NENA/APCO Next Generation 9-1-1 Public Safety Answering Point (NG-PSAP) Requirements

This DRAFT document is not intended for distribution beyond the groups developing or reviewing the document. The document is also not intended to be used or referenced for development or procurement purposes until final publication. All draft material is subject to change and it is possible that the document itself may never be approved for publication.

NENA/APCO Next Generation 9-1-1 Public Safety Answering Point (NG-PSAP) Requirements

NENA/APCO-REQ-001.1-201X

DSC Approval: MM/DD/YYYY
PRC Approval: MM/DD/YYYY
NENA Executive Board Approval: MM/DD/YYYY
APCO Executive Director Approval: MM/DD/YYYY

Prepared by:
National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) Next Generation 9-1-1 Public Safety Answering Point (NG-PSAP) Work Group

Published by: NENA and APCO
Printed in USA

NENA/APCO
REQUIREMENTS DOCUMENT
NOTICE

This Requirements Document (REQ) is published by the National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO), and is intended to be used by Standard Development Organizations (SDO) including NENA, APCO, and/or designers, manufacturers, administrators and operators of systems to be utilized for the purpose of processing emergency calls. It should be considered to be a source for identifying the requirements necessary to meet the needs of the emergency services industry as it applies to the subject covered in this REQ. It is not intended to provide complete design or operation specifications or parameters, nor to assure the quality of performance for systems that process such equipment or services.

NENA/APCO reserves the right to revise this Requirements Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Or to reflect changes in the design of equipment, network interfaces or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA/APCO documents are subject to change as technology or other influencing factors change. Therefore, this NENA/APCO document should not be the only source of information used. NENA and APCO recommend that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA, APCO or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the use of 9-1-1 System Service Providers, network interface and system vendors, participating telephone companies, 9-1-1 Authorities, etc.

By using this document, the user agrees that NENA and APCO will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

The NENA/APCO NG9-1-1 PSAP Working Group has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Road, Suite 500
Alexandria, VA 22314
202-466-3911
Email: commleadership@nena.org

or

Association of Public-Safety Communications Officials International
351 N. Williamson Blvd
Daytona Beach, FL 32114
386-322-2500

77 **ACKNOWLEDGEMENTS**

78

79 The National Emergency Number Association (NENA), the Association of Public-Safety
80 Communications Officials (APCO), the NENA Agency Systems Committee and the NENA/APCO
81 NG9-1-1 PSAP Working Group developed this document.

82 NENA and APCO recognize the following industry experts and their employers for their
83 contributions in development of this document.

84

85 Executive Board Approval Date [MM/DD/YYYY]

86 APCO Executive Director Approval: [MM/DD/YYYY]

Members	**Employer**
Michael Smith, Agency Systems Committee Co-Chair and Work Group Co-Chair	DSS Corporation
Rick Blackwell, ENP, Agency Systems Committee Co-Chair and Work Group Co-Chair	Greenville County Office of E9-1-1 SC
Mike Vislocky, Past Agency Systems Committee Co-Chair	Network Orange
Charles Corprew, Past Work Group Leader	AT&T
Joe Gallelli, Past Work Group Leader	Zetron
Glenn Bowers, Past Work Group Leader	AT&T
Amy McDowell, ENP	Greenville County Office of E9-1-1 SC
Dan Mongrain, Technical Editor	Bell Canada
Bob Connell, ENP	Zetron
Theresa Connell, OPMA	Office of Emergency Management, State of Oregon
Jay English, ENP	APCO International
Robert Leathers	McLennan County 9-1-1 Emergency Assistance District TX
Steve O'Conor, ENP	Synergem Technologies, Inc.
Brian Rosen	Neustar Inc.
Jerry, Schlesinger, PMP	City of Portland, Oregon, PSSRP
Tommy Tran	North Central Texas Council of Governments
Holly Barkwell	BH Group Inc.
Theresa Williams	Riverside County Fire CA
Lisa M. Wirtanen	AT&T
Nadine Boulanger	Sarasota County FL

Eric Caddy-PMP	Mission Critical Partners
Gordon Chinander-GISP	Metropolitan Emergency Services Board MN
Guy Churchouse-ENP-CCNA	Revcord
Bob Finney III-ENP	Collier County FL
John Geib-ENP	Montgomery County PA
Alan Harker	Spillman Technologies Inc.
Will Hickey	Spectracom Corp
Clint Hugghins, PE, ENP	RCC Consultants Inc.
Glenna Johnson	DeKalb County IL
Steve Lagreid	King County WA
Robert Leathers-ENP	McLennan County 9-1-1 Emergency Assistance District TX
Roger Marshall	TeleCommunication Systems Inc. (TCS)
Crystal McDuffie	APCO International HQ
Ernest McFarland-ENP	Manatee County FL
Paul McLaren	Intrado Inc.
Kathy McMahon	Mission Critical Partners Inc.
Christian Militeau-ENP	Intrado Inc.
Mart Nelson	Avista
Linda Ogilvie	Intergraph Corporation
Mike Page, ENP	Ontario Ministry of Health
Kantu Patel	AT&T
John Quattrocchi	AT&T
Philip Reichl	Modular Communication Systems Inc.
Remi Rundzio	Motorola Solutions Inc.
Jim Shepard-ENP	911 Datamaster Inc.
Robert Sherry-ENP	Intrado Inc.
Steve Simpkin	Modular Communication Systems Inc.
Michael Slater-ENP	State of Massachusetts
James Soukup	City/County of Durham NC
Richard St. Jean	Airbus DS Communications Inc. (formerly Cassidian Communications Inc.)
Bob Tilden	AT&T
Henry Unger	Hitech Systems Inc.
Lisa Vasquez	Unisys Corporation
Raymond Vilis	Solacom Technologies
Robert Walthall	AT&T, National Public Safety Solutions Inc.
Ron Wilson	Cassidian Communications Inc.
James Winegarden	CenturyLink Inc.

87

This working group also thanks Pete Eggimann and Jim Shepard, Development Steering Council Co-Chairs; Roger Hixson, Technical Issues Director; and Ty Wooten, Education and PSAP Operations Director.

Table of Contents

1 Executive Overview

Major changes in the existing emergency services architecture are being driven by the rapid evolution of the types of devices and services that can be used to request emergency services. There is an increasing volume and diversity of information that can be made available to assist PSAPs and responders in an emergency. NENA and APCO recognize this is a fundamental update to the North American 9-1-1 system, and are addressing the challenge with a system design called "Next Generation 9-1-1" (NG9-1-1). NG9-1-1 is the evolution of Enhanced 9-1-1 to an all IP-based emergency communications system.

This technical requirements document introduces requirements for a NG9-1-1 Public Safety Answering Point (PSAP) that is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the latest version of the NENA i3 Architecture document [4]. An emergency call enters the i3 PSAP using Session Initiation Protocol (SIP [17]) signaling. NG9-1-1 encourages the creation of many new coordination and information access services to enrich collaborative interactions between all agencies involved in processing emergency service requests. This document is issued as NENA/APCO recommended requirements for functions and interfaces between an i3 PSAP and NG9-1-1 Core Services (NGCS), and among Functional Elements associated with the i3 PSAP.

This document is primarily intended to drive the development of one or more standards that meet the technical requirements specified herein. Unless otherwise indicated, the requirements in this document do not apply to products and services unless and until matching specifications are published in applicable standards.

Scope

The scope of this document is intended to provide the detailed technical requirements for an i3 PSAP that is capable of interoperating with NGCS. It also describes the application service environment of the i3 PSAP and the interfaces required for processing of an Incident. In this context a PSAP is not intended to indicate a single physical premises. A PSAP may consist of Telecommunicators, Dispatchers, applications and services within a single physical location or geographically distributed using IP connectivity.

The lifecycle of an incident begins at the moment an emergency call is initiated. For the purposes of this document, the life cycle of the PSAP Incident starts with the arrival of the emergency call at the PSAP and ends with its final archiving and closure.

An emergency call encompasses all communication(s) between the originator (caller) and the i3 PSAP including voice. This document uses the word "call" to refer to a session established either by signaling with two way real-time media involving a human making a request for help, or an automated device sending a notification or other data. This document sometimes uses "voice call", "video call", or "text call" when specific media is of primary importance.

The Functional Elements described in this document interact from PSAP Incident initiation to closure. The interfaces identified in this section are those necessary to facilitate this interaction.

The requirements in this document apply to any features that are used to operate in a NG9-1-1 environment. This document is not intended to define the requirements for transitioning from a legacy PSAP into an operational i3 PSAP.

2 Introduction

2.1 Operations Impacts Summary

NG9-1-1 encompasses a complete redesign of the entire 9-1-1 system, affecting all elements, protocols, processes and procedures. It will have far reaching impacts on all participants in the 9-1-1 system. This document contains the requirements for PSAPs operating within a NG9-1-1 system. A PSAP which conforms to the standard that will be developed from these requirements and conforming to the PSAP section of NENA-STA-010 [4] is called an i3 PSAP. The requirements in this document reflect the long-term view of the networks that connect the caller to PSAPs and PSAPs to alternate destinations, including responders, will evolve to be IP-based. Location of the caller (or a reference to it) will be conveyed with the emergency call so that location is available as soon as possible. The PSAP must support both civic and geodetic forms of location; which implies a GIS system. GIS systems impact system management, system integrity, training and a host of methods and procedures.

2.2 Technical Impacts Summary

This document states requirements that will drive development of one or more standards. Those standards are expected to impact development of future systems and/or processes. Anticipation of those standards may result in decisions to delay development or implementation, since requirements are not sufficient to drive those. This document may cite specific published standards in these requirements. Those requirements and standards may change during the development of the standard(s) that result from this document.

2.3 Security Impacts Summary

As the PSAPs evolve from the existing E9-1-1 processes and procedures into an IP-based network, a multitude of security topics arise. While security is beyond the scope of this TRD, further requirements can be obtained via the NENA Security for Next-Generation 9-1-1 Standard [6].

2.4 Document Terminology

The terms "shall", "must", "mandatory", and "required" are used throughout this document to indicate normative requirements and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "should", "may", "desirable" or "preferable".

2.5 Reason for Issue/Reissue

NENA and APCO reserve the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Doc #	Approval Date	Reason For Changes
NENA/APCO-REQ-001.1-201X	[MM/DD/YYYY]	Initial Document

2.6 Recommendation for Additional Development Work

This document provides requirements for i3 PSAP Functional Elements and interfaces. From these requirements, standards will need to be developed in order to achieve interoperable implementations. This document also provides guidance which needs to be incorporated in operational standards.

This document also specifies additional work that must be addressed:

- Define what constitutes a relevant change to an Incident or asset that requires an EIDD to be sent.
- Define standardized SNMP MIBs and traps for NG9-1-1 Functional Elements.
- Define physical requirements for NG9-1-1 equipment such as electrical, environmental, space, etc.

2.7 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application(s), computer-based or any other type application.

2.8 Anticipated Timeline

The evolution to NG9-1-1 is a major change to the 9-1-1 system and adoption of this standard will take several years. Experience with major change to 9-1-1 (i.e., previous integration to Phase II wireless) suggests that unless consensus among government agencies at the local, state and federal levels, as well as carriers, vendors and other service providers is reached, implementation for the majority of PSAPs could take a decade. The adoption of these requirements will be coincident with the evolution of the NGCS since there is an inherit dependency upon those services being available to support the functionality specified in this document.

2.9 Cost Factors

This is an all-new 9-1-1 system; the cost of all components will change. Since the scope of NG9-1-1 introduces new functionality and interfaces, there will be costs associated with introducing these. At the time of the writing of this document, it is difficult to predict the costs of the system. More work will be needed by vendors and service providers to determine the impact of the changes on their products and operations.

2.10 Cost Recovery Considerations

Not applicable.

2.11 Additional Impacts (non-cost related)

Certain requirements contained in this NENA document are known to have impacted existing NENA standards, and are expected to impact future NENA standards. At the date of publication of this document, some development work had begun. Existing documents already known to have been impacted include NENA 08-003 version 1 and NENA-STA-010 (a.k.a. 08-003 version 2) [4], the NENA/APCO Emergency Incident Data Document (EIDD) Information Document [25], and other NENA standards and information documents. These requirements are intended to guide development of i3 PSAP specifications, which will be published in a future NENA standard. The authoring group expects that these requirements will influence future standards development in a variety of areas, including but not limited to, NG9-1-1 network, security, and communications technology, as well as PSAP operations.

2.12 Intellectual Property Rights Policy

NOTE–The user's attention is called to the possibility that compliance with these requirements may require use of an invention covered by patent rights. By publication of these requirements, NENA and APCO take no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA and APCO invite any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement these requirements.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202-466-3911
or commleadership@nena.org

or

Association of Public-Safety Communications Officials
351 N. Williamson Blvd
Daytona Beach, FL 32114
386-322-2500

2.13 Acronyms/Abbreviations, Terms and Definitions

Some acronyms/abbreviations, terms and definitions used in this document may have not yet been included in the NENA or APCO master glossary. After initial approval of this document, they will be included. See NENA-ADM-000, NENA Master Glossary of 9-1-1 Terminology, located on the NENA web site for a complete listing of terms used in NENA documents. All acronyms used in this document are listed below, along with any new or updated terms and definitions.

The following Acronyms are used in this document:		
Acronym	**Description**	**(N)ew (U)pdate**
ACD	Automatic Call Distribution	
ANSI	American National Standards Institute	
APCO	Association of Public Safety Communications Officials	
BCF	Border Control Function	
CAD	Computer Aided Dispatch	
CAP	Common Alerting Protocol	
CPE	Customer Premises Equipment	U
CJIS	Criminal Justice Information System	
ECRF	Emergency Call Routing Function	
EIDD	Emergency Incident Data Document	
ESInet	Emergency Services IP Network	
ESRP	Emergency Services Routing Proxy	
FE	Functional Entity or Functional Element	
GIS	Geographic Information System	
IDE	Incident Data Exchange	N
IMR	Interactive Multimedia Response	
IP	Internet Protocol	
IRR	Instant Recall Recorder	N
ISSI	Inter-RF Sub System Interface	N
i3	NENA Detailed Functional And Interface Standard for NG9-1-1	
LEO	FBI's Law Enforcement Online	N
LDAP	Lightweight Directory Access Protocol	
LIS	Location Information Server	
LTE	Long Term Evolution	
LVF	Location Validation Function	
LoST	Location-to-Service Translation	

The following Acronyms are used in this document:		
MIS	Management Information System	
MSAG	Master Street Address Guide	
NCIC	National Crime Information Center	
NENA	National Emergency Number Association	
NG9-1-1	Next Generation 9-1-1	
NG-SEC	Security for Next Generation 9-1-1	N
NTP	Network Time Protocol	
P25	Project 25	N
PBX	Private Branch Exchange	
PIDF-LO	Presence Information Data Format-Location Object	
PRF	Policy Routing Function	
PSAP	Public Safety Answering Point	
PSTN	Public Switched Telephone Network	
RMS	Records Management System	
RoIP	Radio over IP	N
RTT	Real Time Text	
SBC	Session Border Control	
SDO	Standards Development Organization	
SIF	Spatial Information Function	
SIP	Session Initiation Protocol	
SLA	Service Level Agreement	
SNMP	Simple Network Management Protocol	
TCP/IP	Transaction Control Protocol/Internet Protocol	
TDD	Telecommunications Device for the Deaf or Time Division Duplex Mode	
TRD	Technical Requirements Document	
TTY	Teletypewriter (a.k.a. TDD Telecommunications Device for the Deaf and Hard-of Hearing)	
UCADFR	Unified Computer Aided Dispatch Functional Requirements	

The following Acronyms are used in this document:		
URI	Uniform Resource Identifier	
URL	Uniform Resource Locater	
XML	eXtensible Markup Language	

285

The following New Terms and Definitions are used in this document:		
Term	**Definition**	**(N)ew (U)pdate**
Call Handling Functional Element	Functional Element concerned with the details of the management of calls. It handles all communication from the caller. It includes the interfaces, devices and applications utilized by the Agents to handle the call.	**N**
Collaboration Functional Element	Functional Element that provides for collaborative communications among agents, both within and between agencies.	**N**
Dispatch System Functional Element	Functional Element used to assign appropriate resources (emergency responders) to an incident, monitor the response and relay relevant information. Tracks and logs all transactions associated with the emergency response.	**N**
Incident	From i3 definition "An Incident is a real world event, like a car crash, a heart attack, or a fire in a building."	**N**
Incident Data Exchange Functional Element	Functional Element that facilitates the exchange of Emergency Incident Data Documents (EIDDs) among other Functional Elements both within and external to an agency.	**N**
Incident Record Handling Functional Element	Functional Element responsible for creation and/or handling of Incident records.	**N**

The following New Terms and Definitions are used in this document:		
i3	The first technical specification defined by NENA for NG9-1-1, as embodied in NENA NENA-STA-010 [4].	**U**
Interactive Media Response Functional Element	Functional Element that handles audio, video and text media. Similar to an Interactive Voice Response (IVR).	**N**
Management Console Functional Element	Functional Element that supports general management functions for the PSAP. It also sends and receives Discrepancy Reports on behalf of the PSAP.	**N**
Map Database Functional Element	Functional Element that stores a set of layers obtained from a GIS system and provides a query function that returns a set of features within a defined boundary that may be used to create a map for display.	**N**
NG9-1-1 Core Services (NGCS)	The base set of services needed to process a 9-1-1 call on an ESInet. Includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network.	
NG9-1-1 PSAP	This term is used to denote a PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA NENA-STA-010 [4], and referred to therein as an "i3 PSAP".	**N**
Outgoing Alert Functional Element	Functional Element that provides interfaces that allows an Agency to provide information to emergency services personnel or entities, or to the public at large.	**N**
PSAP Incident Management	PSAP Incident Management is that portion of the incident life cycle that is processed by an individual i3 PSAP.	N

The following New Terms and Definitions are used in this document:		
PSAP Incident Record	This is the record that is used to track to the incident through the PSAP Incident Management life cycle. There may not be a PSAP Incident Record for each emergency call. May be referred to as a CAD (or Dispatch) record.	N
Responder Data Services Functional Element	Functional Element enables near real time wireless data transmissions between PSAPs and emergency responder devices. This includes transmitting dispatch information, creating new Incidents, updating active and closed Incidents. The Responder Data Services FE can support the transmission and receipt of media, or a reference (i.e. URL) to that media.	**N**
"five-nines" reliability	0005:16 minutes of downtime per year	N
Service Request	A Service Request may be any request for emergency assistance.	N
Time Server Functional Element	Functional Element that provides NTP time services to other Functional Elements.	**N**

286

3 Operational or Technical Description

This section defines a reference model for the i3 PSAP and requirements associated with them. The elements defined are functional and may or may not represent specific physical equipment. The functional elements may reside with equipment at the PSAP or may be hosted as a service.

3.1 Architecture

The ESInet, as defined in the NENA Master Glossary, is the foundation upon which an i3 PSAP is implemented. The Functional Elements (FEs) described herein are interconnected, and communicate, via this ESInet. The i3 PSAP architecture consists of these FEs, their interfaces, and the ESInet to which they are connected. This architecture must support multimedia, enabling communication with callers via voice, video, and text-based methods, as well as non-human-initiated communication with devices. The architecture allows for the FEs to be collocated, and also for the concept of the "virtual PSAP", i.e. a PSAP where personnel and the FEs do not have to be collocated.

3.1.1 Assumptions

This document assumes an i3-compliant PSAP and NGCS. This document does not cover the transitional states involved in moving to an i3 PSAP. The NENA NG9-1-1 Transition Planning Committee (NGTPC) has produced a Transition Plan [11] describing transition options and procedures.

3.1.2 Functional Elements

This document uses the concept of Functional Elements (FEs) to describe the functionality present in an i3 PSAP. A Functional Element does not correspond to a specific product or system. In fact, a product may include more than one FE. Also an FE may be offered by multiple products at the same PSAP. Also an FE does not correspond to a specific type of position at the PSAP; e.g. Telecommunicator, Dispatcher, Supervisor. Multiple FEs will be present at the same position and an FE may be present at multiple positions.

The purpose of an FE is to define a set of functions and the external interfaces to those functions that can be implemented independently. The current structure is logical and understandable and will allow the functionality to be described and assigned requirements. This document describes the i3 PSAP Functional Elements, their interfaces, and their requirements. Many of the FEs described in this document use the Emergency Incident Data Document (EIDD) [25], a proposed XML document standard, to exchange emergency incident related data.

The assignment of technical requirements to an FE through this document sets the framework to allow an FE to function as a part of an i3 PSAP. The requirements were chosen to avoid unnecessary constraints. Every effort was made to allow vendors the freedom of innovation in designing their products to be competitive in NG9-1-1 and to give PSAP management the flexibility to configure their PSAP as they choose.

Many of these requirements address interface protocols and data formats for FEs. Conforming to these requirements is essential for NG9-1-1 to operate in a plug and play fashion. A product offering

one or more FEs must meet the interface requirements for interfacing to FEs not contained in the product specified for that FE. Functional Elements interact to allow efficient processing of calls.

Figure 1shows the network reference model used in this document.

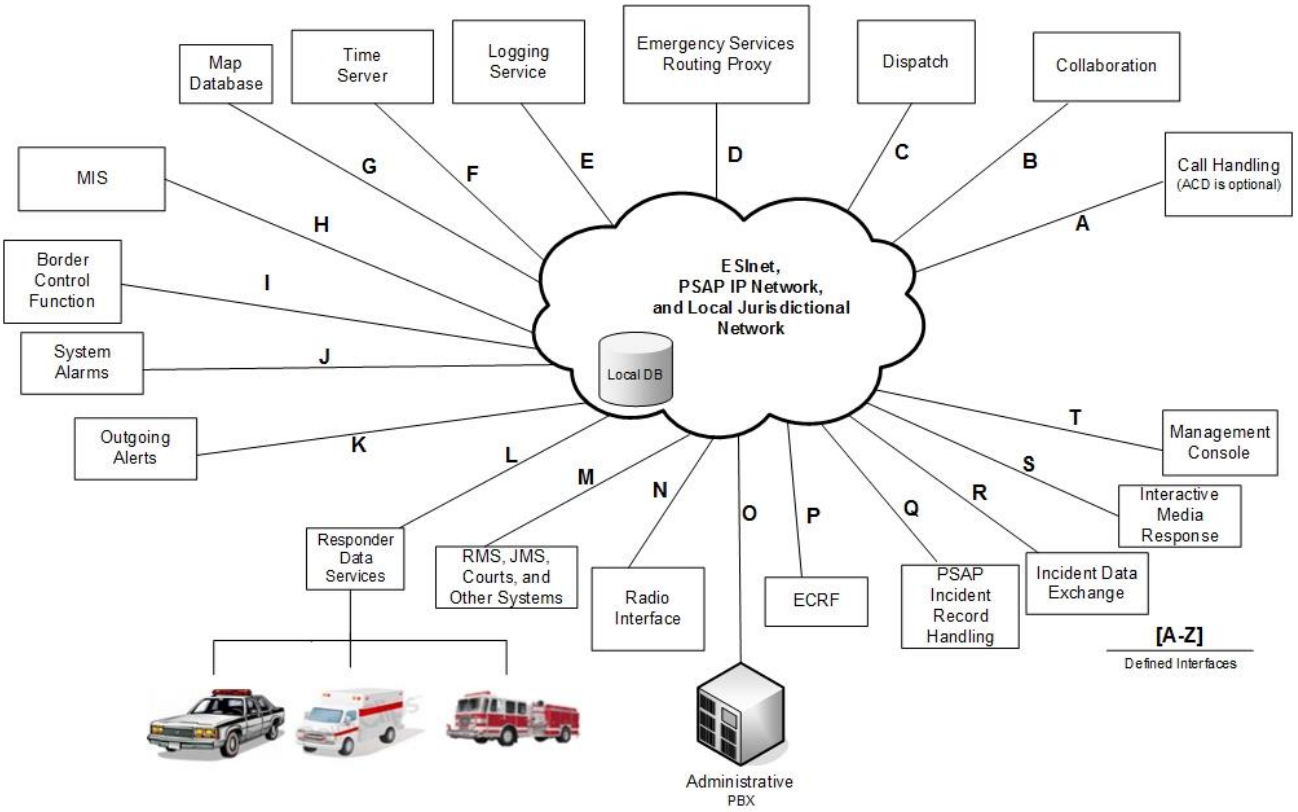

Figure 1 Functional Elements

This document uses the word "call" to refer to a session established by signaling with two way real-time media and typically involves a human making a request for help. The term also includes a one-time notification or series of data exchanges with a device such as a burglar alarm. This document sometimes uses "voice call", "video call" or "text call" when specific medium is of primary importance.

The following nomenclature is used in specifying requirements.

TOPIC XXXX-YYYY

Where

TOPIC denotes a functional area (e.g. GENERAL)

XXXX represents the top level (parent) requirement

YYYY represents the secondary level requirement. Child elements clarify or expand a parent requirement (e.g. XXXX-0100, XXXX-0101, etc.)

3.2 General Functional Element Requirements

Requirements:

GEN 0100-0100 A Product offering a Functional Element as described in this document, shall support the interfaces required for that FE, when interfacing with FEs offered by other vendors.

GEN 0200-0100 PSAP Functional Elements shall synchronize their internal clocks to the Time Server Functional Element described in Section 3.8.1.PSAP Functional Elements must maintain an accuracy of ±.25 seconds relative to the Time Server FE.

GEN 0300-0100 If an FE provides a GIS server interface, the FE must support the Spatial Information Function (SIF) server interface as described in the Spatial Information Function section of NENA-STA-010 [4].

GEN 0400-0100 If an FE provides a GIS client interface, the FE must support the SIF client interface as described in the Spatial Information Function section of NENA-STA-010 [4].

GEN 0500-0100 If an FE provides a GIS replica, the FE must support the SIF client interface as described in the SIF section of NENA-STA-010 [4].

GEN 0500-0200 If an FE provides a GIS which is used to provision other FEs, the FE must support the SIF server interface as described in the SIF section of NENA-STA-010 [4].

GEN 0600-0100 If a PSAP FE provides the MSAG conversion service, the FE must use the server-side interface as described in the MSAG Conversion Service section of NENA-STA-010 [4].

GEN 0700-0100 If a PSAP FE uses an external MSAG Conversion Service it must implement the client-side interface as described in the MSAG Conversion Service section of NENA-STA-010 [4].

GEN 0750-0100 Any FE that implements policy defined in a NENA and/or APCO standard to control its operation shall obtain such a policy from a policy store.

GEN 0800-0100 Any FE that implements a Policy Store as described in the Policy Store Web Service section of NENA-STA-010 [4] must implement the server side of the policy web service functions as described therein.

GEN 0900-0100 Any FE that interfaces to an external policy store must implement the client side of the policy web service functions as described in NENA-STA-010 [4].

GEN 1000-0100 Any FE that needs to dereference Additional Data URIs shall provide an Additional Data dereference interface as described in the Data Associated with call/caller/location/PSAP section of NENA-STA-010 [4].

GEN 1100-0100 Any FE may implement the Discrepancy Reporting client functionality to provide a convenient method for users of that FE to file a Discrepancy Report.

GEN 1200-0100 An FE may send a discrepancy report automatically if it has sufficient data available to complete the report.

GEN 1300-0100 All FEs must support emitting SNMP traps for alarm notification. The required MIBs and traps will be specified in future work.

GEN 1400-0100 Every FE must implement the notifier side of the Element State interface described in NENA-STA-010 [4].

GEN 1500-0100 Policy must control which FEs are allowed to subscribe to Element State for a particular FE.

GEN 1600-0100 FEs must support the security mechanisms defined in the Security section of NENA-STA-010 [4].

GEN 1700-0100 An FE that discovers a discrepancy must report it to the entity responsible for the data that is erroneous using the Discrepancy Reporting mechanism described in NENA-STA-010 [4].

GEN 1700-0200 Any FE that sends or receives Discrepancy Reports (defined in the Discrepancy Reporting section of NENA-STA-010 [4]) must log the report it sent or received.

GEN 1800-0100 Any FE that sends or receives Discrepancy Reports (defined in the Discrepancy Reporting section of NENA-STA-010 [4]) must send a copy of the Discrepancy Report to the Management Console.

GEN 2000-0100 Any FE must be able to discover other FEs within an Agency.

GEN 2100-0100 FEs must enforce Security mechanisms for Identity, Roles, Authentication, Authorization, and Data Rights Management, as described in the Security section of NENA-STA-010 [4].

GEN 2200-0100 An FE that determines the destination of a call or message based on the location of the caller, incident, etc. must use the ECRF to determine the route.

GEN 2300-0100 FEs that use Map Data shall be capable of obtaining data from an appropriate Map Database FE.

GEN 2500-0100 An FE that receives a PIDF-LO containing a location marked as a "default location" shall ensure that the location is treated and processed appropriately.

GEN 2600-0100 If an FE forwards a default location, the FE shall ensure that the default marking is preserved on the forwarded default location.

GEN 2700-0100 FEs that log events must do so as specified in the Logging Service section of NENA-STA-010 [4].

GEN 2800-0100 FEs that require location based routing to another Agency must use an ESRP to route a location based Service Request (selective transfer).

GEN 2900-0100 Appropriate FEs shall support a mechanism to generate a request for dispatch and to cancel the request.

GEN 3000-0100 FEs shall respond to requests for dispatch sent to them and any follow up cancellation of the requests.

GEN 3100-0100 All FEs that render or generate any media type must support the media formats required for that type. Required media formats are described in the Media section of NENA-STA-010 [4].

GEN 3300-0100 Any FE that requires access to real-time or recorded streaming media shall support retrieving such media by dereferencing a provided URL.

GEN 3400-0100 Any FE that requires access to real-time or recorded streaming media shall support RTSP (Real Time Streaming Protocol, RFC 2326 [8]) to access those media.

3.2.1 FEs Shared by Multiple Agencies must:

Requirements:

MULTI-TENANT 0100-0100 Allow each Agency to have its own policies including security policies.

MULTI-TENANT 0200-0100 Allow each Agency to control who has access to configuration data specific to that Agency.

MULTI-TENANT 0300-0100 Not allow the provisioning of an Agency to affect the provisioning of another Agency.

3.3 Policy Routing of Calls and Incidents

Within a PSAP, there are several circumstances where a call or an EIDD must be routed to one of several destinations. These destinations may be inside a PSAP (such as one of several different agency dispatchers), outside the PSAP (one of several other agencies) or a combination.

Requirements:

POLICY 0100-0100 wherever a destination for a call or an EIDD must be selected from a list of destinations based on state, load, location, and similar factors, the choice of destination must be contained within a policy. Rationale: This requirement is to constrain implementations to provide a standardized mechanism for PSAP management to control routing within the PSAP and between PSAPs much like the ESRP “Policy Routing Function” controls routing of calls in the NGCS. Implementations may provide additional routing capability, but must support the standardized mechanism.

3.4 General Topics

3.4.1 Emergency Incident Data Document

An Emergency Incident Data Document (EIDD) [25] is an XML document that is used in a structured data exchange between a source and one or more destinations regarding the current state of an incident. The current state is defined as the information known by an FE at the time that an EIDD is sent. The transmitted EIDD must contain the mandatory data elements defined in the EIDD

XML schema and one or more optional elements as dictated by the status of the incident and nature of the exchange. All of the data elements contained in the exchange must conform to the EIDD XML schema. An EIDD can be exchanged via two methods:

1. A notification EIDD is sent in response to specific triggering events. When an Agency or FE needs to communicate the current state of an incident to one or more subscribing FEs or agencies, e.g. call arrival triggers EIDD to be sent from the Call Handling FE to the PSAP Incident Record Handling FE.
2. A solicited EIDD is sent in response to a request to provide the state of a specific incident.

EIDDs are always sent to specific destinations. The destination of an EIDD is a Functional Element of a specific agency. Access to specific data is dependent upon the role/s of the intended recipient. Possible destinations for an EIDD include:

1. Other local functional elements such as dispatch, logging, RMS etc.
2. Functional Elements in external agencies such as other PSAPs, FBI, hospitals, etc.

The Incident data Exchange (IDE) FE may be used to facilitate the transmission of the EIDD. See the Incident data Exchange (IDE) FE section for further Information.

The Emergency Incident Data Document format specifications will be documented in a NENA/APCO standard based on the published NENA/APCO Emergency Incident Data Document (EIDD) informational document (NENA-INF-005).

3.4.2 Requirements for FEs sending or receiving EIDDs

Requirements:

SEND-EIDD 0100-0100 All EIDDs must be logged as specified in the Logging Service section of NENA-STA-010 [4].

SEND-EIDD 0200-0100 Whenever an EIDD is sent, a notice of the exchange must be logged.

SEND-EIDD 0300-0100 Whenever an EIDD is received, a notice of the exchange must be logged.

SEND-EIDD 0400-0100 When a relevant change in Incident information occurs, an EIDD must be sent to communicating FEs, within the constraints of any installed filter. *What constitutes a relevant change will be determined in future work.*

SEND-EIDD 0500-0100 When an agency receives a call, the first FE handling the associated Incident must send an EIDD to the logger. This requirement also applies when an Incident is communicated through some means other than a call.

SEND-EIDD 0600-0100 All EIDDs must conform to the EIDD schema.

SEND-EIDD 0700-0100 The transmission of an EIDD must comply with the data rights management policy of the agency that created the data. The data rights management policy must conform to local, state/provincial and federal laws and regulations.

SEND-EIDD 0800-0100 The Incident Data Exchange FE shall present a discoverable query point to other agencies and FEs through which incident information may be obtained regarding incidents handled by FEs registered with the Incident Data Exchange FE.

SEND-EIDD 0900-0100 The FE may respond to a request for incident information by replying with an EIDD containing data extracted from its own internal databases. The Incident Data Exchange FE may reply with an EIDD obtained by querying appropriate FEs.

SEND-EIDD 1000-0100 The FE must be able to send an EIDD to an agency based on an agency type and location using the ECRF.

SEND-EIDD 1000-0200 The FE must be able to send an EIDD to an agency based on an agency name using the Agency Locator.

SEND-EIDD 1000-0300 An FE must be able to request notifications of any new incidents, or updates to an existing incident, from an FE within an agency or the IDE of another agency.

SEND-EIDD 1000-0400 An FE must be able to request EIDDs based on data contained in an EIDD such as incident types, location, etc.

SEND-EIDD 1100-0200 The FE must implement an asynchronous notification mechanism for sending EIDDs.

SEND-EIDD 1200-0100 The FE must implement a Request-Response messaging mechanism for sending EIDDs.

SEND-EIDD 1300-0100 The FE must support sending and receiving EIDDs either by reference or by value, based on policy. When sent by value, the EIDD is transmitted in the notification or response. When sent by reference, a URI is sent in the notification or response, and the recipient may retrieve the EIDD by dereferencing the URI.

SEND-EIDD 1400-0100 The FE must be able to request that an EIDD be sent by value or by reference.

SEND-EIDD 1400-0200 The FE receiving a subscription or request for an EIDD must be able to respond with an appropriate error if the requested format (value or reference) is not acceptable per the agency policy.

SEND-EIDD 1500-0100 The FE sending an EIDD may send an EIDD by reference to those that have requested an EIDD by value if dictated by agency policy.

SEND-EIDD 1600-0100 The specification resulting from these requirements shall identify which FE(s) must populate specific component(s) of an EIDD.

3.4.3 Management Console

The Management Console supports general management functions for the PSAP, including reporting PSAP Security Posture and PSAP Service State. It also sends and receives Discrepancy Reports on behalf of the PSAP, and may implement a Policy Editor.

Requirements:

MANAGEMENT 0100-0100 The Management Console shall report the PSAP's Service State to entities inside or outside the PSAP.

MANAGEMENT 0200-0100 An interface between the Management Console FE and the Call Handling FE is required to allow the Call Handling FE to report requests for diversion and the Management Console to approve or deny such requests. Reference the Call Diversion sub-section of the PSAP Interface section in NENA-STA-010 [4].

MANAGEMENT 0300-0100 An interface between the Management Console FE and all PSAP FEs is required so those FEs can report their Element State and/or Service State to the Management Console.

MANAGEMENT 0400-0100 The Management Console must implement the Security Posture notification as described in the Security Posture section of NENA-STA-010 [4].

MANAGEMENT 0500-0100 An interface between the Management Console FE and the Call Handling FE is required to allow the Management Console FE to control whether diverted calls are accepted by the Call Handling FE, as described in the Dequeue Registration Event Package section of NENA-STA-010 [4]. The Call Handling FE is responsible for informing the Terminating ESRP of this status.

MANAGEMENT 0600-0100 The Management Console must host a Discrepancy Report Web Service for the agency as described in the Discrepancy Reporting section of NENA-STA-010 [4].

MANAGEMENT 0700-0100 The Management Console must receive discrepancy reports from sources outside and inside of the Agency.

MANAGEMENT 0800-0100 The Management Console shall support sending and receiving Status Updates and Status Update Requests as described in the Discrepancy Reporting section of NENA-STA-010 [4].

MANAGEMENT 0900-0100 The Management Console interfaces shall be discoverable.

3.5 Network Layer Functional Elements

3.5.1 i3 PSAP Network

The i3 PSAP Network may be described as an overlay network consisting of ESInets, local LANs and additional IP functionality supporting a PSAP or Jurisdiction. i3 PSAP Networks are private, managed, routed IP networks. An i3 PSAP Network serves a PSAP which is not necessarily restricted to single physical premises. That is, Agents may be located remotely from the main premises and connected to the i3 PSAP Network via IP.

While it has been common to have multiple physical networks for separate functions, this practice is strongly discouraged. Best practices in network engineering dictate that a unified, ideally redundant, physical network infrastructure is used and any necessary separation for security or functional purposes is accomplished logically in network devices. Where possible, the same configuration is encouraged in PSAP networking. Best practices in network management dictate centralized network management.

During the transition from legacy to NG networking in existing PSAPs, it is likely that multiple, limited-purpose networks will already exist. One NG transition goal should be to consolidate the legacy networks into a single network and accommodate any required separation logically. Vendors and system architects should not design products or systems that rely on single purpose networks unless no other alternatives exist. The architecture of the i3 PSAP Network must allow access to all systems that conform to the specifications stated in the network requirements section below.

Network management is responsible for setting network policy for all parts of the i3 PSAP Network, including acceptable use policies and information security. Because the i3 PSAP Network connects with many other networks and systems, much thought will need to go into network policy development. For example if connectivity to the FBI's Law Enforcement Online (LEO) databases and systems or to the National Crime Information Center (NCIC) is provided, then compliance with the FBI's Criminal Justice Information System (CJIS) security policy will have to be implemented. i3 PSAP Networks that communicate with other local, state and national networks may have to accommodate various and, possibly, conflicting network policies. APCO/NENA cannot arbitrate between various network policies; the best that APCO/NENA can do is offer guidance in best practices for the development of network policy.

Requirements:

NET 0100-0100 The i3 PSAP Network design shall adhere to the following specifications:

NENA-STA-010: Detailed Functional and Interface Standards for the NENA i3 Solution [4][1]

NENA 75-001: NENA Security for Next-Generation 9-1-1 (NG-SEC) [6]

NENA 08-506: NENA Emergency Services IP Network Design for NG9-1-1[10]

3.5.2 Emergency Call Routing Function/Location Validation Function and Emergency Services Routing Proxy Functional Elements

The ECRF/LVF and ESRP functional elements are documented in detail in NENA-STA-010 [4] and are covered here to describe how they function in the context of the PSAP.

The Call Handling FE of the PSAP uses the ESRP when making a call to another agency or transferring or conferencing an existing call outside of the PSAP. The Call Handling FE determines the intended destination of the call or transfer request, for example using the ECRF for service-and-location based routing or the Agency Locator for name based routing, and the Call Handling FE forwards the call to wherever that routing mechanism determines, which would normally be an ESRP. The ESRP will route the call, possibly through one or more intermediate ESRPs to the terminating ESRP of the ultimate destination. For example a PSAP sends a call to a fire department by querying the ECRF with the location of the incident and an appropriate Service URN such as urn:nena:service:sos.fire.

[1]specifically, the Emergency Services IP Networks section of NENA-STA-010 [4] mandates implementation of DiffServ quality of service mechanisms which must be deployed within a PSAP to maintain QoS

The ECRF and ESRP function together on the ESInet for the purpose of routing calls and other data to the correct PSAP. The ECRF provides the nominal destination for a call or other data based on the type of service needed and the location. The ESRP queries the ECRF to obtain the destination URI. The ESRP routes based on policy rules and the state of the destination. A Policy Routing Function (PRF) is used by the ESRP to apply the policy rules. A call is routed through one or more ESRPs to its final destination. See the ESRP and ECRF Sections in the NENA-STA-010 [4] document for more information.

The PSAP Call Handling FE, Incident Record Handling FE, Dispatch FE or other PSAP Services must use the ESRP to route a location based Service Request (selective transfer). Routing the request through an ESRP for any location based services allows the ESInet to take advantage of the PRF feature.

3.5.3 Border Control Function (BCF)

A BCF sits between external networks and the ESInet and between the ESInet and PSAP networks. The BCF provides a secure entry point into the PSAP from outside networks such as the ESInet. The BCF incorporates firewall and Session Border Control (SBC) functions, and may include other security functions, including functions designed to recognize and block external attacks on PSAP infrastructure.

The ESInet will provide BCF functionality between the ESInet and the outside origination networks including the Internet.

It is highly recommended that a BCF exist between the ESInet and the PSAP.

A BCF must exist between the PSAP NG9-1-1 Network and any other external networks to which it is connected. This does not imply that a virtual PSAP necessarily requires a BCF between any part of that virtual PSAP and the network that connects them together.

Refer to the NENA i3 documents 08-002 [3] and NENA-STA-010[4] for a detailed description of BCF functionality and interfaces.

3.5.4 PSAP Administrative PBX

The PSAP Administrative PBX includes telecommunication equipment that handles processing of administrative, non-emergency telephone communications. This PBX can also be integrated with other systems within the organization in order to provide additional administrative services such as email, instant messaging, voicemail and other non-emergency related processing. The administrative PBX could utilize some of the same core physical elements (including call processing and networking) as the communication equipment supporting NG9-1-1 as long as the processing of administrative tasks does not affect the performance of the emergency services.

Requirements:

PBX 0100-0100 If the PSAP Administrative PBX is involved in handling NG9-1-1 calls, then processing of administrative tasks shall not affect the performance of the emergency services.

3.5.5 Radio Interface

While an Agency's radio system and its over-the-air interface is out of scope for this document, some FEs will need to interface to the radio system. A Logging Service is expected to be able to record radio traffic. Since FEs may be located on a remote network such as the ESInet, a Radio over IP (RoIP) interface is needed. One example of such a RoIP interface is the Project 25 (P25) ISSI (Inter-RF Sub System Interface)[18]. Because ISSI only supports P25 radio systems, gateway protocols would be required to interface to the many types of legacy radio systems that will continue to be used in Public Safety. One example of such a gateway protocol is the U.S. Department of Homeland Security's Bridging Systems Interface[19]. Future support for LTE (Long Term Evolution) will also be required.

When identifying a transmission source and destination, the technology used by the radio system determines the form of address. This address could be a radio channel, a Subscriber Group [18], an IP address, a telephone number or any other form of address for a specific technology. The source and destination address information is important metadata that other interested FEs will need to receive along with the audio, video or data payload being transmitted.

Requirements:

RADIO 0100-0100 The Radio Interface shall support transmitting audio, video and text (both two-way interactive and streaming), and associated metadata to and from a radio system and other FEs. Note: Not every radio system will support all forms of media.

RADIO 0200-0100 The Radio Interface shall support a mechanism for other FEs to register for specific addresses that it wishes to receive traffic from.

RADIO 0300-0100 The Radio Interface shall support a mechanism for other FEs to specify an address that it wishes to send traffic to.

RADIO 0400-0100 The Radio Interface shall support authentication and authorization of client FEs that wish to use supported radio system features.

RADIO 0500-0100 The Radio Interface shall support privacy and message integrity of all traffic.

RADIO 0700-0100 The Radio Interface shall support bridging of emergency and other calls to the radio

3.6 Communications Functional Elements

These functional elements are involved in communications and call handling.

3.6.1 Call Handling

The Call Handling Functional Element is concerned with the details of the management of calls. It handles all communication from the caller. It includes the interfaces, devices and applications utilized by the Agents to handle the call. It receives and may display the content of multimedia calls such as text and video to the Agent.

3.6.1.1 Receiving Calls

Requirements:

CALL 0100-0100 The Call Handling FE shall deploy the SIP call interface as defined in the SIP Call sub-section of the Interfaces section in NENA-STA-010 [4].

CALL 0200-0100 The Call Handling FE shall accept the location specified in the Geolocation Header or within an EIDD in the SIP message.

CALL 0300-0100 If a call is received with location by reference, the Call Handling FE shall use the reference to retrieve (dereference) the location via HELD or SIP per NENA-STA-010 [4].

CALL 0400-0100 The i3 PSAP shall be able to receive and display either geo or civic information received in the PIDF-LO.

CALL 0500-0100 The location reference, if received, may also be used for subsequent location updates.

CALL 0600-0100 Call Handling FE shall implement at least one incoming call queue [as defined in NENA-STA-010 [4].

CALL 0700-0100 The Call Handling FE shall support the QueueState notification function for its queues so it can notify as described in the QueueState Event Package section of NENA-STA-010 [4].

CALL 0800-0100 The Call Handling FE may support the QueueState Subscribe function for downstream queues in other elements as described in the QueueState Event Package section of NENA-STA-010 [4].

CALL 0900-0100 The Call Handling FE shall subscribe to the Management Console's Service State so that the Call Handling FE's QueueState can be changed to the state dictated by local policy whenever the PSAP's Service State has changed.

CALL 1000-0100 The Call Handling FE shall support the dequeue registration function as described in the DequeueRegistration Event Package section of NENA-STA-010 [4].

CALL 1100-0100 In order to support call diversion for other PSAPs in overload conditions, the Call Handling FE shall support the dequeue function with standby flag set to true as described in the DequeueRegistration Event Package section of NENA-STA-010 [4].

CALL 1200-0100 The Call Handling FE shall provide an interface to the Management Console to support standby diversion as described in the DequeueRegistration Event Package section of NENA-STA-010 [4].

CALL 1300-0100 The Call Handling FE must support Non-Human-Initiated calls as defined in NENA-STA-010 [4].

3.6.1.2 Processing Calls

Requirements:

CALL 1400-0100 An optional Automatic Call Distribution function may be used to distribute calls to appropriate Agent Positions.

CALL 1500-0100 Routing to the appropriate Agent may use any available information in the signaling message, for example language preference.

CALL 1600-0100If the i3 PSAP receives a call request and all Agents are busy, it may return a "486 busy here" indication. The PSAP may invoke alternative call treatment based upon local procedures.

CALL 1700-0100 If the Call Handling FE detects call abandonment, the Call Handling FE should have the capability to display the call data to an Agent.

CALL 1800-0100 If an emergency call has been alternate routed from a PSAP, the Call Handling FE will receive indication of call rerouting, and shall be able to handle this indication.

CALL 1900-0100 If an i3 PSAP is designated as the default PSAP it may receive the call request with a default location. This i3 PSAP shall process the call as a normal emergency call.

CALL 2000-0100 Additional data about a call, caller or location may be retrieved using the processes described in the "Data Associated with call/caller/location/PSAP" section of NENA-STA-010 [4].

CALL 2100-0100 The Call Handling FE shall provide an Additional Data dereference interface as described in the Data Associated with call/caller/location/EIDD section of NENA-STA-010 [4].

CALL 2200-0100 The Call Handling FE shall implement the LoST client interface as defined in the "LoST" subsection of the "Interfaces" section of NENA-STA-010 [4] to interact with the ECRF and LVF FEs.

CALL 2300-0100 The Call Handling FE shall implement the HELD interface to query the LIS FE to obtain the current location for a call.

CALL 2400-0100 The Call Handling FE shall implement the SIP Presence Event Package interface to obtain the current location for a call.

CALL 2500-0100 The Call Handling FE shall dereference the location sent by reference for all calls.

CALL 2600-0100 The Call handling FE shall provide a standardized interface to allow an authorized agent to barge into the call.

CALL 2700-0100 The Call handling FE shall provide a standardized interface to allow an authorized agent to monitor a call in a listen-only mode.

CALL 2800-0100 If the Call Handling FE is used to clear an Incident, the Call Handling FE shall initiate logging of a ClearIncident LogEvent to the Logging Service as specified in the Logging Service section of NENA-STA-010 [4].

CALL 2910-0100 The Call Handling FE shall implement the test call function capability as described in the Test Calls section of NENA-STA-010 [4].

3.6.1.3 Call Hold and Park

Requirements:

CALL 3000-0100 A form of call Hold functionality shall be provided.

CALL 3100-0100 Placing an emergency call "on hold" or muting or park shall not interrupt recording of the caller's media and recording of any media (e.g. from an Announcement Server) sent to the Caller.

Rationale: In NG9-1-1, because a SIP "Hold" function results in disconnected media by design, the SIP one-way or two-way mute mechanism in NG9-1-1 replaces what is referred to as "Call Hold" in legacy PSTN systems.

CALL 3200-100 The legacy feature known as park or Non-Exclusive Hold in legacy systems shall be supported in some to-be-specified form.

Rationale: Emergency calls that are intended for transfer to a call-taker that is not yet available, can be temporarily parked. Unlike an exclusive Hold, a call shall be able to be suspended in a state where any authorized agent can retrieve it.

CALL 3300-100 Both sides of one-way, as well as two-way, mute capabilities (i.e. not rendering the media of a party) for all NG9-1-1 emergency media shall be supported.

3.6.1.4 State Management

Requirements:

CALL 3400-0100 The Call Handling FE must report its state to subscribing FEs. (A registry of appropriate Call Handling FE states will be required).

CALL 3500-0100 The Call Handling FE shall be able to subscribe to ESRP notify events occurring within the NG9-1-1 routing network. For example, an element in the NG9-1-1 routing network may have changes in routing conditions of which it needs to notify the PSAP.

CALL 3600-0100 The Call Handling FE shall report the PSAP Element State as defined in the "Element State" section of NENA-STA-010 [4] to the Terminating ESRP.

CALL 3700-0100 The Call Handling FE shall have an interface to the Management Console that will allow the Management Console to influence the PSAP Element State value.

CALL 3800-0100 The state of the individual agents shall be reported to the Management Console by the Call Handling FE.

CALL 3900-0100 The Call Handling FE shall support all the options listed in the NENA-STA-010 [4] section titled "Transfer Involving Devices Not Supporting Replaces". Provisioning of the Call Handling FE shall be able to select one of these options.

3.6.1.5 Bridging Calls

Calls may be bridged between i3 PSAPs or between an i3 PSAP and a legacy PSAP. An i3 PSAP must not have to know if the destination PSAP is IP or legacy. Bridging capabilities can be mediated by the ESInet. These requirements are divided into receiving calls that have been bridged and establishing a bridge. SIP parameters will denote that the call has been redirected (bridged) from another i3 PSAP or legacy PSAP. See the Bridging section of NENA-STA-010 [4] for more information.

Requirements:

BRIDGE 0100-0100 The Call handling FE must provide the functionality allowing the Agent to have a side bar conversation with others without the calling party hearing the conversation.

3.6.1.6 Receiving Bridged Calls

Requirements for receiving an initial call apply to receiving bridged calls.

Requirements:

BRIDGE-IN 0100-0100 When an i3 PSAP is bridged into a 9-1-1 call the receiving PSAP must have the ability to receive all of the data that the initial PSAP sends, including location, etc. This information will be found in the EIDD embedded or referenced in the received INVITE message as described in the Bridging section of NENA-STA-010 [4].

BRIDGE-IN 0200-0100 The Bridge FE shall support all the options listed in the NENA-STA-010 [4] section titled "Transfer Involving Devices Not Supporting Replaces". Provisioning of the Bridge FE shall be able to select one of these options.

3.6.1.7 Originating Bridged Calls

A PSAP Agent may need to add on another PSAP or authorized agency. The destination may be either another i3 PSAP or a legacy PSAP.

Requirements:

BRIDGE-OUT 0100-0100 The Call Handling FE must have the ability to establish a bridge to one or more NG9-1-1 entities or legacy (e.g., PSTN) entities.

BRIDGE-OUT 0200-0100 When a i3 PSAP initiates a bridge it shall transmit all of the data that it knows.

BRIDGE-OUT 0300-0100 The bridge signaling for calls shall include the PSAP identifier of the originating PSAP. See NENA-STA-010 [4] for more information.

BRIDGE-OUT 0400-0100 When an emergency call is bridged, the Call Handling FE shall make available the location or location reference information in the bridge signaling that was received in the original emergency call plus Additional Data references per local policy. See the "Passing data to Agencies via bridging" section of NENA-STA-010 [4].

BRIDGE-OUT 0500-0100 When an emergency call is bridged, the Call Handling FE may pass the local notes collected during interactions with the caller in an EIDD passed in the signaling as defined in NENA-STA-010 [4].

BRIDGE-OUT 0600-0100 The i3 PSAP may implement a transfer (bridge) function based upon the location of the caller and classification of the call, e.g. to police, fire, EMS or other authorized agencies.

BRIDGE-OUT 0700-0100 The Call Handling FE shall support using the ECRF to determine the route to the appropriate agency.

BRIDGE-OUT 0800-0100 The Call Handling FE shall use the Incident location and proper service identifier (eg. urn:nena:service:responder.police) to query the ECRF in order to determine the agency to which the call should be bridged.

BRIDGE-OUT 0900-0100 The Call Handling FE shall support using a URI to initiate a bridge, the URI being obtained from the ECRF or from a local database.

BRIDGE-OUT 1000-0100 The i3 PSAP shall have the capability to drop from the bridge without terminating the bridge.

BRIDGE-OUT 1100-0100 The Call Handling FE shall support the capability to blind or attended transfer a call to another Agent, PSAP or authorized agency. Attended transfer uses the "Bridging" and related sections of NENA-STA-010 [4].

BRIDGE-OUT 1200-0100 On a transfer, the Call Handling FE may provide ancillary supplemental information collected during the dialogue with the caller (e.g. Agent notes).

3.6.1.8 Bridge Floor Management

It is desirable for the i3 PSAP Agent that initiated the bridge to have control of the bridge and of the parties on the bridge. This may include adding parties, dropping parties, muting parties, etc. Supervisory barge-in and monitoring may also involve the bridge. Refer to the Bridging section of NENA-STA-010 [4] for information on bridging parties who are external to the PSAP.

Requirements:

FLOOR 0100-0100 When an NG9-1-1 Call Handling FE initiates a bridge it shall transmit all of the data that the PSAP's policy allows.

FLOOR 0200-0100 The Call Handling FE must support the capability to add parties to the bridge.

FLOOR 0300-0100 The Call Handling FE must support the capability to selectively drop parties from the bridge.

FLOOR 0400-0100 The Call Handling FE must support the capability to selectively mute parties on the bridge.

FLOOR 0500-0100 The Call Handling FE shall have the capability to allow parties on the bridge to converse without another party's knowledge.

FLOOR 0600-0100 The Call Handling FE must support the ability for an authorized supervisor to barge into the call.

FLOOR 0700-0100 The Call Handling FE must support the ability for an authorized supervisor to monitor the call without the other parties' awareness.

FLOOR 0800-0100 The Call Handling FE (or the bridge acting on its behalf) must log an event to the Logging Service denoting that someone has initiated monitoring of the call.

FLOOR 0900-0100 Call Handling FEs on the bridge should be notified of status of other parties on the bridge. See Bridging section of NENA-STA-010 [4] for more information.

FLOOR 1000-0101 The notification capability shall be configurable such that notification of certain parties' (e.g. supervisors) presence is not notified to other parties on the bridge.

3.6.1.9 Media

Requirements:

MEDIA 0100-0100 The Call Handling FE shall support the media requirements in the Media Section of NENA-STA-010 [4].

3.6.1.10 Callback

Requirements:

CALLBACK 0100-0100 The Call Handling FE must support immediate call backs to the original callers specified in NENA-STA-010 [4].

CALLBACK 0200-0100 The Call Handling FE must be able to support non-immediate call back to the original caller after call termination, as specified in NENA-STA-010 [4].

3.6.1.11 TTY/TDD

TTY is a teletypewriter, aka TDD or Telecommunications Device for the Deaf, Hard-of-Hearing and speech impaired.TTY/TDD is part of the Call Handling Functional Element. The term 'TDD' means a Telecommunications Device for the Deaf, which is a machine that employs graphic communication in the transmission of coded signals through a wire or radio communication system.

TTY/TDD devices are rapidly being replaced by newer technology for normal communications among the hearing and speech impaired. As long as TTY/TDD devices are used they must be supported in the NG9-1-1 system. The TTY/TDD call consists of a series of analog tones representing characters encoded in either Baudot or TN1663 (old Bell-103), commonly known as ASCII TTY encoding. Characters are received one at a time and displayed on receipt.TTY is a form of “Real Time Text (RTT)” as opposed to messaging, which usually is sent and displayed a line at a time. Real time text is more interactive, but requires that both ends maintain state to deal with erasures.

Carrying TTY tones reliably through IP networks may be difficult. Consequently, the transcoding (conversion of Baudot/ASCII tones to RFC 4103 [12]) may have to be done at entry to the ESInet. ESInets can be engineered to transport TTY reliably or they must provide transcoding at the entrance to the network. The PSAP network must also be engineered to transport TTY reliably, provide transcoding at the entrance to the network or the ESInet to which it is connected must transcode the TTY tones before presentation to the PSAP.

The PSAP must support a caller using a TTY device using one of the following methods:

1. The Call Handling FE must be able to accept Baudot and display as text. If the ESInet does not provide transcoding the PSAP portion of the ESInet must be engineered to transport TTY reliably.
2. The PSAP must have a transcoder from Baudot to RFC 4103 [12] at the entrance of the network. The Call Handling FE must be able to accept RFC 4103 [12] and display as text.
3. The ESInet and all other sources of calls to the PSAP must only present RFC 4103 [12] RTT to the PSAP. This implies that all TTY calls must be transcoded (Baudot to RFC 4103 [12])

before presentation to the PSAP. The Call Handling FE must be able to accept RFC 4103 [12] and display as text.

Requirements:

TTY 0100-0100The Call Handling FE must implement option 1 above.

TTY 0200-0100 The Call Handling FE and any other SIP User Agent must support receiving and displaying RFC 4103 [12] Real Time Text.

TTY 0300-0100 The TTY transcoder in the Call Handling FE must conform to section TTY (Baudot tones) of NENA-STA-010 [4]

3.6.2 Outgoing Alert Functional Element

An optional Outgoing Alert FE provides interfaces that allow an Agency to provide some information to emergency services personnel or entities, or to the public at large. Present methods for alerting interested parties to emergencies and other events that may affect them currently use proprietary mechanisms and have limited capabilities. These requirements seek to standardize interfaces to alerting systems and provide improved capabilities for local governments to issue alerts.

In these requirements the term Notifier is the authority issuing the alert and the term Distributor is the system distributing the alert to targeted endpoints. The Authority to Citizen Outgoing Alert Functional Element provides a standardized interface that allows a Notifier to communicate an alert to a Distributor, and a Distributor to communicate the status of the alert back to the Notifier.

Requirements:

OUTGOINGALERT 0100-0100 There shall be a standardized interface between the Notifier and one or more Distributors (entities, typically outside the ESInet, that deliver alerts to targeted devices).

OUTGOINGALERT 0200-0100 The interface shall use the Common Alerting Protocol (CAP) [20].

OUTGOINGALERT 0300-0100 A transport mechanism for CAP shall be specified.

OUTGOINGALERT 04000-100- The Notifier shall be able to select Distributors.

OUTGOINGALERT 0500-0100 The Notifier shall be able to classify targeted devices into groups and to specify which groups are to receive the alert.

OUTGOINGALERT 0600-0100 An acknowledgment mechanism shall be specified for the Distributor to inform the notifier that the alert has been distributed.

OUTGOINGALERT 0700-0100 The interface shall be compatible with IPAWS-OPEN [21] such that alerts may be sent through IPAWS-OPEN to existing distribution mechanisms.

OUTGOINGALERT 0800-0100 Interface shall support specification of distribution by affected area (geo-targeting), pre-determined groups, opt-in and opt-out (including opt-in to a geo-targeted alert using a supplied location), or any combination of these options. This requirement does not impose requirements on any given Distributor to allow all such targeting options.

OUTGOINGALERT 0900-0100 The Outgoing Alert Functional Element shall provide a mechanism to manage a list of Distributors.

OUTGOINGALERT 1000-0100 The Outgoing Alert Functional Element shall support receiving EIDDs in order to provide information about a notification.

OUTGOINGALERT 1100-0100 The Outgoing Alert Functional Element shall log alerts sent and acknowledgement received.

OUTGOINGALERT 1200-0100 There shall be a unique identifier assigned to a notification request.

OUTGOINGALERT 1300-0100 The unique identifier shall accompany all requests and acknowledgements.

OUTGOINGALERT 1400-0100 To support alerts to emergency services personnel or entities, an acknowledgment mechanism shall be provided that allows a Distributor to inform the Notifier that an alert has been acknowledged by an individual target.

3.6.3 Physical Considerations

The physical considerations for a NG-PSAP are similar to those of any facility of a similar size hosting computing and networking equipment.

Requirements:

PHYS 0100–0100 For the physical environmental requirements, please refer to NENA 04-001(Recommended Generic Standards for E9-1-1 PSAP Equipment) [5] section 7 (Physical and Electrical Environment Requirements).

PHYS 0200–0100 For the installation and maintenance requirements, please refer to NENA 04-001 (Recommended Generic Standards for E9-1-1 PSAP Equipment)[5] section 8 (Installation, Maintenance, and Administration).

PHYS 0300-0100 For PSAP site characteristics, please refer to NENA 04-502 (E9-1-1 PSAP CPE Site Characteristics Technical Information Document [26].

3.6.4 System Alarms

Many elements and systems need to notify internal and external entities of errors, failures, or other conditions of interest. A mechanism must be provided to support these “alarms”.

Requirements:

ALARM 0100-0100 Any equipment (alarm sender) shall provide the ability to notify the appropriate personnel (alarm receiver) of its status.

ALARM 0200-0100 A standardized interface shall be specified between the alarm sender and the alarm receiver.

ALARM 0300-0100 The alarm mechanism shall fail-safe such that both ends shall know that the alarm mechanism has failed.

ALARM 0400-0100 Alarm sender shall be able to send status to multiple alarm receivers.

3.6.5 Quality and Reliability

While Next Generation 9-1-1 systems have the same need for reliability as traditional 9-1-1 systems, the NG9-1-1 architecture provides more flexibility to achieve the necessary reliability. Traditional metrics such as five-nines and other carrier-grade measures of reliability are still relevant and can be used; however, the resiliency that is inherent in an IP-based platform lends itself to looking at the reliability of the entire call process, rather than component-by-component. Common statistical process control methods are an appropriate way to measure both quality and reliability of entire processes, such as NG9-1-1 call handling.

Traditional Telco-based 9-1-1 systems have used carrier grade reliability standards, calling for individual components built to "five-nines" reliability standards (5.26 minutes of downtime per year), often deployed in redundant pairs. Equipment is housed in special facilities that have robust power and sophisticated environmental controls. While this approach to ensuring availability is valid, it does come at a cost that can be avoided with a properly engineered IP-based system.

Five-nines reliability in IP-based systems, such as NG9-1-1, is typically achieved by having more than two redundant components, with each component having less reliability than five-nines with less robust power and less sophisticated environmental controls. In this context a PSAP can be considered a component. An individual PSAP is not required to have five-nines reliability. Rather than redundant components in a PSAP, a 9-1-1 Agency can opt to have calls flow to backup PSAPs to provide the required redundancy. In the context of providing a service such as NG9-1-1, call handling reliability should be defined by an SLA.

A 9-1-1 call meets its SLA if the Agent and caller can effectively communicate with each other, all the relevant information is exchanged, and the call-taker can efficiently transfer the incident to the appropriate responding agency. Note that in some cases the caller or call handler may not be a person, but rather some sort of automated system.

Any system anomaly that prevents the caller, call handler, and/or responding agency from effectively communicating should be considered a defect. For example, a call which cannot be answered at one PSAP because of a system problem is not necessarily a defect if a properly designed system allows the call to roll over to another PSAP, where it is properly handled. On the other hand, a call delivered to a call handler that lacks location information, or has severe echo or delay to the degree that the parties have difficulty understanding each other should be considered a defect.

By viewing a 9-1-1 system in this manner, system designers and administrators have a great degree of latitude to leverage the capabilities offered by an IP platform, while being able to ensure that the system maintains the highest standards of availability.

3.6.6 Security

Requirements:

SEC 0100-0100 i3 PSAPs shall adhere to security standards defined in the Security section of NENA-STA-010 [4].

SEC 0200-0100 i3 PSAPs should adhere to the recommendations in NENA 75-001[6].

3.6.7 Interactive Media Response FE

Requirements:

IMR 0100-0100 The Interactive Media Response (IMR) FE is similar to an Interactive Voice Response (IVR) unit, but it handles audio, video and text media. The IMR FE must conform to the requirements in the Interactive Media Response section of NENA-STA-010 [4].

IMR 0200-0100 In order to support call diversion in PSAP overload conditions, the Interactive Media Response FE must support the dequeue function for queues from other PSAPs described in the Dequeue Registration Event Package section of NENA-STA-010 [4].

IMR 0300-0100 In order to enable management control of diversion, an interface between the Interactive Media Response FE and the Management Console would be required.

3.7 Incident Application Service Layer Functional Elements

3.7.1 PSAP Incident Record Handling Functional Element

The PSAP Incident Record Handling FE's responsibility starts immediately after the call is answered. When the call is an NG9-1-1 call, it will be accompanied by a unique Incident Tracking Identifier which is used to track the Incident throughout its lifecycle. If the emergency call is received from a source other than the NG9-1-1 system, such as a non-emergency (7 or 10-digit) call or radio communication, the Incident Record Handling FE must assign a unique Incident Tracking Identifier. Not all emergency calls will trigger the creation of an Incident Record.

The Incident Record Handling FE should automatically populate the Incident screen with supporting information such as caller name, address, and phone number. The Agent will have the ability to edit the data, add comments and other data obtained from the caller. This FE's functionality makes it possible for the Agent to determine if the call is representative of a new Incident or if it is an additional call for an existing Incident. This FE creates the PSAP Incident Record, or, updates existing PSAP Incident Records. The Incident Record Handling FE may submit location information to the Map Display FE to display the caller's location on a map.

The Incident Record Handling FE indicates the presence of Additional Data to the Agent and allows the Telecomunicator to view it upon request. Additional Data may include text, imagery and video.

The Incident Record Handling FE assists the Telecomunicator in selecting the type of responding services that are needed. The specific responding agencies to be alerted may be determined internally or by querying the Emergency Call Routing Function FE. The ECRF FE may be located within the PSAP or hosted in the network.

In some cases the call itself is transferred to the selected agency with all associated data. The PSAP Incident Record Handling FE alerts the selected responding agencies by initiating an Emergency Incident Data Document (EIDD) or by using another internal mechanism.

Requirements:

INCIDENT-HANDLING 0100-0100 When an Incident Record is created, the PSAP Incident Record Handling FE shall provide Emergency Incident Data Documents (EIDDs) to authorized destinations.

INCIDENT-HANDLING 0200-0100 The PSAP Incident Record Handling FE shall provide EIDDs when a relevant change to an incident occurs.

INCIDENT-HANDLING 0300-0100 The PSAP Incident Record Handling FE must subscribe for EIDD updates from the Call Handling FE

INCIDENT-HANDLING 0400-0100 The PSAP Incident Record Handling FE should be capable of rendering multimedia including audio, video, imagery and text.

INCIDENT-HANDLING 0600-0100 The PSAP Incident Record Handling FE may support automatic Alarm notifications using the APCO/CSAA ANS 2.101.1-2008 Automated Secure Alarm Protocol [13] alarm standard.

INCIDENT-HANDLING 0800-0100 The PSAP Incident Record Handling FE shall support manually entered locations.

INCIDENT-HANDLING 0900-0100 The PSAP Incident Record Handling FE shall implement the LoST client interface as defined in the "LoST" subsection of the "Interfaces" section of NENA-STA-010 [4] to interact with the ECRF and LVF FEs if an internal mechanism is not available.[2][3]

INCIDENT-HANDLING 1000-0100 If the Incident Tracking Identifier is assigned by the PSAP Incident Record Handling FE then it must use the format for the incident number standard as defined in the Identifiers section of NENA-STA-010 [4],

INCIDENT-HANDLING 1100-0100 If the call is determined to be associated with a previous Incident, the current and prior Incidents shall be merged as described in the Logging Service section of NENA-STA-010 [4].

INCIDENT-HANDLING 1200-0100 Once a merge has been performed with a prior Incident Tracking Identifier, the prior Incident Tracking identifier shall be used from that point forward.

INCIDENT-HANDLING 1300-0100 If it is determined that an incident must be split, then a copy of the Incident Record shall be made and a new Incident Tracking Identifier assigned.

INCIDENT-HANDLING 1400-0100 If the call is determined to be sufficiently related to a previous Incident, the current and prior Incidents shall be linked as described in the Logging Service section of NENA-STA-010 [4].

INCIDENT-HANDLING 1500-0100 The Incident Record Handling FE must be able to obtain the current and updated location for a call.

INCIDENT-HANDLING 1500-0101 The Incident Record Handling FE shall implement the HELD interface to query the LIS FE for this purpose.

[2] Note: This is required in the case there is no call associated with the incident in which case no ECRF lookup would have been done

[3] Note: An internal mechanism would require access to a master or replica GIS system. If no internal mechanism is available, the ECRF/LVF FEs would be used by the Incident Record Handling FE to determine the correct service for the given incident location.

INCIDENT-HANDLING 1500-0102The Incident Record Handling FE shall implement the SIP Presence Event Package interface to query for current location.

INCIDENT-HANDLING 1600-0100 If the Incident Record Handling FE is used to close an Incident, the Incident Record Handling FE shall initiate logging of a ClearIncident LogEvent to the Logging Service as specified in the Logging Service section of NENA-STA-010 [4].

3.7.2 Map Database Functional Element Description

The Map Database FE stores a set of layers obtained from a GIS system and provides a query function that returns a subset of the data within a defined boundary specified in the view. The Map Database FE could be a standalone element, in which case it is provisioned from authoritative GIS systems and provides the view query server interface to an external Map Display. It could also be integrated into a GIS (meaning the GIS system provides the view query server interface). Map Data, as used herein can include geospatial features, photographic, and topographical data for display.

Note: A client queries the Map Database FE to obtain a view and generates user interfaces of this view, together with other information obtained from sources such as EIDDs.

Requirements:

MAPPING 0100-0100 The Map Database must contain a set of GIS layers that replicate authoritative layers maintained in a GIS system.

MAPPING 0200-0100 The layers supported by the Map Database must include, but are not limited to, the layers defined by NENA-STA-006 [24].

MAPPING 0300-0100 The provisioning interface for the Map Database shall be the Spatial Information Function (SIF) interface defined in NENA-STA-010 [4].

MAPPING 0400-0100 The query interface shall accept a view definition such as specification of a rectangle, an address or a point with radius, and return the set of features from a subset of the layers in the database bounded by the query parameters.

MAPPING 0500-0100 The query interface shall have a method for specifying which layers are returned.

MAPPING 0600-0100 There shall be a mechanism by which a client can discover the mapping database that serves a specific location.

3.7.3 Management Information System (MIS)

The MIS Functional Element provides reporting services based on data collected from FEs. The types of collected data may include:

- Communications processing data generated by Functional Elements.
- Authentication, authorization, and data access events from other FEs.
- Call and Incident object state change information.

The reports generated are used to analyze statistics for management purposes.

Requirements:

MIS 0300-0100 The MIS FE must support the LogEvent client interface to retrieve LogEvents from one or more Logging Services as defined in NENA-STA-010 [4].

MIS 0400-0100 The MIS FE may support the LogEvent server interface to receive LogEvents as defined in NENA-STA-010 [4].

3.7.4 Dispatch System Functional Element

The Dispatch FE is considered core functionality and is critical for ensuring effective responses to Emergency Events. The primary function of the Dispatch System Functional Element (Dispatch FE) is to:

- Identify appropriate resources (emergency responders) to assign to an Incident
- Dispatch assigned emergency responders to the location of an Incident
- Monitor the response and dispatch additional responders as required
- Relay relevant information to emergency responders
- Track/log all transactions associated with the emergency response

The Dispatch FE also assists in managing emergency resources within its geographic area. It tracks the real-time statuses and locations of emergency resources. It provides relevant information for management and other reports on resource deployment, specific incidents and other data.

The Dispatch FE can be configured for one or more emergency service types (e.g., EMS, Fire, Law Enforcement, and various combinations of these service types).Dispatch FEs assist both primary and secondary PSAPS with the processing and management of emergency events and resources.

Computer Aided Dispatch (CAD) systems have traditionally provided an integrated solution (application) for handling both the dispatch function and the PSAP Incident creation function associated with an emergency call. The NG9-1-1 design decouples these two functions and specifies the requirements of each function along with the required interfaces between them. In NG9-1-1 the PSAP Incident Record Handling FE, which is the traditional CAD call taking function and the Dispatch FE may be located at completely unrelated sites and possibly in different regions or states. As such, the requirements of these two functions are discussed separately in this document.

The requirements for the Dispatch FE and PSAP Incident Record Handling FE are documented separately within this document. A solution that combines both of these functions and others into a single application (i.e., a CAD system) may be appropriate and implementation of this type of multifunctional solution is entirely at the discretion of local PSAPs. In many cases the call taking (Call Handling and PSAP Incident Record Handling) and Dispatch functions may be handled by one or more operators located at a single facility or even at single workstation. The products providing this functionality may be provided by multiple vendors or a single vendor.

It is beyond the scope of this document to fully describe all of the technical functionality of Dispatch FEs used in NG9-1-1 compliant communication centers. This document concentrates on specific Dispatch FE requirements that are related to NG9-1-1 technology and processes. For a complete

listing of functions see the dispatch section of the APCO International and IJIS Institute Unified Computer-Aided Dispatch Functional Requirements (UCADFR) [22],

Requirements:

DISPATCH 0100-0100 The Dispatch FE should support the relevant requirements contained in the dispatch section of the APCO International and IJIS Institute Unified Computer-Aided Dispatch Functional Requirements (UCADFR) [22].

DISPATCH 0200-0100 The Dispatch FE shall receive requests for service at its registered URL or URI.

DISPATCH 0300-0100 The Dispatch FE shall support the exchange of Emergency Incident Data Documents (EIDD) with other FEs as a mechanism for obtaining initial and updated emergency event information.

DISPATCH 0400-0100 The Dispatch FE shall support the transfer of Incident data to the registered URL/URI of other FEs through the exchange of EIDDs.

DISPATCH 0500-0100 The Dispatch FE shall support the transfer of updated Incident data to the URL/URI of other FEs through the exchange of EIDDs.

DISPATCH 0600-0100 The Dispatch FE shall be able to automatically transfer and update RMS systems with Incident data through the exchange of EIDDs.

DISPATCH 0700-0100 The Dispatch FE shall provide a mechanism for updating an Incident based on information provided by emergency responders.

DISPATCH 0800-0100 The Dispatch FE shall provide a mechanism for modifying the location of emergency events based on information provided by emergency responders.

DISPATCH 0900-0100 The Dispatch FE shall support a mechanism for determining the responsible agencies for handling emergency events whose location has changed.

DISPATCH 1000-0100 The Dispatch FE may support an interface to Map Display FE.

DISPATCH 1100-0100 The Dispatch FE shall support merging of Incidents as defined in the Logging Service section of NENA 08 003.

DISPATCH 1200-0100 The Dispatch FE shall support undoing an Incident merge operation.

DISPATCH 1300-0100 The Dispatch FE should support cloning or splitting of existing Incidents.

DISPATCH 1400-0100The Dispatch FE should support replicating of Incident data when undoing a merge, or doing a split/clone operation on an Incident.

DISPATCH 1600-0100 The Dispatch FE shall post all transactions related to an Incident to the Logging Service using its WEB Service interface.

DISPATCH 2000-0100 Dispatch FE shall implement the LoST client interface as defined in the "LoST" subsection of the "Interfaces" section of NENA-STA-010 [4] to interact with the ECRF and LVF FEs if an internal mechanism is not available[4].

DISPATCH 2100-0100 The Dispatch FE shall support obtaining updated locations for a call.

DISPATCH 2100-0101 The Dispatch FE must implement the HELD interface to query the LIS FE for this purpose.

DISPATCH 2100-0102 The Dispatch FE must implement the SIP Presence Event Package interface to query the LIS FE for this purpose.

DISPATCH 2200-0100 If the Dispatch FE is used to close an Incident, the Dispatch FE shall initiate logging of a ClearIncident LogEvent to the Logging Service as specified in the Logging Service section of NENA-STA-010 [4].

3.7.5 Records Management System (RMS) Interface

Public Safety Records Management Systems (RMS) are often interfaced to public safety communication centers. RMSs are sometimes accessed directly through computer systems deployed within communication centers for research and analysis purposes. This section of the TRD describes the interface requirements between public safety RMSs and NG9-1-1 FEs.

The RMS interface requirements support the following general categories:

A. Emergency Incident Information exchanges – Information about in-progress and completed incidents are often transmitted from communication centers to the RMSs of agencies involved in the incidents. The transferred information is used as the basis for follow-up agency reports and for statistical and other types of analysis.

B. Queries and responses – information relevant to in-progress emergency incidents such as premise information, alarms, caution flags and previous history is often available within RMSs. Queries from NG9-1-1 compliant FEs along with appropriate RMS responses should be supported by the interface. An FE may request a case number for an emergency Incident from RMS or RMS may request a case number from an FE.

C. Staffing assignment transfers – staffing information for emergency responders and sometimes for the communication center may be stored in an RMS. Transferring staffing information from an RMS to appropriate NG9-1-1 FEs should be supported by the interface.

Records management systems contain highly confidential information such as criminal activity, ongoing investigations, personal medical data, and the location of valuable items and other confidential information. The RMS interface, therefore, must support the standard NG9-1-1 authentication and security requirements (section3.6.6) and the most current Criminal Justice

[4] Note: An internal mechanism would require access to a master or replica GIS system. If no internal mechanism is available, the ECRF/LVF FEs would be used by the Dispatch FE to determine the correct service for the given incident location.

Information System (CJIS) security policy [23] for exchanging criminal history and other justice information.

Requirements:

RMSINTERFACE 0100-0100 The RMS Interface shall support EIDD information exchanges as described in the General FE section of this document.

RMSINTERFACE 0200-0100 The RMS Interface may support the exchange of the multimedia data supported by NG9-1-1 as specified in NENA-STA-010 [4].

RMSINTERFACE 0300-0100 The RMS Interface should support a premise history query and response that returns historical incident information for a provided location.

RMSINTERFACE 0400-0100 The RMS Interface should support a vehicle query and response that returns vehicle information for a specified vehicle.

RMSINTERFACE 0500-0100 The RMS Interface should support a query and response that returns information for a specified individual or entity. This includes information regarding internal personnel.

RMSINTERFACE 0600-0100 The RMS Interface should support a location query and response that returns caution flag, key holder, emergency equipment, camera and other detailed information for a specified location.

RMSINTERFACE 0700-0100 The RMS Interface should support a staffing query and response that returns the individuals staffing an Emergency Response Unit.

RMSINTERFACE 0800-0100 The RMS Interface should support a shift schedule query and response that returns the shift schedule for Emergency Response Units.

RMSINTERFACE 0900-0100 The RMS Interface should support a shift schedule query and response that returns the shift schedule for an Agency.

RMSINTERFACE 1000-0100 The RMS Interface should support a case number query and response that returns the next sequential case number for an agency.

RMSINTERFACE 1100-0100 The RMS interface shall use Data Access Controls to ensure that the entity attempting to access information through the interface has access rights to the data.

RMSINTERFACE 1200-0100 Based on the credentials of the user attempting to access the data, the RMS Interface should be able to transform and filter data contained in an EIDD transmitted through the interface based on the data owner's policy for the data.

3.7.6 Responder Data Services Functional Element

The primary function of the Responder Data Services Functional Element (Responder Data Services FE) is to enable near real time wireless data transmissions between PSAPs and emergency responder devices. i3 PSAPs can support full NG9-1-1 functionality without implementing an NG9-1-1 compliant Responder Data Services FE.

The type of data transmissions between the PSAP and emergency responders that are handled by the Responder Data Services FE include transmitting dispatch information such as location of Incident, names of parties, nature of Incident, hazard codes, etc., creating new Incidents, updating active and

closed Incidents, as well as sending and receiving different types of messages. The Responder Data Services FE can support the transmission and receipt of media (text, sound, imagery, video clips, and streaming video), or a reference (i.e. URL) to that media. Media transmissions should be supported between mobile devices and a variety of origins and destinations including PSAPs, command centers and other mobile devices connected to this or another Responder Data Services FE.

This document describes requirements for the Agency-facing interface of the Responder Data Services. The Responder-facing interface is not described in this document.

The Responder Data Services Responder Data Services FE should be able to continuously and/or upon demand provide the location and/or status of its responders or responder devices, which may become the location of an emergency incident. To avoid inundating emergency responders with information, all real-time media information that is directly transmitted to emergency responders (mobile devices) should be controlled and routed by PSAP personnel. However, emergency responders should be able to use information provided in the Emergency Incident Data Document to access media associated with their assigned incidents.

A uniform list of status codes, while outside the scope of this document, is being created as part of the Emergency Incident Data Document effort. Implementation of this Status Code standard, along with standards for Disposition Codes and Call Types, is important in ensuring a uniform implementation, and interoperable capabilities of any mobile data system.

Requirements

The Responder Data Services FE is an optional functional element. To be fully NG9-1-1 compliant, if a Responder Data Services FE is implemented its requirements are:

RESPONDER-DATA 0200-0100 The Responder Data Services FE interface shall support creating an Incident, subject to provisioning and policy.

RESPONDER-DATA 0300-0100 The Responder Data Services FE interface shall support the ability to request, receive and modify an incident as defined by EIDD data elements.

RESPONDER-DATA 0400-0100 The Responder Data Services FE interface shall support the ability to send and receive an EIDD.

RESPONDER-DATA 0500-0100 The Responder Data Services FE should support the Collaboration FE client interface.

RESPONDER-DATA 0600-0100 The Responder Data Services FE shall support logging all application data and media that is shared with other FEs.

RESPONDER-DATA 0700-0100 The Responder Data Services FE shall support the reception and transmission of real-time media or recorded media including text, video, and audio[5].

RESPONDER-DATA 0900-0100 The Responder Data Services FE should support SIP [17] to allow multimedia communication.

[5]This requirement does not imply any requirement or limitation of the over the air interface.

RESPONDER-DATA 1100-0100 The Responder Data Services FE shall be able to support reporting the current location and other available information (e.g., speed, direction of travel, etc.) of emergency responders or responder devices if the information is available.

RESPONDER-DATA 1200-0100 The Responder Data Services FE should support requests for the current location and other available information (e.g., speed, direction of travel, etc.) of responders or responder devices.

RESPONDER-DATA 1300-0100 The Responder Data Services FE shall be able to support reporting status information received from its remote devices.

RESPONDER-DATA 1400-0100The Responder Data Services FE shall support interoperation between remote devices and the Collaboration FE.

3.7.7 Logging Service

In order to maintain a legal record of emergency incident communications and related data, and to provide a common repository for other uses, every PSAP must have access to a Logging Service. A Logging Service can exist in the ESInet, and may be utilized by the PSAP to support the logging functions described herein. A PSAP may have its own Logging Service, and support the same interfaces defined. All required information must be logged but the choice of where PSAP data is logged is at the discretion of the local jurisdiction.

The Logging Service is considered a primary (required) service for a PSAP's serving NGCS, and for the PSAP itself. Every significant event that occurs within the PSAP boundary must be logged: routing events, queries/responses that determine routing decisions and queries/responses of additional Incident-related data.

All emergency communications media that originate or terminate in the PSAP must be logged. This includes all communications between the PSAP and persons or devices initiating a request for assistance, and all communications with responders.

Additional metadata associated with those communications may be logged, as determined by local business rules; including annotations that may be added during or after the Incident is closed.

Logged data is utilized by the PSAP in numerous ways, including, but not limited to, the following:

- For internal reviews of incident-related communications and events.
- For production of logged data in response to outside requests (prosecutor's office, subpoena, media requests, etc.)
- For conducting studies of communications quality and traffic patterns, see also MIS section of this document.
- To provide input for purposes of conducting evaluations and assessments of PSAP personnel performance, i.e. quality assurance and quality monitoring activities.
- To provide logged data to another agency to which handling of the incident has been transferred.

- To support Instant Recall Recorder (IRR) capabilities used by Agents and/or Dispatchers.IRR capabilities may be provided by the Logging Service, or be integrated within the Call Handling FE.
- Logging Service can be used as a source of data for incident reconstruction.

Any PSAP Functional Element that requires access to logged events and/or media, and which is allowed such access by local business rules, shall access the data via the standard interfaces defined in NENA-STA-010 [4].These interfaces shall support the following broad functionalities:

- Logging of all significant events that occur within the PSAP boundary, and any required data associated with them.
- Logging of all Media that constitutes an emergency-related communication between the PSAP and an outside entity.
- Retrieval of logged events and media.

Requirements:

LOGGING 0100-0100 The Logging Service shall support logging of all LogEvents that occur within the PSAP as defined in the NENA LogEvent registry, and any required additional data associated with them.

LOGGING 0200-0100 The Logging Service shall support all of the interfaces defined in the Logging Service section of NENA-STA-010 [4].

LOGGING 0300-0100 The Logging Service shall support logging of all media that terminates in, or originates from, the PSAP.

LOGGING 0400-0100 The Logging Service shall support playback of multiple audio streams and/or audio mixing (combining of multiple audio streams into a single stream for playback, i.e. bridging).

LOGGING 0500-0100 The Logging Service shall support playback of multiple video streams and/or video mixing (combining of multiple video streams into a single stream for playback, i.e. compositing).

LOGGING 0600-0100 The Logging Service shall support playback of multiple text streams mixed into a single stream together with identification of parties and timing.

LOGGING 0700-0100 The Logging Service shall support a media seek function for audio, video and text media.

LOGGING 0800-0100 The Logging Service shall support synchronizing of multiple played back media streams to each other and to original NTP time.

LOGGING 0900-0100 The Logging Service shall support acquisition of radio media and metadata via the Radio Interface described in section 3.3.6.

LOGGING 1000-0100 The Logging Service shall support acquisition of media from administrative communications via the standard interface (See NENA-STA-010 [4]).

LOGGING 1100-0100 The Logging Service shall support acquisition of display data (i.e. screen capture) with timing information.

LOGGING 1200-0101 Log records must be retrievable from the Logging Service FE for as long as the records are retained by the Agency.

LOGGING 1300-0100 The Logging Service shall support high availability of logged data.

LOGGING 1400-0100 The Logging Service shall support the fault tolerance mechanisms defined in the Logging Service section of NENA-STA-010 [4].

LOGGING 1500-0100 The Logging Service shall keep an "audit trail" of all attempts to access logged data (successful and unsuccessful).

LOGGING 1600-0101 This audit trail shall contain the type of access, the identification of the data accessed, the username, and the date/time of the access.

LOGGING 1700-0100 The Logging Service shall support retention policies for logged data that retains and deletes data as required.

LOGGING 1800-0100 The Logging Service shall support "protect from deletion" functionality that allows certain logged data to be marked to prevent deletion when its retention period has expired.

3.7.8 Incident Data Exchange

The Incident Data Exchange (IDE) FE facilitates the exchange of Emergency Incident Data Documents (EIDDs) among other FEs both within and external to an agency. An individual FE has its own view (the state of an incident known to that FE) of an incident, and can generate EIDDs to express its view. However, many FEs, especially those outside an agency, need a comprehensive view (all the state of an incident known by an agency) of an incident, which can be thought of as the union of the EIDDs of the FEs' EIDDs.

An IDE FE is provisioned with the constituent FEs that it serves. Those FEs may belong to the same agency or different agencies. A single IDE FE may support one or more agencies.

The IDE FE can also coordinate the exchange of incident related information between 9-1-1 Authorities and other entities that are authorized to receive that information via the exchange of EIDDs. The IDE FE, like all other FEs, filters EIDDs to contain only the information that the data owner authorizes the recipients to receive.

Each agency FE that generates an EIDD must supply the EIDD to at least one IDE FE, so that the IDE can provide a comprehensive view of an incident. This requires that the IDE subscribe to EIDD data from the FEs that it serves. In some circumstances, FEs may exchange EIDDs without the use of an IDE FE.

The IDE provides two interfaces: a Subscription-Update interface and a Request-Response interface. Through these interfaces the IDE supplies either EIDDs representing the complete, current state of an incident or EIDDs representing changes to the status of incidents. When FEs request or subscribe to an IDE, they indicate the type of incident update desired; either a full, complete incident update or merely changes (deltas) to an incident's state. The IDE then provides EIDDs in the type requested.

As specified in the General Functional Element Requirements section, agency data rights management policies must be enforced by all FEs when exchanging EIDDs. Agency data rights management policies for an individual FE might be simple, using the IDE FE to provide the centralized point for enforcing data rights management for exchanged EIDDs. The IDE FE can be

the point where the enforcement of filtering and other complex policies for EIDD exchanges occurs. See the "Security Authorization" section of NENA-STA-010 [4] for further information.

Requirements:

IDE 0100-0100 Every Agency must have an IDE, the element that sends and receives EIDDs to and from other agencies.

IDE 0200-0100 The IDE FE shall be able to aggregate the information contained in multiple EIDDs about an incident to generate a comprehensive representation of the current state of an incident.

IDE 0300-0100 The IDE FE must subscribe to EIDDs from all FEs within the Agency.

IDE 0400-0100 The IDE FE must support filtering the contents of an EIDD to conform to policies of the Agency.

IDE 0500-0100 An IDE must be discoverable by other FEs.

IDE 0600-0100 The IDE FE shall be capable of providing an EIDD that contains the complete status of an incident to any FE which requests it, subject to Agency policy restrictions.

3.8 Incident Supporting Layer Functional Elements

3.8.1 Time Server Functional Element

The time used by all functional elements must be synchronized in order to ensure the consistency of time stamps added to event records, reports, and media recordings. The PSAP must utilize an NTP time service as specified in Section 5.17 of NENA-STA-010 [4].

The Time Server FE provides NTP time services to other Functional Elements. See the Section 3.1.2 "General Functional Element Requirements" for time synchronization requirements of the other FEs.

Requirements:

TIMESYNC 0100-0100 The Time Server FE shall meet the requirements specified in Section 5.17 of NENA-STA-010 [4].

3.9 Collaboration FE Requirements

Collaboration among agents, both within and between agencies, is a highly desirable, optional capability of a next generation public safety system. The collaboration FE enables agents to communicate with each other using the same set of media (voice, video and text) supported elsewhere in the NG9-1-1 system. Both intercom (agent initiated with automatic connection to other agents) and "chat room" (agent join to an existing or new chat room) mechanisms are specified to initiate collaboration. It is anticipated that both client and server functions will be specified.

Requirements:

COLLABORATION 0100-0100 An interoperable mechanism to subscribe to the presence of agents is required

COLLABORATION 0200-0100 An interoperable mechanism for supporting an intercom (point-to-point) function between two or more agents with real-time voice, video and/or text media shall be specified

COLLABORATION 0300-0100 An interoperable mechanism for supporting a chat room function among multiple agents with real-time voice, video and/or text media shall be specified

COLLABORATION 0400-0100 All requirements in this section shall support one agency or multiple agencies or both

COLLABORATION 0500-0100 An interoperable mechanism for discovering the contacts of agents in an agency must be specified

COLLABORATION 0600-0100 An agent must have the ability to positively accept or reject invitation for intercom as specified in 0200-0100

COLLABORATION 0700-0100 An agent must have the ability to mute media as specified in 0300-0100

COLLABORATION 0800-0100 Must be able to retrieve an EIDD given a particular Call or Incident Tracking ID

COLLABORATION 0900-0100 All media and signaling must be logged as per policy

COLLABORATION 1000-0100 Logging of intercom or chat room discussions associated with an incident must include the incident tracking ID

COLLABORATION 1100-0100 A chat room shall be identifiable through a URI

COLLABORATION 1200-0100 It must be possible to discover a chat room associated with an incident or a call.

4 Recommended Reading and References

1. Network Time Protocol (Version 3) Specification, Implementation and Analysis, Mills, Internet Engineering Task Force RFC 1305
2. NENA 08-751, Issue 1, NENA i3 Technical Requirements Document, September 28, 2006
3. NENA 08-002, Version 1.0, NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3) December 18, 2007
4. NENA-STA-010, Detailed Functional and Interface Standards for the NENA i3 Solution, Work in progress
5. NENA 04-001, Recommended Generic Standards for E9-1-1 PSAP Equipment, March 2001
6. NENA 75-001, Security for Next-Generation 9-1-1, February 6, 2010
7. LoST: A Location-to-Service Translation Protocol, T. Hardie et. al., Internet Engineering Task Force, RFC 5222
8. Real Time Streaming Protocol (RTSP), H. Schulzrinne, A. Rao, M. Lanphier, Internet Engineering Task Force, RFC 2326
9. NENA 54-750, Human Machine Interface & PSAP Display Requirements, October 20, 2010
10. NENA 08-506, NENA Emergency Services IP Network Design for NG9-1-1 (NID), December 14, 2011

11. NENA-INF-008, NG9-1-1 Transition Planning Considerations Information Document
12. RTP Payload for Text Conversation, G. Hellstrom, P. Jones, Internet Engineering Task Force, RFC 4103
13. APCO/CSAA 2.101.2-2014, Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP), August 5, 2014
14. Lightweight Directory Access Protocol (LDAP):Technical Specification Road Map, RFC 4510
15. NENA 04-002, PSAP Master Clock, April 9, 2007
16. ANSI/TIA-102.AABC, Project 25, Trunking Control Channel Messages, April 18, 2009
17. Session Initiation Protocol, J, Rosenberg et. al., Internet Engineering Task Force, RFC 3261
18. Project 25 Inter-RF Subsystem Interface Messages and Procedures for Voice Services, Mobility Management, and RFSS Capability Polling Services, TIA-102.BACA
19. Implementation Profile for Interoperable Bridging Systems Interfaces, BSI-Core 1.1
20. Common Alerting Protocol Version 1.2
21. Integrated Public Alert & Warning System Open Platform for Emergency Networks
22. Unified Computer-Aided Dispatch Functional Requirements (UCADFR), APCO International and IJIS Institute (work in progress)
23. Criminal Justice Information Services (CJIS) Security Policy, version 5.2, U.S. Department of Justice, August 09, 2013
24. NENA-STA-006, NENA Standard for NG9-1-1 GIS Data Model (work in progress)
25. NENA/APCO-INF-005, NENA/APCO Emergency Incident Data Document (EIDD) Information Document, Feb 21, 2014
26. NENA 04-502, E9-1-1 PSAP CPE Site Characteristics, March 31, 2004

5 Previous Acknowledgments

None. This is the original document.