acronym ALI. In the context of NENA, ALI refers to Automatic Location Information.

| Element | Type | Description |
|---|---|---|
| EMS | (complex) | Agency name and telephone number. |
| Others | (complex) | Agency name and telephone number. Unlike the three above, an arbitrary number of other agencies may be included. |
| Additional information | string | Up to 75 characters of free-form information on additional responders. |
| ESN | integer (3–5 digits) | An emergency service number associated with a house, street, or community. |
| Call Information | (complex) | Information on callers. |
| Callback # | telephone # | Telephone number that can be dialed to reach a specific calling party. In an ALI response, this number may be different than the CallingPartyNum for Wireless and VoIP calls. The PSAP receives a “pseudo-ani,” which is used as CallingPartyNum for the ALI Query. The ALI queries the correct MPC or VPC and sets CallBackNum using the information sent back from the MPC or VPC. The ALI will “echo-back” the ESQK as CallingPartyNum and will set CallBackNum to the actual Call Back Number returned from the MPC or VPC. |
| Calling Party # | telephone # | Emergency Location ID Number (ELIN). |
| Class of service | enumeration | Values from 0-9, A-K, V (not in that order). |
| Type of service | enumeration | 0=NotFX nor Non-published; 1=FX in 911 serving area; 2=FX outside of 911 serving area; 3=non-published; 4=non-published FX in 911 serving area; 5=non-published FX outside 911 serving area; 8=PS/ALI published; 9=PS/ALI non-published. |
| Source of service | enumeration | In the future, this may be returned from the V-E2 interface for VOIP calls. If this is returned, the V-E2 interface should also return an accurate Class of Service (e.g., Residence instead of VoIP) and Type of Service for the call. When Source of Service is returned, all 3 fields should be included in the ALI Response so that the CPE can determine the best way to present the information to the PSAP. This field should also be set for non-VoIP calls. This field is used in the ALI Response schema only. V = VoIP; W = wireless L = Landline. |
| Main Tel # | telephone # | Main Billing Number associated with the calling party. |
| Customer name | string | Subscriber name associated with the Calling Party Number. |
| Customer code | string | Code used to uniquely identify a wireline customer. |
| Attention indicator | enumeration | Identifier for calls that may require special attention. 1=TTY call; 2=ACN (Automatic crash/collision notification). |
| Special message | string | Message text for communicating special call conditions/warnings. |
| Also-rings-at address | string | Civic address in textual (free-form) representation. |
| Language preference | string | Language preference, from the IANA language subtag registry. |
| Location information | | Elements related to a call’s location. |

| Element | Type | Description |
|---|---|---|
| Street address | (complex) | Options for specifying street address. Includes NENA-specific items (e.g., MSAGCommunity). |
| Geolocation | (complex) | Options for specifying geolocation. |
| Cell site | (complex) | Cell ID, sector ID (best practice: include both), descriptive text . |
| comment | string | |
| Source | (complex) | Elements related to the source of ALI provisioning. |
| Data provider | (complex) | NENA registered Company ID for Service Provider supplying ALI record source information. |
| Access provider | (complex) | NENA registered Company ID for Service Provider providing wireline, wireless, or VoIP service to the customer. |
| Update time | date-time | Date/Time when ALI record last updated. |
| Retrieval time | date-time | Date/Time ALI DB request received or broadcast. |
| General uses | tokens | General use tags. |
| Network | | Type definition for set of elements related to Emergency Service Network components associated with the call. |
| PSAP ALI | string | Identifier of the ALI Host Computer transmitting the ALI response to the PSAP (or through a node if applicable). |
| Resp ALI | string | Identifier of the ALI Host Computer that is the source of the ALI response message. |
| PSAP ID | string | PSAP ID for the PSAP associated with the ESN determined by the caller's location. |
| PSAP Name | string | Textual PSAP identity (PSAPID). |
| Router ID | string | Selective Router Identifier (E911 Tandem). |
| Exchange | string | A defined area served by one or more telephone Central Offices within which a LEC furnishes service. |
| CLLI | string | CLLI code (Common Language Location Identifier). The CLLI code is an 11 character alphanumeric field of the form AAAABBCCDDD, where AAAA represents the city/county, BB represents the State, CC represents the building or location, and DDD represents the network. |
| Extension | any | Type definition for container elements that can be used to “append” additional payload data elements in cases in which those data elements have not been yet ratified by NENA for integration in SORecord as first-class elements. |

## 2. Master Street Address Guide

The Master Street Address Guide (MSAG) is a database populated with locations keyed by telephone numbers. A record includes a street name, along with sufficient identifying information to disambiguate that street from other similar or identically named streets. It further includes house numbers, although these are given not necessarily as single numbers but as ranges.

The MSAG transmits information in records. Table B-2 describes the contents of a record.

**Table B-2. Master Street Address Guide Data Elements**

| Element | Type | Description |
|---|---|---|
| Header | (complex) | A header definition for a collection of records, usually in a file. |
| Company Name | string | The name of a company forwarding a file of records. |
| Cycle Counter | integer | A sequential number used to verify files processed sequentially. |
| Extract Date | date | The date data was processed. |
| Record Count | string | Used by sender and receiver to provide and consume additional information; limited to 20 characters. |
| Freeform | | |
| MSAG Record | (complex) | A set of elements representing a change to the MSAG. |
| Function of Change | character | If "D," an MSAG record indicates deletion; if "I," the record indicates insertion. |
| Street | (complex) | Contains sufficient information to identify a street, including name, direction (N, NE, etc.), county, and state/province. Must specify the MSAG community name, a valid service community name as identified by the MSAG. May also specify a valid service community name as identified by the U.S. Postal Service. |
| Completion | date | States the completion date of the service order for an MSAG record. |
| Number of Ranges | integer | Specifies the number of ranges in an MSAG record (see next row). |
| Range | (complex) | Defines a range of addresses in an MSAG—for example, the lowest street number to the highest. |
| General Use | string | Used by sender/receiver companies to pass information not defined in other fields in an MSAG record. |
| Extension | (complex) | Used to add additional payload elements to an MSAG record. |

## B. Service Order

A NENA service order (SO) record describes the location at which the service is to occur. Location is given as an address, again as a street address, geolocation, or cell tower site. It is also given in terms of the customer receiving the service. Information on the customer includes the customer's name and telephone number, as well as the nature of the telephone and descriptions of the kind of service requested.

Table B-3 lists the data elements in a service order.

**Table B-3. Service Order Data Elements**

| Element | Type | Description |
|---|---|---|
| TNInfo | (complex) | Elements related to telephone number and customer. |
| Calling Party Number | telephone # | An Emergency Location ID Number (ELIN). |
| Class of Service | enumeration | Describes service class, e.g., residence, business, residence PBX, coin-operated pay phone, VoIP. NENA defines 25 classes of service (including Not Available). |
| Type of service | enumeration | Combinations of foreign exchange vs. non-foreign exchange; published vs. non-published; private switch vs. non-private switch. |
| Main telephone number | telephone # | The (main) billing number associated with the calling party. |
| Callback number | telephone # | Telephone number that can be dialed to reach a specific calling party. |
| Customer name | telephone # | The subscriber name associated with the calling party number. |
| Customer code | string | A three-digit code used to uniquely identify a wireline customer. |
| Special attention indicator code | enumeration | An identifier for calls that may require special attention. Currently it has only two values: “1” means a TTY call; “2” means an Automatic Crash/Collision Notification. |
| Exchange | string | A four-digit string identifying a defined area served by one or more telephone Central Offices within which a Local Exchange Carrier (LEC) furnishes service. |
| Emergency Services Number | string | An Emergency Service Number associated with a House number, Street name, and Community name. |
| Pseudo-ANI | telephone # | Pseudo-Automatic Number Identification (ANI) or locally specific code identifying the receiving antenna for the wireless 9-1-1 call for routing purposes. |
| Alternate Telephone Number | telephone # | A remote call-forwarding number used during Interim Number Portability. |
| Comment | string | Optional notes that may appear at a PSAP. |
| Location Information | (complex) | Information related to the location of a telephone number. |
| Street Address | (complex) | Information on street addresses. |
| Geo-position | (complex) | Latitude, longitude, and optional elevation. |
| Cell site | (complex) | Identification of a cell site by cell site ID, sector ID, or textual description. Best practice is to include both cell site ID and sector ID. |
| Also-Rings-at Address | string | A textual description of an address at which a telephone number also rings. |

| Element | Type | Description |
|---|---|---|
| Source Information | (complex) | Elements related to the source and status of a service order. |
| Status Indicator | enumeration | Whether the record indicates error, completion, pending work, or an unprocessed order. |
| Function of Change | enumeration | The type of activity the service order prescribes. Values include: change, delete, insert, unlock, migrate, and delete error record. |
| Data Provider | (complex) | NENA-registered Company ID for Service Provider supplying ALI record source information. |
| Access Provider | (complex) | NENA-registered Company ID for Service Provider providing wireline, wireless, or VoIP service to the customer. |
| Completion Date | date | Service order completion date. |
| Order Number | string | Service order number. |
| Initial Load | Boolean | True if a service order record is part of an initial load. |
| Errors | list of strings | Instances of error codes that apply to a service order record. |
| General Use | string | Used by sender/receiver companies to pass information not defined in previous fields. |
| Extension | (complex) | Used to append additional payload data elements to a Service Order, in cases in which those data elements have not been yet ratified by NENA for integration in Service Order record as first-class elements. |

## C. ALI Query Service

The ALI Query Service (AQS) specifies new protocols between a PSAP and the Next Generation Emergency Services Network (NGESN). It overcomes ALI limitations described further in the AQS standard.[2] The specification includes Web Service Description Language (WSDL) descriptions of the query operations AQS supports.

The ALI Query Service is provided as a Standard Preview Release. This means it expresses a "relatively mature" standard that "nevertheless" remains a work in progress and is subject to change.

The ALI Query Service's elements are defined in a single XML schema that lays out the syntaxes of an AQS query and the response to that query. The schema also provides for an advisory message. The query may be an advisory request, in which case the response will be an advisory.

Table B-4 shows the data elements in the schema.

[2] See *NENA ALI Query Service Standard*, Section 1. This document is included in the NENA schemas distribution, in file aqs/doc/DocSet/ NENA AQS Draft 1.3.docx.

**Table B-4. ALI Query Service Data Elements**

| Element | Type | Description |
|---|---|---|
| Query Request | (complex) | A query request message. |
| Query Type | enumeration | The type of query to perform. Values include: Normal, Rebid, Refresh, Manual, and Test. Application-specific query types are also allowed. |
| Query Key | (complex) | The key for the query. It may be given in numeric form, as a URI, or using an extension (i.e., an application-specific form). |
| Query Properties | (complex) | Ancillary information related to a query request. It includes one or more of a trunk ID, a call-taker position, and an extension. |
| Query Response | (complex) | A message sent in response to a query request message. |
| Status | (complex) | Status information about the response message. It includes a code value; sample values are OK, OKMore (more information can be obtained), and Request Refused. It may also include textual descriptions of the status. |
| Query Key | (complex) | The query key given in the query request. |
| Query Properties | (complex) | The query properties given in the query request. |
| Query Result Data | (complex) | The result message payload. It is delivered as XML, in a syntax dependent on the query server. |
| Advisory | (complex) | An advisory notification. |
| Advisory Type | enumeration | Types of advisories; includes a standard set (e.g., Alert, Call Terminated) and the ability to accommodate application-specific types. |
| Advisory Data | (complex) | The advisory payload. It can be either free text or XML content in a non-AQS namespace. |

## D. Geographic Information System

A Geographic Information System (GIS) is a computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a street address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It also can be used to graphically display coordinates on a map, i.e., latitude and longitude from a wireless 9-1-1 call.

NENA provides a single schema related to Geographic Information Systems, the NENA GISsfProfile, which provides an extension to the Geographical Markup Language (GML) XML schema. It provides ways to describe geographic features that are advantageous to 9-1-1-related messages. Table B-5 shows the data elements supported.

**Table B-5. Geographic Information System Data Elements**

| Element | Type | Description |
|---|---|---|
| NENA Features | (complex) | The root element for describing NENA features. |
| Cell | (complex) | Describes a cell site location. |
| Company ID | (complex) | A telephone number/name pair identifying a NENA company ID for a Location Determination Technology Provider. |
| Site Numeric ID | string | A numeric ID for a cell site. |
| Site Unique ID | string | An ID provided by a wireless service provider; it must be unique to a cell site. |
| Site Address | (complex) | Gives a street address for a cell site location. |
| Air interface technology | enumeration | A code stating whether cell service is analog, digital, TDMA, or GSM. |
| Data source | string | (unknown) |
| Last Update | string | (unknown) |
| Point | (complex) | The geolocation of the cell site. This element is required. All other elements of Cell are optional. |
| Cell Coverage | (complex) | Coverage boundaries of a cell site. |
| Provider ID | (complex) | A telephone number/name pair identifying a NENA company ID for a Location Determination Technology Provider. |
| Site Numeric ID | string | A numeric ID for a cell site. |
| Site Unique ID | string | An ID provided by a wireless service provider; it must be unique to a cell site. |
| Sector ID | string | Subset/section of a cell. When Phase II location cannot be provided, Phase I information, i.e., the cell site or sector where the call is received, should be reported. |
| Numeric Sector ID | integer | (unknown) |
| ESRD | telephone # | Emergency services routing digit. |
| Sector orientation azimuth | integer (0..360) | Orientation of the cell sector antenna face, with North being 0 degrees and South being 180 degrees. |
| Sector compass orientation | string | (unknown) |
| Sector Beam Width | integer | (unknown) |
| Sector Average Radius | integer | (unknown) |
| Coverage Source | enumeration | The source of information on sector coverage. Values: company map; digital data, GIS propagation [sic] study; line-of-site analysis; range definition. |
| Data source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of coverage area as a polygon. This element is required; all others are optional. |
| County | (complex) | Data to identify a county. |

| Element | Type | Description |
|---|---|---|
| County ID | string | A code that identifies a county. Usually from FIPS. |
| Data source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of the county's area as a polygon. This element is required; others are optional. |
| Emergency Service Agency Boundary | (complex) | Defines the boundaries of an Emergency Service Agency. |
| PSAP ID | string | PSAP ID for the PSAP associated with the ESN determined by the caller's location. |
| County Name | string | A county's name. |
| County ID | string | A code that identifies a county. Usually from FIPS. |
| Agency ID | string | (unknown) |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of the Emergency Service Agency's area as a polygon. This element is required; others are optional. |
| Emergency Service Zone | (complex) | Defines the boundaries of an Emergency Service Zone (ESZ). |
| Community ID | string | The name of the community in which an ESZ is located. |
| PSAP ID | string | PSAP ID for the PSAP associated with the ESN determined by the caller's location. |
| County Name | string | A county's name. |
| County ID | string | A code that identifies a county. Usually from FIPS. |
| Agency ID | string | (unknown) |
| Emergency Service Number | integer | An Emergency Service Number (ESN) associated with a community. |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of the Emergency Service Zone's area as a polygon. This element is required; others are optional. |
| Hydrology Boundary | (complex) | Hydrology boundary. |
| Surface water line | string | Type of Surface Water (pond, lake, large waterway, reservoir, etc.). |
| Segment ID | integer | Unique identifier for a segment in a hydrology boundary. |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of the Hydrology Boundary's area as a polygon. This element is required; others are optional. |
| Hydrology centerline | (complex) | Center line through a hydrological area. |
| Surface water type | string | Type of Surface Water (river, stream, etc.). |

| Element | Type | Description |
|---|---|---|
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Segment List | (complex) | One or more line segments that, taken together, describe the centerline. |
| Mile Marker | (complex) | Location described by a mile marker on a route. |
| Milepost ID | integer | Identifier for the milepost ID of a mile marker. |
| Mile marker type | enumeration | Values include: railroad, road, and trail. |
| Route system name | string | Name of route system (example: Interstate 85). |
| Segment ID | string | (unknown) |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Point | (complex) | The geolocation of a mile marker. This element is required; others are optional. |
| Municipal Boundary | (complex) | Describes the boundary of a municipality. |
| Community ID | string | A unique identifier for the community described by a municipal boundary. |
| MSAG Community Name | string | Valid service community name as identified by the MSAG. |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Polygon | (complex) | Specification of a municipality's area as a polygon. This element is required; others are optional. |
| Railroad | (complex) | Specifies the centerline of a railroad. |
| Line owner | string | Railroad Line Owner (Code of Association of American Railroads). |
| Line type | enumeration | One of Main, Secondary, or Siding. |
| Line status | enumeration | One of Active or Inactive. |
| Passenger rail indicator | Boolean | True if the railroad line is for passenger rail, false if not. |
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Rail segment list | (complex) | One or more elements describing a segment on a rail line. |
| Railroad Grade Crossing | (complex) | Gives the location of a railroad grade crossing. |
| Grade crossing ID | string | Grade Crossing ID assigned to USDOT.[3] |
| Crossing position | enumeration | One of at-grade, railroad under, or railroad over. |

[3] The annotation for Grade Crossing ID states that the ID is assigned to USDOT (File nenaGISsfProfile.xsd, line 256). This is probably a mistake; more probably, the ID is assigned *by* USDOT.

| Element | Type | Description |
|---|---|---|
| Data Source | string | (unknown) |
| Last update | date | (unknown) |
| Point | (complex) | The geolocation of the railroad grade crossing. This element is required; others are optional. |

## E. Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)

NENA has released evolving versions of standards. One, released in 2006, is known as the Interim VoIP Architecture for Enhanced 9-1-1 Services, and is also known as i2. NENA's i3 services represent next-generation services; these are covered below, in Section K.

### 1. Presence Information Data Format

Presence information describes the ability and willingness of an entity to communicate. NENA supports Internet Engineering Task Force RFC 4481,[4] *Timed Presence Extensions to the Presence Information Data Format (PIDF) to Indicate Status Information for Past and Future Time Intervals*. Table B-6 shows the elements in the NENA schema.

**Table B-6. Presence Information Data Elements**

| Element | Type | Description |
|---|---|---|
| Presence | (complex) | Geolocation information. |
| Tuple | (complex) | A sequence of status, notes, points of contact, and timestamp information. |
| Note | (complex) | Natural language notes, each marked with the language in which it is written. |

### 2. Emergency Routing Database

The Emergency Routing Database (ERDB) is a database of Emergency Service Zones in a service area, along with routing information among those zones. Zones are defined in terms of geographic boundaries. The NENA ERDB XML schema specifies messages that may be used to communicate and update those boundaries. Table B-7 shows the data elements in an ERDB message.

[4] https://tools.ietf.org/html/rfc4481

**Table B-7. Emergency Routing Database Data Elements**

| Element | Type | Description |
|---|---|---|
| Boundary Definition | (complex) | A sequence of (ERDB identifier, geolocation) pairs. |
| ERDB ID | string | An identifier for an ERDB. |
| Geometry | (complex) | Specifies the geometry of the identified ERDB. |

## F. VoIP Positioning Center to/from Emergency Services Routing (V2)

The V2 schema defines messages sent across the V2 interface to a VoIP Positioning Center (VPC). Table B-8 shows the data elements in the schema.

**Table B-8. V2 Data Elements**

| Element | Type | Description |
|---|---|---|
| ESR Request | (complex) | An Emergency Services Routing Request, used to retrieve routing keys from a VPC based on location information. |
| VPC | (complex) | A provider of either service or information. |
| Source | (complex) | A provider of either service or information. The source provider type is added when a node adds information to a request or result. |
| VSP | (complex) | A provider of either service or information. |
| Call ID | string | Any identifier that can be used to uniquely identify the call at the Call-Server. |
| Callback | integer | E.164 number that can be dialed by a PSAP operator to reach the call originator. |
| LIE | (complex) | The Location Information Element (LIE) contains location information that is used to determine the routing and query keys to be used for the call. |
| Call Origin | string | Used by a VPC when it sends a Location Key to the LIS over the V3 interface. |
| Timestamp | date-time | Date and time a message was generated. |
| Customer | (complex) | Subscriber name associated with the Calling Party Number. Should be formatted as LastName, FirstName. |
| ESR Response | (complex) | A response to an ESR request. |
| Result | 3-digit integer | Codes that indicate whether or not a VPC was able to provide routing information and the means by which the routing data was determined. |
| VPC | (complex) | A provider of either service or information. |
| Destination | (complex) | A provider of either service or information. |
| Call ID | string | Any identifier that can be used to uniquely identify the call at the Call-Server. |
| ERT | (complex) | Emergency Route Tuple. |
| ESQK | integer | Emergency Services Query Key |

| Element | Type | Description |
|---|---|---|
| ESGWRI | string | Emergency Services GateWay Route Identifier. |
| LRO | URI | The Last Routing Option LRO provides the Call-Server with a fallback destination for the call in the event that there are trunk issues between the ESGW and the Selective Router, or between the Selective Router and the PSAP (if detectable). This number is provided directly from the ERDB, and will in most cases represent the DN of the PSAP, and will usually be supplied in conjunction with an ESRN and ESQK. This element should be either a tel URI or it should provide equivalent function, such as a SIP URI. |
| Timestamp | date-time | Date and time a message was generated. |

## G. Location Information Server to/from VoIP Positioning Center (V3)

The V3 schema defines messages sent across the V3 interface between a Location Information Server (LIS) and a VoIP Positioning Center (VPC). It is deprecated, so its elements are not included in this document.

## H. Validation Database Interface (V7)

The V7 schema defines messages sent across the V7 interface to a Validation Database (VDB). Table B-9 shows the data elements in the schema.

**Table B-9. V7 Data Elements**

| Element | Type | Description |
|---|---|---|
| Validate Address In | (complex) | An incoming message requesting address validation. |
| Message ID | string | An optional identifier for a message; if sent by the caller it will be echoed in the response. |
| Customer ID | string | An optional customer identifier, assigned by a VDB operator and provided to a customer. |
| Street Address | (complex) | Civic address, in NENA format, using NENA field definitions. |
| Validate Address Out | (complex) | An outgoing message in response to a Validate-Address-In message. |
| Message ID | string | The message identifier provided in the Validate-Address-In message, if one was given. |
| Return Code | enumeration | Signifies whether address validation succeeded. Example codes: success; street name required; state not found. |
| Valid | enumeration | Indicates whether the address in the Validate-Address-In message is valid. Values: valid address; invalid address; N/A (used for specific return codes). |
| Address List | (complex) | A list of addresses in response to the address provided in the Validate-Address-In message. Each element in the list is a civic address (street, city, etc.), a geolocation, or both. |

| Element | Type | Description |
|---|---|---|
| Alternate URI | URI | URI-based information that may provide additional information about the address in the Validate-Address-In message. |

## I. VoIP Positioning Center to/from Emergency Routing Databases (V8)

The V8 schema defines messages that are sent across the V8 interface to a VPC. Table B-10 shows the data elements in the schema.

**Table B-10. V8 Data Elements**

| Element | Type | Description |
|---|---|---|
| ERDB Request | complex | Used by a VPC to retrieve routing information from the ERDB. |
| Message ID | string | Uniquely identifies a message from the perspective of a VPC. |
| Source | (complex) | A provider of either a service or information. |
| VPC | (complex) | Identifies the VPC as the provider of a routing information service. |
| Location | (complex) | Location for which information from the ERDB is desired. It may be an address, a geolocation, or both. |
| Timestamp | date-time | The date and time of the message. |
| Destination | (complex) | The ERDB from which routing information is being requested. |
| ERDB Response | (complex) | Sent by an ERDB to a VPC in response to an ERDB Request message. |
| Message ID | string | The message ID provided in the ERDB Request. |
| Source | (complex) | The source provided in the ERDB Request. |
| ERDB | (complex) | The ERDB that is providing the routing information. |
| ERT | (complex) | An Emergency Route Tuple. It consists of a Selective Routing Identifier, a routing Emergency Services Number, and a Numbering Plan Area. |
| Admin ESN | integer | An Emergency Services Number associated with a house number, street name and community name. |
| CRN | integer | Contingency Routing Number |
| MSAG Valid Civic Address | (complex) | The address, in MSAG format, provided by the ERDB. |
| Geocoded Location | (complex) | The geolocation of the provided address. |
| Result | enumeration | Describes whether the ERDB provided information, and if so, the nature of the information; if not, why. Example values: success (geodetic); success (civic); error (bad location). |
| Timestamp | date-time | The time a response message was sent. |
| Destination | (complex) | A node requesting the routing information. |

## J. Request/Response on Database for Location of the Sender (V9)

The V9 schema defines messages that are sent across the V9 interface to determine which Validation Database (VDB) or Emergency Routing Database (ERDB) to query. Table B-11 shows the elements in the schema.

**Table B-11. V9 Data Elements**

| Element | Type | Description |
|---|---|---|
| Identity Request | (complex) | Used by a VPC to determine which ERDB to request routing information from, or by an LIS operator to determine which VDB to use to validate civic information. |
| Query Type | enumeration | Either ERDB or VDB. |
| Location | (complex) | Specifies the location at which to search for ERDBs or VDBs. It may be a civic address, a geolocation, or both. |
| Identity Response | (complex) | Sent in response to an Identity Request message. Its content is one of the three elements “ambiguous”, “error”, or “found”, described in the next three rows. |
| ambiguous | (complex) | A list of civic addresses satisfying an Identity Request. Each civic address lists the fields that must be resolved before an answer can be determined. |
| error | enumeration | An indication that an Identity Request message is erroneous. Values are “Not Found” and “General Error”. |
| found | (complex) | Lists ERDBs or VDBs that serve the location submitted in the Identity Request. ERDBs and VDBs are identified by URI. An ERDB may also include a point of contact. |

## K. NextGen (i3)

NextGen is, as the name implies, NENA’s effort to promote next-generation 9-1-1 communications standards. It has several high-level schemas (collectively known as i3), covered in the following subsections, which encapsulate query-response communications (request-response, in NENA parlance). The NENA distribution also includes Web Services Description Language (WSDL) specifications of the requests and responses.

The NextGen area also contains schemas with elements used in the high-level schemas. These schemas provide the details of acceptable addresses, geolocations, and the like. It seems sufficient to note that NextGen requires address and geolocation data elements without deep exploration of their precise syntax (at least for now). These common schemas are not included below.

### 1. Data With Call

The Data With Call schema specifies the data that is associated with a 9-1-1 call. This data includes information on the device making the call, the URL of the caller (if known), and whether

the call is from a business or residence. Information about the caller is provided in the standard vCard format.[5] Table B-12 shows the elements in the schema.

**Table B-12. Data With Call Data Elements**

| Element | Type | Description |
|---|---|---|
| Data Associated With Call | (complex) | The Data Associated with a Call. Additional data may be associated with a specific 9-1-1 call. This data may be provided by the device which places the call, or any intermediary, such as a carrier, telematics provider, alarm company or video relay, who handles the call. Devices may provide additional data; any intermediary handling the call must provide additional data, when available. |
| Data Provided By | (complex) | Information on the organization that provides the data associated with a call. |
| Caller Data URL | URI | The URL for Data Associated with the Caller. The URL is provided by the caller to his carrier. The carrier is not responsible for the URL or the data that the URL points to. |
| Service Environment | enumeration | Business or Residence. |
| Service Delivered By Provider | string | The type of service the end user has subscribed to. The implied mobility of this service cannot be relied upon. A NENA Registry System will contain valid entries. |
| Device Classification | string | The kind of device making the 9-1-1 call. A NENA Registry System will contain valid entries. |
| Device Manufacturer | string | The manufacturer of the device making the 9-1-1 call. A NENA Registry System will contain valid entries. |
| Device Model | string | (unknown) |
| Device ID | string | (unknown) |
| Device ID Type | string | The type of device identifier being generated in the unique device identifier data element. A NENA Registry System will contain valid entries. |
| Device-Specific Schema | XML | Additional data about a device. |
| Privacy Indicator | enumeration | Whether the call service type is a Business or Residence caller. Currently, the only valid entries are Business or Residence. |
| Subscriber vCard | string | Information known by a Service Provider about a subscriber; i.e., Name, Address, Calling Party Number, Main Telephone Number and any other data. |

[5] IETF RFC 6350, *vCard Format Specification*, available at https://tools.ietf.org/html/rfc6350

## 2. Discrepancy Reporting

The Discrepancy Reporting schema defines messages to maintain and query discrepancy reports. There must be a discrepancy report (DR) function to notify agencies and services (including BCF, ESRP, ECRF, Policy Store, and LVF) when any discrepancy is found. The discrepancy reporting audience is anyone who is using the data and finds a problem. Table B-13 lists the NENA discrepancy reporting data elements. These elements are structured into two query-response formats. One deals with querying discrepancies and receiving reports in response. The other deals with requesting reports on discrepancy resolutions. The data elements for both formats are summarized in Table B-13.

**Table B-13. Discrepancy Reporting Data Elements**

| Element | Type | Description |
|---|---|---|
| Discrepancy Report Request | (complex) | A message requesting information on a discrepancy report. |
| Timestamp | date-time | The date and time the request was sent. |
| Report ID | string | (unknown) |
| Agency | string | The name of the agency requesting a discrepancy report. |
| Agent | string | (unknown) |
| Contact | string | Contact information, in vCard format. |
| Service | string | (unknown) |
| Severity | string | (unknown) |
| Comment | string | (unknown) |
| Discrepancy | (complex) | Specification of the different types of discrepancies requested. It may be either a Location Validation Function (LVF) discrepancy or a policy discrepancy. |
| Discrepancy Report Response | (complex) | A response to a Discrepancy Report Request. |
| Agency | string | The name of the agency requesting a discrepancy report. |
| Agent | string | (unknown) |
| Contact | string | Contact information, in vCard format. |
| Estimated Response Timestamp | date-time | (unknown) |
| Comment | string | (unknown) |
| Error Code | enumeration | Possible responses to a discrepancy-related request message. Sample values: OK; Unknown Service/Database; Unauthorized Reporter. |
| Discrepancy Resolution Request | (complex) | A message requesting information on a discrepancy resolution. |
| Query Key | string | Provides a key for a discrepancy resolution request query. |

| Element | Type | Description |
|---|---|---|
| Reporting Agency | string | The name of an agency submitting a discrepancy resolution request. |
| Discrepancy Resolution Response | (complex) | A message in response to a Discrepancy Resolution Request message. |
| Query Key | string | The query key submitted in the Discrepancy Resolution Request message. |
| Resolution Report | (complex) | The resolution report, if the query succeeds (see the Error Code element). It includes a description of the resolution, using enumerated values. Examples include (for policy discrepancies) “policy added”, “policy updated”, and “no such policy”. |
| Error Code | enumeration | Possible responses to a discrepancy-related request message. Sample values: OK; Unknown Service/Database; Unauthorized Reporter. |
| Status Update Request | (complex) | A message requesting a status update. |
| Report ID | string | The identifier of a report for which a status update is desired. |
| Agency | string | The name of the agency requesting a status update. |
| Agent | string | (unknown) |
| Contact | string | Contact information, in vCard format. |
| Comment | string | (unknown) |
| Status Update Response | (complex) | A message sent in response to a status update request. |
| Agency | string | The name of the agency requesting a status update. |
| Agent | string | (unknown) |
| Contact | string | Contact information, in vCard format. |
| Estimated Response Timestamp | date-time | (unknown) |
| Comment | string | (unknown) |
| Error Code | enumeration | Possible responses to a status update-related request message. Sample values: OK; Unknown Service/Database; Unauthorized Reporter. |

## 3. Emergency Call Routing Function Messages

The Emergency Call Routing Function (ECRF) must report gaps and overlaps larger than the provisioned threshold. To do so, it makes uses of the GapOverlap event. All 9-1-1 Authorities who provide source GIS data to an ECRF must subscribe to its GapOverlap event. The event notifies both agencies when it receives data that shows a gap or overlap larger than the threshold. The notification includes the layer(s) where the gap/overlap occurs, whether it is a gap or an overlap, and a polygon that represents the gap or overlap area.

Table B-14 lists the data elements in the schema.

**Table B-14. Emergency Call Routing Function Data Elements**

| Element | Type | Description |
|---|---|---|
| Gap Overlap | (complex) | |
| Agency | URI | (unknown) |
| Layer | string | The layers where the gap or overlap occurs. |
| Gap | Boolean | If true, the message refers to a gap; if false, to an overlap. |
| Polygon | (complex) | The gap or overlap area. |

## 4. Emergency Services Routing Proxy Messages

The Emergency Services Routing Proxy (ESRP) assists in routing 9-1-1 messages. The ESRP schema defines messages used by the ESRP. Table B-15 lists the elements in the schema.

**Table B-15. Emergency Services Routing Proxy Data Elements**

| Element | Type | Description |
|---|---|---|
| Dequeue Registration Request | (complex) | DequeueRegistration is web service whereby the registering entity becomes one of the de-queuing entities, and the ESRP managing the queue will begin to send calls to it. The registration includes a value for DequeuePreference, which is an integer from 1–5. |
| Queue | URI | URI of the queue to use for ESRP. |
| Dequeue Preference | integer between 0 and 5 | (unknown) |
| Dequeue Registration Response | (complex) | A message sent in response to a Dequeue Registration Request. |
| Error Code | enumeration | Indicates the response to a Dequeue Registration Request. Values are: Okay (no error); Unspecified error; Bad dequeue preference; policy violation. |
| Queue State | (complex) | An event that indicates to an upstream entity the state of a queue. The SIP Notify mechanism described in RFC 3265 is used to report QueueState. The event includes the URI of the queue, the current queue length, allowed maximum length and a state. |
| Queue | URI | The URI of a queue. |
| Queue Length | integer | (unknown) |
| State | enumeration | The state of the queue specified by the Queue URI. One of: Active; Inactive; Disabled; Full; Standby. |

## 5. Logging Services

NENA standards include support for a logging capability to keep track of 9-1-1 messages and events. Each log entry includes a timestamp, information about the agency that logged an event, and technical details of the 9-1-1 call. The Logging Services schema defines messages for logging services. Table B-16 lists its data elements.

**Table B-16. Logging Service Data Elements**

| Element | Type | Description |
|---|---|---|
| Log Event | (complex) | Logs an event into a logging service. |
| Timestamp | date-time | Timestamp for a log event. |
| Agency or Element | string | AgencyID or hostname of an element which logged the event. An Agency is an organization that is a client of a database or service, which is represented by a domain name (hostname from STD013 [108]). Agencies must use one domain name consistently in order to correlate actions across a wide range of calls and incidents. Any domain name in the public DNS is acceptable so long as each distinct agency uses a different domain name. This implies that each agency ID is globally unique. An example of an agency identifier is psap.allegheny.pa.us. |
| 3Agent ID | string | An agent is a person employed by or contracted by an agency. An agent identifier is a user name, using the syntax for “Dot-string” in RFC2821 (that is, the user part of an email address, without the possibility of a “Quoted-String”). Usernames must be unique within the domain of the agency, which implies that the combination Agent and Agency IDs is globally unique. Examples of this include tom.jones@psap.allegheny.pa.us and tjones.atroop@state.vt.us. |
| Call ID | string | (unknown) |
| Incident ID | string | (unknown) |
| Call Process | (empty) | Each element which is not call stateful, but handles a call, logs the fact that it saw the call pass through by logging a CallProcess event. There are no parameters to “Call Process” |
| Start Call | string | Each element which is call stateful logs the beginning and end of its processing of a call with Start Call and End Call events. StartCall includes a copy of the headers in the INVITE message, encoded in header tags. |
| End Call | string | Each element which is call stateful logs the beginning and end of its processing of a call with Start Call and End Call events. EndCall includes the response code that ended the call (200 OK in the case of a successful call), encoded in a responseCode tag. |
| Transfer Call | string | When a call is transferred, the transfer is logged by the transferor (the PSAP which had the call prior to transferring it. The transfer target URI is logged in a transferTarget tag. |

| Element | Type | Description |
|---|---|---|
| Route | (complex) | Proxy servers that make routing decisions (ESRPs or other SIP proxy servers in the path of the call) log the route it selected with the Route EventType. The URI where it decided to send the call (encoded in a URI tag, plus a text string reason for choosing that route are included in the LogEvent. For ESRPs, the name of the rule is included in a rule tag. |
| Media | (complex) | Media is the log of call media (voice, video and interactive text). The media event includes a text string udp tag that contains an RFC2327 Session Description Protocol [55] description of the media. The SDP must include SDES keys if the RTP stream is protected with SRTP. Each independent stream must include an RFC4574 [138] label to identify each stream and the label must be logged with a mediaLabel tag. More than one Media event can occur for a call. Recorded media streams include integral time reference data within the stream. |
| End Media | string | EndMedia causes the logging service to terminate recording of media. The EndMedia event includes one or more mediaLabel tags which must match the SDP labels in the corresponding Media event. More than one EndMedia (with different mediaLabels) may occur for a call. |
| Message | string | A SIP Message (Instant Message) is logged with a Message log event. The text of the message is included as a text parameter. |
| Additional Agency | string | When an agency becomes aware that another agency may be involved, in any way, with a call, it must log an AdditionalAgency event. The AdditionalAgency event includes an agency tag which is an Agency Identifier (see Section 3.1.1). Among other uses, this event is used by PSAP management to query all logging services that may have records about a call or incident. |
| Merge Incident | (complex) | At some point in processing, an agency may determine that a call marked with an IncidentId may in fact be part of another, previously determined Incident. When it is determined that two IncidentIds have been assigned for the same real world Incident, the Ids are merged with MergeIncident. The MergeIncident record contains the IncidentId of the incorrectly assigned incident in the incidentId tag in the header of the log record, and the Incident Id of the actual Incident in an actualIncident tag. Note that other agencies may not know that the Incidents are being merged, and therefore could log events against the originally assigned IncidentId. |
| Clear Incident | (empty) | When an agency finishes its handling of an Incident, it logs a ClearIncident record. Other agencies may still be processing the Incident. |
| ECRF Query | (complex) | Any element that queries the ECRF and the ECRF itself generate an ECRFquery LogEvent. The LogEvent includes the PIDF-LO (and only the Location Object) using the RFC4119 tags and the service URN in a service-urn tag. |
| ECRF Response | string | Both the elements that query the ECRF and the ECRF generate the ECRFresponse. The entire response is logged using the LoST tags. |

| Element | Type | Description |
|---|---|---|
| Log Response | (complex) | A message in response to a Log Event. |
| Log Identifier | string | The identifier for a Log Event. |
| Retrieve Log Request | (complex) | To retrieve a logged event from the logging service, RetrieveLogEvent will return the log record for all events. The request to RetrieveLogEvent includes a logIdentifer parameter, as returned by the original LogEvent. When the event is a Media event, the returned event from RetrieveLogEvent will not have the SDP parameter, but will instead have an rtsp parameter that must be an RTSP URL. The RTSP URL can be used to play back the media stream(s). |
| Log Identifier | string | The identifier of a logged event. |
| Retrieve Log Response | (complex) | A message in response to a Retrieve Log Request message. |
| Log Event | (complex) | An event logged into a logging service. |
| RSTP | URI | (unknown) |
| Error Code | enumeration | Possible responses to a Retrieve Log Request. Sample values: Okay (no error); No such log identifier; No such incident identifier. |
| List Events by Call ID | (complex) | A request to retrieve Logging Events using a Call ID as the query key. |
| Call Identifier | string | The Call ID to use in a List-Events-by-Call-ID query. |
| List Events by Incident ID | (complex) | A request to retrieve Logging Events using an Incident ID as the query key. |
| Incident ID | string | The Incident ID to use in a List-Events-by-Incident-ID query. |
| List Incidents by Date Range | (complex) | A request to retrieve Logging Events that occurred during a specified date range. |
| Start Time | date-time | The starting time of a List-Incidents-By-Date-Range query. |
| End Time | date-time | The ending time of a List-Incidents-By-Date-Range query. |
| List Incidents by Date and Location | (complex) | A request to retrieve Logging Events that occurred during a specified date range at a specified location. |
| Start Time | date-time | The starting time of a List-Incidents-By-Date-and-Location query. |
| End Time | date-time | The ending time of a List-Incidents-By-Date-and-Location query. |
| Area of Interest | (complex) | A polygon specifying the area of interest in a List-Incidents-By-Date-and-Location query. |
| List Logs Response | (complex) | A response to a query to list logging events (List Events by Call ID, List Events by Incident ID, List Events by Date Range, List Events by Date and Location). |
| Log ID | string | Zero or more log identifiers that match the parameters specified in the query. |
| Error Code | enumeration | Possible responses to a List Log Request. Sample values: Okay (no error); No such log identifier; Unspecified error. |
| List Agencies by Call ID | (complex) | A request to retrieve agencies matching a call identifier. |
| Call Identifier | string | The call identifier to use in a List-Agencies-by-Call-ID query. |

| Element | Type | Description |
|---|---|---|
| List Agencies by Incident ID | (complex) | A request to retrieve agencies matching an incident identifier. |
| Incident Identifier | string | The incident identifier to use in a List-Agencies-by-Incident-ID query. |
| List Agencies Response | (complex) | A message sent in response to a List-Agencies query. |
| Agency Identifier | string | An agency identifier matching the parameters in a List-Agencies query. |
| Error Code | enumeration | Possible responses to a List Agencies query. Sample values: Okay (no error); No such call identifier; No such incident identifier. |

## 6. Policy Store

NENA maintains a common policy store from which policies can be retrieved. The Policy Store XML schema defines messages to add, maintain, and query policies. Table B-17 lists its data elements.

**Table B-17. Policy Store Data Elements**

| Element | Type | Description |
|---|---|---|
| Retrieve Policy Request | (complex) | Retrieves a policy set from the common policy store. The function's parameters include the policy name, the identity of the agency whose policy is needed, and an indication of the maximum size of the return. The response is the policy set, if it is smaller than the indicated maximum size, or the first chunk of the policy set if it is large, plus an identifier that can be used with MoreRetrievePolicy to obtain more chunks of a large policy set if the policy is too large to send in the response, and an expiration time. The policy store may reduce the size of the chunk returned if it us unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The policy retrieved is valid until the expiration time. If the policy is needed for use after expiration, it must be retrieved again from the policy store. The response may not return the policy requested. Instead, it may return a referral to another policy store that may have the policy. |
| Policy Name | string | Policy name to retrieve. |
| Agency | string | The agency whose policy is requested. Must be a domain name or URI that contains a domain name. |
| Max Chunk Size | integer | Large retrieve-policy requests may receive responses in several "chunks". This element specifies the maximum chunk size. |
| Retrieve Policy Response | (complex) | A message sent in response to a Retrieve Policy Request message. |
| Policy Data Chunk | string | The first "chunk" of data in a policy request. |
| TTL | time | Expiration time. |

| Element | Type | Description |
|---|---|---|
| Next Chunk ID | string | If the policy cannot be retrieved in a single chunk and must be obtained through subsequent More-Retrieve-Policy-Request messages, this element specifies the identifier of the next chunk. |
| Referral | URI | (unknown) |
| Error Code | enumeration | Indicates the results of the query request. Sample values: OK (no error); Unknown or bad policy name. |
| More Retrieve Policy Request | (complex) | Retrieves another chunk of a large policy set. The request includes the identifier returned to the requester in a RetrievePolicy or prior MoreRetrievePolicy operation and an indication of the maximum size of the return. The response is the next chunk of the policy set, plus an identifier that can be used on a subsequent invocation of MoreRetrievePolicy. The policy store may reduce the size of the chunk returned if it is unable or unwilling (by local policy) to serve a chunk as large as the requester specifies. The policy store must be able to accept and respond to a request it has already sent (that is, the identifiers may be used repeatedly, in case of error). The identifiers can be expired in a reasonable time period (perhaps 30 minutes). |
| Next Chunk ID | string | The identifier of the next chunk to retrieve. It is obtained from a previous Retrieve-Policy-Response or More-Retrieve-Policy-Response message. |
| Max Chunk Size | integer | The maximum allowed size of the next chunk. |
| More Retrieve Policy Response | (complex) | Returned in response to a More-Retrieve-Policy-Request message. |
| Policy Data Chunk | string | The next chunk of data in a policy request. |
| Next Chunk ID | string | The identifier of the next chunk of data, if the remaining data is larger than the Max Chunk Size parameter of the More-Retrieve-Policy-Request. |
| Error Code | enumeration | Indicates the results of the query request. Sample values: OK (no error); Bad chunk ID. |
| Store Policy Request | (complex) | Initiates the storage of a policy set in the policy store. This function's parameters include the name of the policy, the agency whose policy is being stored, the size of the entire policy set, the expiration time, and the maximum chunk size the sender is willing to send. If the name of the agency is omitted, the sender's identity is used. The response contains the maximum size of the initial chunk, which must be no larger than the sender's maximum chunk size, and an identifier to be used with the MoreStorePolicy function. |
| Policy Name | string | The name of the policy to store. |
| Agency | string | The name of the agency whose policy is being stored. |
| Policy Size | integer | The size of the policy. |
| TTL | time | Expiration time. |

| Element | Type | Description |
|---|---|---|
| Max Chunk Size | integer | The maximum size of the initial chunk. |
| Store Policy Response | (complex) | The response to a Store Policy Request. |
| Max Chunk Size | integer | The maximum allowed size of the initial chunk. |
| Next Chunk ID | string | An identifier to pass in the next More-Store-Policy-Request message. |
| Error Code | enumeration | The result of the Store-Policy-Request message. Sample values: OK (no error); Policy too large; Bad TTL. |
| More Store Policy Request | (complex) | Sends a chunk of the policy set to the store. Its parameters include the identifier returned from StorePolicy or a prior invocation of MoreStorePolicy, and a chunk of the policy set. The response contains the maximum size of the next chunk (which must be no larger than the maximum chunk size indicated by the sender on the original StorePolicy invocation) and an identifier to be used on a subsequent MoreStorePolicy to send the next chunk. Identifiers may be reused, but if they are, any later chunks are discarded by the store and must be re-sent. Identifiers may be expired in a reasonable time (perhaps 30 minutes). |
| Next Chunk ID | string | The identifier of a data chunk, obtained either from a Store Policy Response message (for the first chunk) or from the last-received More-Store-Policy-Response message (for subsequent chunks). |
| Policy Data Chunk | string | The data chunk of the policy. |
| More Store Policy Response | (complex) | The response to a More-Store-Policy-Request message. |
| Max Chunk Size | integer | The maximum size of the next chunk. |
| Next Chunk ID | string | An identifier for the next chunk, if more of the policy remains to be transmitted. |
| Error Code | enumeration | The result of the More-Store-Policy-Request message. Sample values: OK (no error); Chunk too big. |
| Enumerate Policies Request | (complex) | Returns a list of policy names available in the store for a specific agency. The parameters of the request include the name of the policy set and the name of the agency. The response includes a list of the policy names in the store, the last date they were stored, expiration time, and the size of the policy. The enumeration includes only those policies that are actually stored in this specific instance of the policy store. |
| Policy Name | string | The name of a policy set. |
| Agency | string | The name of the agency storing the policy set. |
| Enumerate Policies Response | (complex) | A response to an Enumerate-Policies-Request message. |

| Element | Type | Description |
|---|---|---|
| Policy Name | string | The name of a policy in the store. |
| Agency | string | The name of the agency that stored the policy. |
| Policy Size | integer | The size of the policy. |
| TTL | time | The expiration time. |
| Last Modification | date-time | The date the policy was last stored. |
| Error Code | enumeration | The result of the Enumerate-Policies-Request message. Sample values: OK (no error); Unknown or bad agency name. |
| Updated Policies Request | (complex) | Returns a list of policies updated in the Policy Store since a given time. The request includes a timestamp. The response is a list of policy names and agencies whose policy has been updated since the timestamp in the request. |
| Policy Name | string | The name of a policy set. |
| Agency | string | The name of the agency storing the policy set. |
| Updated Since | date-time | Policies last stored on or after this time are to be retrieved as a result of this request. |
| Updated Policies Response | (complex) | Sent in response to an Updated-Policies-Request message. |
| Policy Name | string | The name of a policy updated on or after the moment denoted by the Updated-Since element in an Updated-Policies-Request message. |
| Agency | string | The name of the agency that stored the named policy. |
| Policy Size | integer | The size of the policy. |
| TTL | time | The policy's expiration date. |
| Last Modification | date-time | The date the policy was last stored. |
| Error Code | enumeration | The result of the Updated-Policies-Request message. Sample values: OK (no error); Unknown or bad agency name. |

## 7. Spatial Information Function

The Spatial Information Function (SIF) is the base database for NG9-1-1. Nearly all location-related data is ultimately derived from the SIF. If a datum is somehow associated with location, the base data will reside in the SIF.

Table B-18 lists the SIF data elements.

**Table B-18. Spatial Information Function Data Elements**

| Element | | Type | Description |
|---|---|---|---|
| Geocode Request | | (complex) | |
| Presence | | (complex) | Geolocation information. This element must contain at least one tuple; within that tuple there must be a status element that contains location information. Location information must be provided as valid geo-coordinates using the GML-pidf-lo-shape schema or as a civic address using the civic-Address schema. See draft-ietf-geopriv-pidf-lo-provile-06.txt for best practice recommendations for location data. |
| Geocode Response | | (complex) | |
| presence | | (complex) | Geolocation information. |
| Referral | | URI | (unknown) |
| Error Code | | enumeration | Values: OK (no error); Unspecified error; No address found. |
| MSAG to PIDF Request | | (complex) | |
| MSAG | | (complex) | |
| MSAG to PIDF Response | | (complex) | |
| presence | | (complex) | |
| Referral | | URI | |
| Error Code | | enumeration | Values: OK (no error); Unspecified error; No address found. |
| PIDF to MSAG Request | | (complex) | |
| Presence | | (complex) | |
| PIDF to MSAG Response | | (complex) | |
| MSAG | | (complex) | |
| Referral | | URI | |
| Error Code | | enumeration | |
| Reverse Geocode Request | | (complex) | |
| Presence | | (complex) | |
| Reverse Geocode Response | | (complex) | |
| Presence | | (complex) | |
| Referral | | URI | |
| Error Code | | enumeration | |

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE (DD-MM-YY) | 2. REPORT TYPE | 3. DATES COVERED (From – To) |
|---|---|---|
| 03-21-17 | Final | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| Department of Defense Public Safety and Emergency Management Communications: Interoperability Data Requirements | HQ0034-14-D-0001 |
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBERS |

| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
|---|---|
| Serena Chan, Brian A. Haugh, Francisco L. Loaiza-Lemos, Steven P. Wartik | ET-5-4155 |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Institute for Defense Analyses<br>4850 Mark Center Drive<br>Alexandria, VA 22311-1882 | D-8416<br>H 2017-000202 |

| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR'S / MONITOR'S ACRONYM |
|---|---|
| Joseph M. Wassel<br>Director, C4 Resilience & Mission Assurance<br>DoD CIO, 6000 Defense Pentagon, Arlington, VA 20301 | DoD CIO |
| | 11. SPONSOR'S / MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Serena Chan

14. ABSTRACT

This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence and Deputy Chief Information Officer (DCIO) and for the Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO). The objective of this project is to assess the current state of communications interoperability between DoD Public Safety and Emergency Management (PS/EM) entities and United States (US) civilian PS/EM entities and how that is likely to change as the next generation of public safety information systems is implemented across the nation. This white paper addresses the data reuqirements for information exchanges involving DoD and US civilian PS/EM entities. IDA's investigations have identified a set of data standards that need to be considered for use in future DoD and US civilian PS/EM communications systems, such as FirstNet. IDA will use these standards in developing a semantic model (an ontology) of core PS/EM communications data requirements to facilitate semantic interoperability and enable automated reasoning with such data.

15. SUBJECT TERMS

Public safety and emergency management communications; information exchange; data standards; interoperability

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Joseph M. Wassel |
| Unclassified | Unclassified | Unclassified | Unlimited | 90 | 19b. TELEPHONE NUMBER (Include Area Code)<br>703-901-7360 |