Common Alerting Protocol, v. 1.1

Committee Specification, 11 August 2005

Document Identifier:
> CAP-V1.1

Location:
> http://docs.oasis-open.org/emergency/CAP/V1.1/

Technical Committee:
> OASIS Emergency Management TC

Editor(s):
> Elysa Jones, Warning Systems, Inc <ejones@warningsystems.com>
> Art Botterell, Individual <acb@incident.com>

Abstract:
> The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

Status:
> This document is a Committee Specification of the Emergency Management Technical Committee. This document is updated periodically. Send comments about this document to the editor.
> Committee members should send comments on this specification to the emergency@lists.oasis-open.org list. Others should subscribe to and send comments to the emergency-comment@lists.oasis-open.org list. To subscribe, send an email message to emergency-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Emergency Management TC web page (http://www.oasis-open.org/committees/emergency/).

Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS President.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS President.

Copyright © OASIS Open 2005. *All Rights Reserved.*

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1 Introduction

1.1 Purpose

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as Web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) Weather Radio and the Emergency Alert System (EAS), while offering enhanced capabilities that include:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital encryption and signature capability; and,
- Facility for digital images and audio.

Key benefits of CAP will include reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning sources and dissemination systems involved in all-hazard warning. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent national and international "warning internet."

1.2 History

The National Science and Technology Council report on "Effective Disaster Warnings" released in November, 2000 recommended that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems."

An international working group of more than 130 emergency managers and information technology and telecommunications experts convened in 2001 and adopted the specific recommendations of the NSTC report as a point of departure for the design of a Common Alerting Protocol (CAP). Their draft went through several revisions and was tested in demonstrations and field trials in Virginia (supported by the ComCARE Alliance) and in California (in cooperation with the California Office of Emergency Services) during 2002 and 2003.

In 2002 the CAP initiative was endorsed by the national non-profit Partnership for Public Warning, which sponsored its contribution in 2003 to the OASIS standards process. In 2004, CAP version 1.0 was adopted as an OASIS Standard.

1.3 Structure of the CAP Alert Message

Each CAP Alert Message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> segments. Under most circumstances CAP messages with a <msgType> value of "Alert" SHOULD include at least one <info> element. (See the document object model diagram in section 3.1, below.)

1.3.1 <alert>

The <alert> segment provides basic information about the current message: its purpose, its source and its status, as well as unique identifier for the current message and links to any other, related messages. An <alert> segment may be used alone for message acknowledgements, cancellations or other system functions, but most <alert> segments will include at least one <info> segment.

1.3.2 <info>

The <info> segment describes an anticipated or actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well as providing both categorical and textual descriptions of the subject event. It may also provide instructions for appropriate response by message recipients and various other details (hazard duration, technical parameters, contact information, links to additional information sources, etc.) Multiple <info> segments may be used to describe differing parameters (e.g., for different probability or intensity "bands") or to provide the information in multiple languages.

1.3.3 <resource>

The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears in the form of a digital asset such as an image or audio file.

1.3.4 <area>

The <area> segment describes a geographic area to which the <info> segment in which it appears applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed in standard latitude / longitude / altitude terms in accordance with a specified geospatial datum.

1.4 Applications of the CAP Alert Message

The primary use of the CAP Alert Message is to provide a single input to activate all kinds of alerting and public warning systems. This reduces the workload associated with using multiple warning systems while enhancing technical reliability and target-audience effectiveness. It also helps ensure consistency in the information transmitted over multiple delivery systems, another key to warning effectiveness.

A secondary application of CAP is to normalize warnings from various sources so they can be aggregated and compared in tabular or graphic form as an aid to situational awareness and pattern detection.

Although primarily designed as an interoperability standard for use among warning systems and other emergency information systems, the CAP Alert Message can be delivered directly to alert recipients over various networks, including data broadcasts. Location-aware receiving devices could use the information in a CAP Alert Message to determine, based on their current location, whether that particular message was relevant to their users.

The CAP Alert Message can also be used by sensor systems as a format for reporting significant events to collection and analysis systems and centers.

1.5 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **[RFC2119]**.

The words *warning*, *alert* and *notification* are used interchangeably throughout this document.

The term "coordinate pair" is used in this document to refer to a comma-delimited pair of decimal values describing a geospatial location in degrees, unprojected, in the form "[latitude],[longitude]". Latitudes in the Southern Hemisphere and longitudes in the Western Hemisphere are signed negative by means of a leading dash.

1.6 Normative References

85	**1.6 Normative References**	
86	**[RFC2119]**	S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
87		http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.
88	**[dateTime]**	N. Freed, XML Schema Part 2: Datatypes Second Edition,
89		http://www.w3.org/TR/xmlschema-2/#dateTime, W3C REC-xmlschema-2,
90		October 2004.
91	**[FIPS 180-2]**	National Institute for Standards and Technology, Secure Hash Standard,
92		http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf,
93		August 2002.
94	**[namespaces]**	T. Bray, Namespaces in XML, http://www.w3.org/TR/REC-xml-names/, W3C
95		REC-xml-names-19990114, January 1999.
96	**[RFC2046]**	N. Freed, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types,
97		http://www.ietf.org/rfc/rfc2046.txt, IETF RFC 2046, November 1996.
98	**[RFC2119]**	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels,
99		http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.
100	**[RFC3066]**	H. Alvestrand, Tags for the Identification of Languages,
101		http://www.ietf.org/rfc/rfc3066.txt, IETF RFC 3066, January 2001.
102	**[WGS 84]**	National Geospatial Intelligence Agency, Department of Defense World Geodetic
103		System 1984, http://earth-info.nga.mil/GandG/tr8350_2.html, NGA Technical
104		Report TR8350.2, January 2000.
105	**[XML 1.0]**	T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition),
106		http://www.w3.org/TR/REC-xml/, W3C REC-XML-20040204, February 2004.
107	**[XMLSIG]**	Eastlake, D., Reagle, J. and Solo, D. (editors), *XML-Signature Syntax and*
108		*Processing*, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, W3C
109		Recommendation, February 2002.
110	**[XMLENC]**	Eastlake, D. and Reagle, J. (editors), *XML Encryption Syntax and Processing*,
111		http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, W3C
112		Recommendation, December 2002.

2 Design Principles and Concepts (non-normative)

2.1 Design Philosophy

Among the principles which guided the design of the CAP Alert Message were:

- **Interoperability** – First and foremost, the CAP Alert Message should provide a means for interoperable exchange of alerts and notifications among all kinds of emergency information systems.

- **Completeness** – The CAP Alert Message format should provide for all the elements of an effective public warning message.

- **Simple implementation** – The design should not place undue burdens of complexity on technical implementers.

- **Simple XML and portable structure** – Although the primary anticipated use of the CAP Alert Message is as an XML document, the format should remain sufficiently abstract to be adaptable to other coding schemes.

- **Multi-use format** – One message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgements / error messages) in various applications (actual / exercise / test / system message.)

- **Familiarity** – The data elements and code values should be meaningful to warning originators and non-expert recipients alike.

- **Interdisciplinary and international utility** – The design should allow a broad range of applications in public safety and emergency management and allied applications and should be applicable worldwide.

2.2 Requirements for Design

> Note: The following requirements were used as a basis for design and review of the CAP Alert Message format. This list is non-normative and not intended to be exhaustive.

The Common Alerting Protocol SHOULD:

- Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
- Enable integration of diverse sensor and dissemination systems;
- Be usable over multiple transmission systems, including both TCP/IP-based networks and one-way "broadcast" channels;
- Support credible end-to-end authentication and validation of all messages;
- Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
- Provide for multiple message types, such as:
  – Warnings
  – Acknowledgements
  – Expirations and cancellations
  – Updates and amendments
  – Reports of results from dissemination systems
  – Administrative and system messages
- Provide for multiple message types, such as:

154   –   Geographic targeting

155   –   Level of urgency

156   –   Level of certainty

157   –   Level of threat severity

158   •   Provide a mechanism for referencing supplemental information (e.g., digital audio or image files,
159   additional text);

160   •   Use an established open-standard data representation;

161   •   Be based on a program of real-world cross-platform testing and evaluation;

162   •   Provide a clear basis for certification and further protocol evaluation and improvement; and,

163   •   Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency
164   response and public safety users and warning system operators.

2.3 Examples of Use Scenarios

166   Note: The following examples of use scenarios were used as a basis for design and
167   review of the CAP Alert Message format. These scenarios are non-normative and not
168   intended to be exhaustive or to reflect actual practices.

2.3.1 Manual Origination

170   "The Incident Commander at an industrial fire with potential of a major explosion decides to issue a public
171   alert with three components: a) An evacuation of the area within half a mile of the fire; b) a shelter-in-
172   place instruction for people in a polygon roughly describing a downwind dispersion 'plume' extending
173   several miles downwind and half a mile upwind from the fire; and c) a request for all media and civilian
174   aircraft to remain above 2500 feet above ground level when within a half mile radius of the fire.

175   "Using a portable computer and a web page (and a pop-up drawing tool to enter the polygon) the Incident
176   Commander issues the alert as a CAP message to a local alerting network."

2.3.2 Automated Origination by Autonomous Sensor System

178   "A set of automatic tsunami warning sirens has been installed along a popular Northwest beach. A
179   wireless network of sensor devices collocated with the sirens controls their activation. When triggered,
180   each sensor generates a CAP message containing its location and the sensed data at that location that is
181   needed for the tsunami determination. Each siren activates when the combination of its own readings and
182   those reported at by other devices on the network indicate an immediate tsunami threat. In addition, a
183   network component assembles a summary CAP message describing the event and feeds it to regional
184   and national alerting networks."

2.3.3 Aggregation and Correlation on Real-time Map

186   "At the State Operations Center a computerized map of the state depicts, in real time, all current and
187   recent warning activity throughout the state. All major warning systems in the state – the Emergency
188   Alert System, siren systems, telephone alerting and other systems – have been equipped to report the
189   details of their activation in the form of a CAP message. (Since many of them are now activated by way
190   of CAP messages, this is frequently just a matter of forwarding the activation message to the state
191   center.)

192   "Using this visualization tool, state officials can monitor for emerging patterns of local warning activity and
193   correlate it with other real time data (e.g., telephone central office traffic loads, 9-1-1 traffic volume,
194   seismic data, automatic vehicular crash notifications, etc.)."

2.3.4 Integrated Public Alerting

196   "As part of an integrated warning system funded by local industry, all warning systems in a community
197   can be activated simultaneously by the issuance by authorized authority of a single CAP message.

198 "Each system converts the CAP message data into the form suitable for its technology (text captioning on
199 TV, synthesized voice on radio and telephone, activation of the appropriate signal on sirens, etc.).
200 Systems that can target their messages to particular geographic areas implement the targeting specified
201 in the CAP message with as little 'spill' as their technology permits.

202 "In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also
203 get corroboration of the alert through multiple channels, which increases the chance of the warning being
204 acted upon."

205 2.3.5 Repudiating a False Alarm

206 "Inadvertently the integrated alerting network has been activated with an inaccurate warning message.
207 This activation comes to officials' attention immediately through their own monitoring facilities (e.g., 2.3.3
208 above). Having determined that the alert is, in fact, inappropriate, the officials issue a cancellation
209 message that refers directly to the erroneous prior alert. Alerting systems that are still in the process of
210 delivering the alert (e.g., telephone dialing systems) stop doing so. Broadcast systems deliver the
211 cancellation message. Other systems (e.g., highway signs) simply reset to their normal state."

212 3 Alert Message Structure (normative)

213 3.1 Document Object Model

214

alert / **info** *

Message ID (identifier)
Sender Code (sender) / (category) *
Sent Date/Time (sent)
Message Status (status) / Type *
Message Type (msgType)
Severity (severity)
Scope (scope) / Certainty (certainty)
Restriction (restriction)
Addresses (addresses) / Event Code (eventCode) *
Effective Date/Time (code) / (effective)
Note (note) / Date/Time (onset)
Reference IDs / *Date/Time (expires)*
Incident IDs (incidents) / Sender Name (senderName)
Headline (headline)
Event Description (description)
Instructions (instruction)
Information URL (web)
Contact Info (contact)
Parameter (parameter) *

resource / **area** *

Description (resourceDesc) / (areaDesc)
MIME Type (mimeType) / Polygon (polygon) *
Elements in **boldface** are mandatory; elements in *italics*
have default values that will be assumed if the element is not
present; asterisks (*) indicate that multiple instances are
permitted.

215

3.2 Data Dictionary

216

217   Note: Unless explicitly constrained within this Data Dictionary or the XML Schema
218   (Section 3.4), CAP elements MAY have null values. Implementers MUST check for this
219   condition wherever it might affect application performance.

220

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
3.2.1 "alert" Element and Sub-elements			

alert	**cap.**
	alert.
	
	group
		The container for all component parts of the alert message (REQUIRED)	(1) Surrounds CAP alert message sub-elements
			
			(2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.:
			`<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">`
			`    [sub-elements]`
			`</cap:alert>`
			
			(3) In addition to the specified sub-elements, MAY contain one or more <info> blocks.

identifier	**cap.** **alert.** **identifier**	**The identifier of the alert message (REQUIRED)**	(1) A number or string uniquely identifying this message, assigned by the sender (2) MUST NOT include spaces, commas or restricted characters (< and &)
sender	**cap.** **alert.** **sender.** **identifier**	**The identifier of the sender of the alert message (REQUIRED)**	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name (2) MUST NOT include spaces, commas or restricted characters (< and &)
sent	**cap.** **alert.** **sent.** **time**	**The time and date of the origination of the alert message (REQUIRED)**	(1) The date and time is represented in **[dateTime]** format (e. g., `2002-05-24T16:49:00-07:00` for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00" or "+00:00.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
status	**cap. alert. status. code**	**The code denoting the appropriate handling of the alert message (REQUIRED)**	Code Values: "Actual" - Actionable by all targeted recipients "Exercise"- Actionable only by designated exercise participants; exercise identifier should appear in <note> "System" - For messages that support alert network internal functions. "Test" - Technical testing only, all recipients disregard "Draft" – A preliminary template or draft, not actionable in its current form.
msgType	**cap. alert. type. code**	**The code denoting the nature of the alert message (REQUIRED)**	Code Values: "Alert" - Initial information requiring attention by targeted recipients "Update" - Updates and supercedes the earlier message(s) identified in <references> "Cancel" - Cancels the earlier message(s) identified in <references> "Ack" - Acknowledges receipt and acceptance of the message(s)) identified in <references> "Error" indicates rejection of the message(s) identified in <references>; explanation SHOULD appear in <note>
source	cap. alert. source. identifier	The text identifying the source of the alert message (OPTIONAL)	The particular source of this alert; e.g., an operator or a specific device.
scope	**cap. alert. scope. code**	**The code denoting the intended distribution of the alert message (REQUIRED)**	Code Values: "Public" - For general dissemination to unrestricted audiences "Restricted" - For dissemination only to users with a known operational requirement (see <restriction>, below) "Private" - For dissemination only to specified addresses (see <address>, below)

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
restriction	cap. alert. restriction. text	The text describing the rule for limiting distribution of the restricted alert message (conditional)	Used when <scope> value is "Restricted"
addresses	cap. alert. addresses. group	The group listing of intended recipients of the private alert message (conditional)	(1) Used when <scope> value is "Private" (2) Each recipient SHALL be identified by an identifier or an address (3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.
code	cap. alert. code	The code denoting the special handling of the alert message (OPTIONAL)	(1) Any user-defined flag or special code used to flag the alert message for special handling. (2) Multiple instances MAY occur within a single <info> block.
note	cap. alert. note. text	The text describing the purpose or significance of the alert message (OPTIONAL)	The message note is primarily intended for use with Cancel and Error alert message types.
references	cap. alert. references. group	The group listing identifying earlier message(s) referenced by the alert message (OPTIONAL)	(1) The extended message identifier(s) (in the form *sender,identifier,sent)* of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
incidents	cap. alert. incidents. group	The group listing naming the referent incident(s) of the alert message (OPTIONAL)	(1) Used to collate multiple messages referring to different aspects of the same incident (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes

3.2.2 "info" Element and Sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
info	cap. alertInfo. info. group	The container for all component parts of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple "info" blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of "info" blocks containing the same language identifier SHALL be treated as a separate sequence. (2) In addition to the specified sub-elements, MAY contain one or more <resource> blocks and/or one or more <area> blocks.
language	cap. alertInfo. language. code	The code denoting the language of the info sub-element of the alert message (OPTIONAL)	(1) Code Values: Natural language identifier per **[RFC 3066].** (2) If not present, an implicit default value of "en-US" SHALL be assumed. (3) A null value in this element SHALL be considered equivalent to "en-US."

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
category	cap. alertInfo. category. code	The code denoting the category of the subject event of the alert message (REQUIRED)	(1) Code Values: "Geo" - Geophysical (inc. landslide) "Met" - Meteorological (inc. flood) "Safety" - General emergency and public safety "Security" - Law enforcement, military, homeland and local/private security "Rescue" - Rescue and recovery "Fire" - Fire suppression and rescue "Health" - Medical and public health "Env" - Pollution and other environmental "Transport" - Public and private transportation "Infra" - Utility, telecommunication, other non-transport infrastructure "CBRNE" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack "Other" - Other events (2) Multiple instances MAY occur within a single <info> block.
event	cap. alertInfo. event. text	The text denoting the type of the subject event of the alert message (REQUIRED)	

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
responseType	cap. alertInfo. responseType. code	The code denoting the type of action recommended for the target audience. (OPTIONAL)	(1) Code Values: "Shelter" – Take shelter in place or per <instruction> "Evacuate" – Relocate as instructed in the <instruction> "Prepare" – Make preparations per the <instruction> "Execute" – Execute a pre-planned activity identified in <instruction> "Monitor" – Attend to information sources as described in <instruction> "Assess" – Evaluate the information in this message. (This value SHOULD NOT be used in public warning applications.) "None" – No action recommended (2) Multiple instances MAY occur within a single <info> block.
urgency	**cap. alertInfo. urgency. code**	**The code denoting the urgency of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Immediate" - Responsive action SHOULD be taken immediately "Expected" - Responsive action SHOULD be taken soon (within next hour) "Future" - Responsive action SHOULD be taken in the near future "Past" - Responsive action is no longer required "Unknown" - Urgency not known

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
severity	**cap. alertInfo. severity. code**	**The code denoting the severity of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Extreme" - Extraordinary threat to life or property "Severe" - Significant threat to life or property "Moderate" - Possible threat to life or property "Minor" - Minimal threat to life or property "Unknown" - Severity unknown
certainty	**cap. alertInfo. certainty. code**	**The code denoting the certainty of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Observed" – Determined to have occurred or to be ongoing. "Likely" - Likely (p > ~50%) "Possible" - Possible but not likely (p <= ~50%) "Unlikely" - Not expected to occur (p ~ 0) "Unknown" - Certainty unknown (3) For backward compatibility with CAP 1.0, the deprecated value of "Very Likely" SHOULD be treated as equivalent to "Likely."
audience	cap. alertInfo. audience. text	The text describing the intended audience of the alert message (OPTIONAL)	

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain

eventCode	cap. alertInfo. event. code	A system-specific code identifying the event type of the alert message (OPTIONAL)	(1) Any system-specific code for event typing, in the form:
			
			`<eventCode>`
			  `<valueName>`*valueName*`</valueName>`
			  `<value>`*value*`</value>`
			`</eventCode>`
			
			where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CEM").
			
			(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).
			
			(3) Multiple instances MAY occur within a single <info> block.

effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in **[dateTime]** format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00" or "+00:00. (3) If this item is not included, the effective time SHALL be assumed to be the same as in <sent>.
onset	cap. alertInfo. onset. time	The expected time of the beginning of the subject event of the alert message (OPTIONAL)	(1) The date and time is represented in **[dateTime]** format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00" or "+00:00.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
expires	cap. alertInfo. expires. time	The expiry time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in **[dateTime]** format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00" or "+00:00. (3) If this item is not provided, each recipient is free to set its own policy as to when the message is no longer in effect.
senderName	cap. alertInfo. sender. name	The text naming the originator of the alert message (OPTIONAL)	The human-readable name of the agency or authority issuing this alert.
headline	cap. alertInfo. headline. text	The text headline of the alert message (OPTIONAL)	A brief human-readable headline. Note that some displays (for example, short messaging service devices) may only present this headline; it SHOULD be made as direct and actionable as possible while remaining short. 160 characters MAY be a useful target limit for headline length.
description	cap. alertInfo. description. text	The text describing the subject event of the alert message (OPTIONAL)	An extended human readable description of the hazard or event that occasioned this message.
instruction	cap. alertInfo. instruction. text	The text describing the recommended action to be taken by recipients of the alert message (OPTIONAL)	An extended human readable instruction to targeted recipients. (If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.)

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
web	cap alertInfo. information. identifier	The identifier of the hyperlink associating additional information with the alert message (OPTIONAL)	A full, absolute URI for an HTML page or other text resource with additional or reference information regarding this alert
contact	cap. alertInfo. contact. text	The text describing the contact for follow-up and confirmation of the alert message (OPTIONAL)	

parameter	cap. alertInfo. parameter. group	A system-specific additional parameter associated with the alert message (OPTIONAL)	(1) Any system-specific datum, in the form:
			
			```<parameter>```
			`  <valueName>valueName</valueName>`
			`  <value>value</value>`
			`</parameter>`
			
			where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CIV".)
			
			(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).
			
			(3) Multiple instances MAY occur within a single <info> block.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain

3.2.3 "resource" Element and Sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
resource	cap alertInfoResource. resource. group	The container for all component parts of the resource sub-element of the info sub-element of the alert element (OPTIONAL)	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file (2) Multiple occurrences MAY occur within a single <info> block
resourceDesc	**cap. alertInfoResource. resourceDesc. text**	**The text describing the type and content of the resource file (REQUIRED)**	The human-readable text describing the content and kind, such as "map" or "photo," of the resource file.
mimeType	cap. alertInfoResource. mimeType. identifier	The identifier of the MIME content type and sub-type describing the resource file (OPTIONAL)	MIME content type and sub-type as described in **[RFC 2046].** (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/media-types/)
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	Approximate size of the resource file in bytes.
uri	cap. alertInfoResource. uri. identifier	The identifier of the hyperlink for the resource file (OPTIONAL)	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
derefUri	cap alertInfoResource. derefUri. data	The base-64 encoded data content of the resource file (CONDITIONAL)	(1) MAY be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible.
			(2) Clients intended for use with one-way data links MUST support this element.
			(3) This element MUST NOT be used unless the sender is certain that all direct clients are capable of processing it.
			(4) If messages including this element are forwarded onto a two-way network, the forwarder MUST strip the <derefUri> element and SHOULD extract the file contents and provide a <uri> link to a retrievable version of the file.
			(5) Providers of one-way data links MAY enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types.
digest	cap. alertInfoResource. digest. code	The code representing the digital digest ("hash") computed from the resource file (OPTIONAL)	Calculated using the Secure Hash Algorithm (SHA-1) per **[FIPS 180-2]**

3.2.4 "area" Element and Sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
area	cap. alertInfoArea. area. group	The container for all component parts of the area sub-element of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks.
			(2) MAY contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> is the union of those represented by the included elements.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
areaDesc	**cap.** **alertInfoArea.** **area.** **text**	**The text describing the affected area of the alert message (REQUIRED)**	A text description of the affected area.
polygon	cap. alertInfoArea. polygon. group	The paired values of points defining a polygon that delineates the affected area of the alert message (OPTIONAL)	(1) Code Values: The geographic polygon is represented by a whitespace-delimited list of **[WGS 84]** coordinate pairs. (See WGS-84 Note at end of this section.) (2) The first and last pairs of coordinates MUST be the same. (3) See Coordinate Precision Note at end of this section. (4) Multiple instances MAY occur within an <area>.
circle	cap. alertInfoArea. circle. group	The paired values of a point and radius delineating the affected area of the alert message (OPTIONAL)	(1) Code Values: The circular area is represented by a central point given as a **[WGS- 84]** coordinates pair followed by a space character and a radius value in kilometers. (See WGS-84 Note at end of this section.) (2) See Coordinate Precision Note at end of this section. (3) Multiple instances MAY occur within an <area>.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain

geocode	cap. alertInfoArea. geocode. code	The geographic code delineating the affected area of the alert message (OPTIONAL)	(1) Any geographically-based code to describe message target area:
			
			`<parameter>`
			`  <valueName>`*valueName*`</valueName>`
			`  <value>`*value*`</value>`
			`</parameter>`
			
			where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113").
			
			(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).
			
			(3) Multiple instances MAY occur within a single <info> block.
			
			(4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it SHOULD be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible.

altitude	cap. alertInfoArea. altitude. quantity	The specific or minimum altitude of the affected area of the alert message (OPTIONAL)	(1) If used with the <ceiling> element this value is the lower limit of a range. Otherwise, this value specifies a specific altitude. (2) The altitude measure is in feet above mean sea level per the **[WGS- 84]** datum.
ceiling	cap. alertInfoArea. ceiling. quantity	The maximum altitude of the affected area of the alert message (conditional)	(1) MUST NOT be used except in combination with the <altitude> element (2) The ceiling measure is in feet above mean sea level per the **[WGS- 84]** datum.

221 3.3 Implementation Notes

222 3.3.1 WGS-84 Note

223 Geographic locations in CAP are defined using **[WGS 84]** (World Geodetic System 1984), equivalent to
224 EPSG (European Petroleum Survey Group) code 4326 (2 dimensions). CAP does not assign
225 responsibilities for coordinate transformations from and to other Spatial Reference Systems. See section
226 1.5 Terminology for the format of coordinate pairs within CAP elements.

227 3.3.2 Security Note

228 Because CAP is an XML-based format, existing XML security mechanisms can be used to secure and
229 authenticate its content. While these mechanisms are available to secure CAP Alert Messages, they
230 should not be used indiscriminately.

231 Note that this section adds two tags to CAP by reference. These are: "Signature and "EncryptedData".
232 Both elements are children of the <alert> element and are optional. If the "EncryptedData" element
233 exists, no other elements will be visible until after the message is decrypted. This makes the minimal
234 CAP message an alert element which encloses an EncryptedData element. The maximal CAP message,
235 if an EncryptedData element is present is an <alert> element enclosing a single EncryptedData element
236 and a single Signature element.

237 3.3.2.1 Digital Signatures

238 The alert element of a CAP Alert Message MAY have an Enveloped Signature, as described by XML-
239 Signature and Syntax Processing **[XMLSIG]**. Other XML signature mechanisms MUST NOT be used in
240 CAP Alert Messages.

241 Processors MUST NOT reject a CAP Alert Message containing such a signature simply because they are
242 not capable of verifying it; they MUST continue processing and MAY inform the user of their failure to
243 validate the signature.

244 In other words, the presence of an element with the namespace URI **[XMLSIG]** and a local name of
245 "Signature" as a child of the alert element must not cause a processor to fail merely because of its
246 presence.

247 3.3.2.2 Encryption

248 The alert element of a CAP Alert Message MAY be encrypted, using the mechanisms described by XML
249 Encryption Syntax and Processing **[XMLENC]**. Other XML encryption mechanisms MUST NOT be used
250 in CAP Alert Messages; however, transport-layer encryption mechanisms may be used independently of
251 this requirement.

252 3.4 XML Schema

```
253
254  <?xml version = "1.0" encoding = "UTF-8"?>
255  <schema xmlns = "http://www.w3.org/2001/XMLSchema"
256     targetNamespace = "urn:oasis:names:tc:emergency:cap:1.1"
257     xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.1"
258     xmlns:xs = "http://www.w3.org/2001/XMLSchema"
259     elementFormDefault = "qualified"
260     attributeFormDefault = "unqualified">
261    <element name = "alert">
262      <annotation>
263        <documentation>CAP Alert Message (version 1.1)</documentation>
264      </annotation>
265      <complexType>
266        <sequence>
267          <element name = "identifier" type = "string"/>
268          <element name = "sender" type = "string"/>
269          <element name = "sent" type = "dateTime"/>
270          <element name = "status">
271            <simpleType>
272              <restriction base = "string">
273                <enumeration value = "Actual"/>
```

```
274                        <enumeration value = "Exercise"/>
275                        <enumeration value = "System"/>
276                        <enumeration value = "Test"/>
277                        <enumeration value = "Draft"/>
278                      </restriction>
279                    </simpleType>
280                  </element>
281                  <element name = "msgType">
282                    <simpleType>
283                      <restriction base = "string">
284                        <enumeration value = "Alert"/>
285                        <enumeration value = "Update"/>
286                        <enumeration value = "Cancel"/>
287                        <enumeration value = "Ack"/>
288                        <enumeration value = "Error"/>
289                      </restriction>
290                    </simpleType>
291                  </element>
292                  <element name = "source" type = "string" minOccurs = "0"/>
293                  <element name = "scope">
294                    <simpleType>
295                      <restriction base = "string">
296                        <enumeration value = "Public"/>
297                        <enumeration value = "Restricted"/>
298                        <enumeration value = "Private"/>
299                      </restriction>
300                    </simpleType>
301                  </element>
302                  <element name = "restriction" type = "string" minOccurs = "0"/>
303                  <element name = "addresses" type = "string" minOccurs = "0"/>
304                  <element name = "code" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
305                  <element name = "note" type = "string" minOccurs = "0"/>
306                  <element name = "references" type = "string" minOccurs = "0"/>
307                  <element name = "incidents" type = "string" minOccurs = "0"/>
308                  <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
309                    <complexType>
310                      <sequence>
311                        <element name = "language" type = "language" default = "en-US" minOccurs = "0"/>
312                        <element name = "category" maxOccurs = "unbounded">
313                          <simpleType>
314                            <restriction base = "string">
315                              <enumeration value = "Geo"/>
316                              <enumeration value = "Met"/>
317                              <enumeration value = "Safety"/>
318                              <enumeration value = "Security"/>
319                              <enumeration value = "Rescue"/>
320                              <enumeration value = "Fire"/>
321                              <enumeration value = "Health"/>
322                              <enumeration value = "Env"/>
323                              <enumeration value = "Transport"/>
324                              <enumeration value = "Infra"/>
325                              <enumeration value = "CBRNE"/>
326                              <enumeration value = "Other"/>
327                            </restriction>
328                          </simpleType>
329                        </element>
330                        <element name = "event" type = "string"/>
331                        <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
332                          <simpleType>
333                            <restriction base = "string">
334                              <enumeration value = "Shelter"/>
335                              <enumeration value = "Evacuate"/>
336                              <enumeration value = "Prepare"/>
337                              <enumeration value = "Execute"/>
338                              <enumeration value = "Monitor"/>
339                              <enumeration value = "None"/>
340                            </restriction>
341                          </simpleType>
342                        </element>
343                        <element name = "urgency">
344                          <simpleType>
345                            <restriction base = "string">
346                              <enumeration value = "Immediate"/>
347                              <enumeration value = "Expected"/>
348                              <enumeration value = "Future"/>
349                              <enumeration value = "Past"/>
350                              <enumeration value = "Unknown"/>
351                            </restriction>
352                          </simpleType>
353                        </element>
354                        <element name = "severity">
355                          <simpleType>
```

```
356                                    <restriction base = "string">
357                                      <enumeration value = "Extreme"/>
358                                      <enumeration value = "Severe"/>
359                                      <enumeration value = "Moderate"/>
360                                      <enumeration value = "Minor"/>
361                                      <enumeration value = "Unknown"/>
362                                    </restriction>
363                                  </simpleType>
364                                </element>
365                                <element name = "certainty">
366                                  <simpleType>
367                                    <restriction base = "string">
368                                      <enumeration value = "Observed"/>
369                                      <enumeration value = "Likely"/>
370                                      <enumeration value = "Possible"/>
371                                      <enumeration value = "Unlikely"/>
372                                      <enumeration value = "Unknown"/>
373                                    </restriction>
374                                  </simpleType>
375                                </element>
376                                <element name = "audience" type = "string" minOccurs = "0"/>
377                                <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
378                                  <complexType>
379                                    <sequence>
380                                      <element ref = "cap:valueName"/>
381                                      <element ref = "cap:value"/>
382                                    </sequence>
383                                  </complexType>
384                                </element>
385                                <element name = "effective" type = "dateTime" form = "qualified" minOccurs = "0"/>
386                                <element name = "onset" type = "dateTime" minOccurs = "0"/>
387                                <element name = "expires" type = "dateTime" minOccurs = "0"/>
388                                <element name = "senderName" type = "string" minOccurs = "0"/>
389                                <element name = "headline" type = "string" minOccurs = "0"/>
390                                <element name = "description" type = "string" minOccurs = "0"/>
391                                <element name = "instruction" type = "string" minOccurs = "0"/>
392                                <element name = "web" type = "anyURI" minOccurs = "0"/>
393                                <element name = "contact" type = "string" minOccurs = "0"/>
394                                <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
395                                  <complexType>
396                                    <sequence>
397                                      <element ref = "cap:valueName"/>
398                                      <element ref = "cap:value"/>
399                                    </sequence>
400                                  </complexType>
401                                </element>
402                                <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
403                                  <complexType>
404                                    <sequence>
405                                      <element name = "resourceDesc" type = "string"/>
406                                      <element name = "mimeType" type = "string" minOccurs = "0"/>
407                                      <element name = "size" type = "integer" minOccurs = "0"/>
408                                      <element name = "uri" type = "anyURI" minOccurs = "0"/>
409                                      <element name = "derefUri" type = "string" minOccurs = "0"/>
410                                      <element name = "digest" type = "string" minOccurs = "0"/>
411                                    </sequence>
412                                  </complexType>
413                                </element>
414                                <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
415                                  <complexType>
416                                    <sequence>
417                                      <element name = "areaDesc" type = "string"/>
418                                      <element name = "polygon" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
419                                      <element name = "circle" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
420                                      <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
421                                        <complexType>
422                                          <sequence>
423                                            <element ref = "cap:valueName"/>
424                                            <element ref = "cap:value"/>
425                                          </sequence>
426                                        </complexType>
427                                      </element>
428                                      <element name = "altitude" type = "string" minOccurs = "0"/>
429                                      <element name = "ceiling" type = "string" minOccurs = "0"/>
430                                    </sequence>
431                                  </complexType>
432                                </element>
433                            </sequence>
434                          </complexType>
435                        </element>
436                      </sequence>
437                    </complexType>
```

```
438        </element>
439        <element name = "valueName" type = "string"/>
440        <element name = "value" type = "string"/>
441   </schema>
442
```

443 Appendix A. CAP Alert Message Example

444 A.1. Homeland Security Advisory System Alert

445 The following is a speculative example in the form of a CAP XML message.

```
446
447  <?xml version = "1.0" encoding = "UTF-8"?>
448  <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
449    <identifier>43b080713727</identifier>
450    <sender>hsas@dhs.gov</sender>
451    <sent>2003-04-02T14:39:01-05:00</sent>
452    <status>Actual</status>
453    <msgType>Alert</msgType>
454    <scope>Public</scope>
455    <info>
456      <category>Security</category>
457      <event>Homeland Security Advisory System Update</event>
458      <urgency>Immediate</urgency>
459      <severity>Severe</severity>
460      <certainty>Likely</certainty>
461      <senderName>U.S. Government, Department of Homeland Security</senderName>
462      <headline>Homeland Security Sets Code ORANGE</headline>
463      <description>The Department of Homeland Security has elevated the Homeland Security Advisory
464  System threat level to ORANGE / High in response to intelligence which may indicate a heightened
465  threat of terrorism.</description>
466      <instruction> A High Condition is declared when there is a high risk of terrorist attacks. In
467  addition to the Protective Measures taken in the previous Threat Conditions, Federal departments
468  and agencies should consider agency-specific Protective Measures in accordance with their
469  existing plans.</instruction>
470      <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
471      <parameter>
472        <valueName>HSAS</valueName>
473        <value>ORANGE</value>
474      </parameter>
475      <resource>
476        <resourceDesc>Image file (GIF)</resourceDesc>
477        <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
478      </resource>
479      <area>
480        <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
481      </area>
482    </info>
483  </alert>
484
```

A.2. Severe Thunderstorm Warning

The following is a speculative example in the form of a CAP XML message.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
  <identifier>KSTO1055887203</identifier>
  <sender>KSTO@NWS.NOAA.GOV</sender>
  <sent>2003-06-17T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Met</category>
    <event>SEVERE THUNDERSTORM</event>
    <responseType>Shelter</responseType>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <eventCode>
      <valueName>same</valueName>
      <value>SVR</value>
    </eventCode>
    <expires>2003-06-17T16:00:00-07:00</expires>
    <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
    <headline>SEVERE THUNDERSTORM WARNING</headline>
    <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED A SEVERE
THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES SOUTHEAST OF KIRKWOOD...MOVING
SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY WITH THIS
STORM.</description>
    <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES.</instruction>
    <contact>BARUFFALDI/JUSKIE</contact>
    <area>
      <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME NORTHEASTERN
CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN CALIFORNIA</areaDesc>
      <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>006109</value>
      </geocode>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>006009</value>
      </geocode>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>006003</value>
      </geocode>
    </area>
  </info>
</alert>
```

536 A.3. Earthquake Report

537 The following is a speculative example in the form of a CAP XML message.

```
538
539 <?xml version = "1.0" encoding = "UTF-8"?>
540 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
541   <identifier>TRI13970876.1</identifier>
542   <sender>trinet@caltech.edu</sender>
543   <sent>2003-06-11T20:56:00-07:00</sent>
544   <status>Actual</status>
545   <msgType>Alert</msgType>
546   <scope>Public</scope>
547   <incidents>13970876</incidents>
548   <info>
549     <category>Geo</category>
550     <event>Earthquake</event>
551     <urgency>Past</urgency>
552     <severity>Minor</severity>
553     <certainty>Observed</certainty>
554     <senderName>Southern California Seismic Network (TriNet) operated by Caltech and
555 USGS</senderName>
556     <headline>EQ 3.4 Imperial County CA - PRELIMINARY REPORT</headline>
557     <description>A minor earthquake measuring 3.4 on the Richter scale occurred near Brawley,
558 California at 8:53 PM Pacific Daylight Time on Wednesday, June 11, 2003. (This is a computer-
559 generated solution and has not yet been reviewed by a human.)</description>
560     <web>http://www.trinet.org/scsn/scsn.html</web>
561     <parameter>
562       <valueName>EventID</valueName>
563       <value>13970876</value>
564     </parameter>
565     <parameter>
566       <valueName>Version</valueName>
567       <value>1</value>
568     </parameter>
569     <parameter>
570       <valueName>Magnitude</valueName>
571       <value>3.4 Ml</value>
572     </parameter>
573     <parameter>
574       <valueName>Depth</valueName>
575       <value>11.8 mi.</value>
576     </parameter>
577     <parameter>
578       <valueName>Quality</valueName>
579       <value>Excellent</value>
580     </parameter>
581     <area>
582       <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of OCOTILLO
583 (quarry); 1 mi. N of the Imperial Fault</areaDesc>
584       <circle>32.9525,-115.5527 0</circle>
585     </area>
586   </info>
587 </alert>
```

588 A.4. AMBER Alert (Including EAS Activation)

589 The following is a speculative example in the form of a CAP XML message.

590
```xml
591 <?xml version = "1.0" encoding = "UTF-8"?>
592 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
593    <identifier>KAR0-0306112239-SW</identifier>
594    <sender>KARO@CLETS.DOJ.CA.GOV</sender>
595    <sent>2003-06-11T22:39:00-07:00</sent>
596    <status>Actual</status>
597    <msgType>Alert</msgType>
598    <source>SW</source>
599    <scope>Public</scope>
600    <info>
601       <category>Rescue</category>
602       <event>Child Abduction</event>
603       <urgency>Immediate</urgency>
604       <severity>Severe</severity>
605       <certainty>Likely</certainty>
606       <eventCode>
607          <valueName>SAME</valueName>
608          <value>CAE</value>
609       </eventCode>
610       <senderName>LOS ANGELES POLICE DEPT - LAPD</senderName>
611       <headline>AMBER ALERT</headline>
612       <description>DATE/TIME: 06/11/03, 1915 HRS.  VICTIM(S): KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
613 LBS. LIGHT COMPLEXION.  DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BLUE COLLAR.
614 LOCATION: 5721 DOE ST., LOS ANGELES, CA.  SUSPECT(S): KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
615 BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
616       <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
617       <area>
618          <areaDesc>Los Angeles County</areaDesc>
619          <geocode>
620             <valueName>SAME</valueName>
621             <value>006037</value>
622          </geocode>
623       </area>
624    </info>
625 </alert>
626
```

Appendix B.   Acknowledgments

OASIS Emergency Management Technical Committee

John Aerts, LA County Information Systems Advisory Body
Patti Aymond, IEM
Mark Benemerito, Sungard Availability Services
Jeff Berg, Motorola
Art Botterell, Partnership for Public Warning
Chris Branton, IEM
Rex Brooks, HumanMarkup.org, Inc.
Thomas Bui, The Boeing Company
Len Bullard, Individual
Charles Campbell, Individual
Richard Carlton, Individual
Eliot Christian, US Department of the Interior
Marc Connolly, Oracle
Robin Cover, OASIS
Michael Daconta, US Department of Homeland Security
David Danko, ESRI
Paul Denning, Mitre Corporation
John Dias, Lawrence Livermore National Laboratory
Matthew Dovey, Oxford University
Sukumar Dwarkanath, Individual
Scott Edson, LA County Information Systems Advisory Body
Nasseam Elkarra, Individual
David, Ellis, Individual
Paul Embley, Individual
Jack Fox, US Department of Homeland Security
Lawrence Freudinger, NASA
Gary Ham, Disaster Management Interoperability Services
Travis Hubbard, Disaster Management Interoperability Services
Stephen Jepsen, Oracle
Elysa Jones, Warning Systems, Inc.
Joyce Kern, Sungard Availability Services
Hong-Eng Koh, Sun Microsystems
Jeff Kyser, Warning Systems, Inc.
Louis Lagonik, Lockheed Martin
Kim Lambert, LMI Government Consulting
Richard Masline, IBM
Carl Mattocks, Individual
Maurice McGinley, Individual
Tom Merkle, Lockheed Martin
Bona Nasution, MTG Management Consultants, LLC.
Steve Ollis, Individual
Ash Parikh, Raining Data Corporation
Brian Pattinson, Unisys Corporation
Gary Poindexter, Individual
Walid Ramadan, Individual
Michelle Raymond, Individual
Carl Reed, Open GIS Consortium (OGC)
Kent Reed, NIST
Jeffrey Ricker, Individual
David Roberts, Unisys Corporation

679   Dave Robinson, Wells Fargo
680   Eleanor Robinson, Anteon Corporation
681   John Ruegg, LA County Information Systems Advisory Body
682   Barry Schaeffer, Individual
683   William Schroeder, ESRI
684   John Silva, Individual
685   Kwasi Speede, Anteon Corporation
686   Michael Thompson, The Boeing Company
687   Rob Torchon, E Team
688   Brett Trusko, OASIS
689   Rick Tucker, Mitre Corporation
690   Richard Vandame, US Department of Homeland Security
691   Jerry Weltman, IEM
692   Preston Werntz, Individual
693   Konstantin Wilms, Individual
694   Bob Wyman Individual
695   Jack Zhang Beijing Harmony Technologies Co, Ltd
696

697 # Appendix C.   Revision History

Rev	Date	By Whom	What
1.1	2005-07-27	Art Botterell	Edits to conform object model, data dictionary and schema: • Reordered items in object diagram and data dictionary to match sequence required by schema. • Edited schema to make <scope> mandatory and to permit multiple instances of <responseType> and <eventCode>, in accordance with the data dictionary.
1.1	2005-07-23	Art Botterell	Applied changes per recommendations of Messaging Subcommittee based on initial public comment period: • Modified XML syntax of <eventCode> , <parameter> and <geocode> • Added "Draft" value for <status> • Changed CAP namespace to URN form • Tightened usage of dateTime formats in <sent>, <effective>, <onset> and <expiration> • Corrected schema to correct value of "CBRNE" in <event> • Conformed examples in Appendix A to new namespace.
1.1	2005-04-28	Elysa Jones	Technical Committee approved the v. 1.1 draft with the following additional changes: • Normative language added to specify uniqueness of <identifier> • Change [dateTime] format for <sent>, <effective>, <onset> and <expires> elements • Change <language> element RFC from 1166 to 3066 and added null • Changed the <mineType> element RFC 1521 to 2046 • Added <derefURI> element • Security Note updated and added Digital Signature and Encryption note paragraphs
1.1	2005-01-04	Art Botterell	Messaging Subcommittee approved v. 1.1 draft for submission to full Technical Committee: • Added <responseType> element • Made <category> element mandatory • Amended enumerated values for the <certainty> element • Deleted the <password> element • Various editorial corrections and clarifications
1.0	2004-04-01	Art Botterell	CAP 1.0 adopted as OASIS Standard (see CAP 1.0 specification document for prior change history.)

698