



Common Alerting Protocol, v. 1.0

Committee Draft, 10 February 2004

Document identifier:

emergency-CAP-1.0

Location:

<http://www.oasis-open.org/committees/emergency/>

Editor:

Art Botterell, Partnership for Public Warning <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/>).

Table of Contents

1. INTRODUCTION.....	3
1.1. PURPOSE	3
1.2. HISTORY	3
1.3. STRUCTURE OF THE CAP ALERT MESSAGE.....	3
1.3.1. <alert>	3
1.3.2. <info>.....	3
1.3.3. <resource>.....	4
1.3.4. <area>	4
1.4. APPLICATIONS OF THE CAP ALERT MESSAGE.....	4
1.5. TERMINOLOGY	4
1.6. NORMATIVE REFERENCES.....	4
2. DESIGN PRINCIPLES AND CONCEPTS (NON-NORMATIVE).....	5
2.1. DESIGN PHILOSOPHY	5
2.2. REQUIREMENTS FOR DESIGN	5
2.3. EXAMPLES OF USE SCENARIOS	6
2.3.1. <i>Manual Origination</i>	6
2.3.2. <i>Automated Origination by Autonomous Sensor System</i>	6
2.3.3. <i>Aggregation and Correlation on Real-time Map</i>	6
2.3.4. <i>Integrated Public Alerting</i>	6
2.3.5. <i>Repudiating A False Alarm</i>	7
3. ALERT MESSAGE STRUCTURE (NORMATIVE).....	8
3.1. DOCUMENT OBJECT MODEL.....	8
3.2. DATA DICTIONARY.....	9
3.2.1. <i>"alert" Element and Sub-elements</i>	9
3.2.2. <i>"info" Element and Sub-elements</i>	11
3.2.3. <i>"resource" Element and Sub-elements</i>	15
3.2.4. <i>"area" Element and Sub-elements</i>	16
3.3. IMPLEMENTATION NOTES.....	18
3.3.1. <i>WGS-84 Note</i>	18
3.3.2. <i>Coordinate Precision Note</i>	18
3.3.3. <i>Security Note</i>	18
3.4. XML SCHEMA.....	19
APPENDIX A. CAP ALERT MESSAGE EXAMPLE	22
A.1. HOMELAND SECURITY ADVISORY SYSTEM ALERT.....	22
A.2. SEVERE THUNDERSTORM WARNING.....	23
A.3. EARTHQUAKE REPORT	24
A.4. AMBER ALERT.....	25
APPENDIX B. ACKNOWLEDGMENTS.....	26
B.1. OASIS EMERGENCY MANAGEMENT TECHNICAL COMMITTEE	26
A.5. COMMON ALERTING PROTOCOL WORKING GROUP.....	27
B.2. PARTNERSHIP FOR PUBLIC WARNING	27
B.3. ADDITIONAL CONTRIBUTORS	28
APPENDIX C. REVISION HISTORY	29
APPENDIX D. NOTICES.....	31

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 NOAA Weather Radio and the Emergency Alert System, 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;
- Facility for 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.

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

Within this document 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.

1.6. Normative References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

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 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:

1. Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
2. Enable integration of diverse sensor, threat-evaluation and dissemination systems;
3. Be usable over multiple transmission systems, including both TCP/IP-based networks and one-way "broadcast" channels;
4. Support credible end-to-end authentication and validation of all messages;
5. Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
6. Provide for multiple message types, such as:
 - a. Warnings
 - b. Acknowledgements
 - c. Expirations and cancellations
 - d. Updates and amendments
 - e. Reports of results from dissemination systems
 - f. Administrative and system messages
7. Provide for flexible description of each warning's:
 - a. Geographic targeting
 - b. Level of urgency
 - c. Level of certainty

- d. Level of threat severity
8. Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
9. Use an established open-standard data representation;
10. Be based on a program of real-world cross-platform testing and evaluation;
11. Provide a clear basis for certification and further protocol evaluation and improvement; and,
12. Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

2.3. Examples of Use Scenarios

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

2.3.1. Manual Origination

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

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

2.3.2. Automated Origination by Autonomous Sensor System

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

2.3.3. Aggregation and Correlation on Real-time Map

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

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

2.3.4. Integrated Public Alerting

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

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

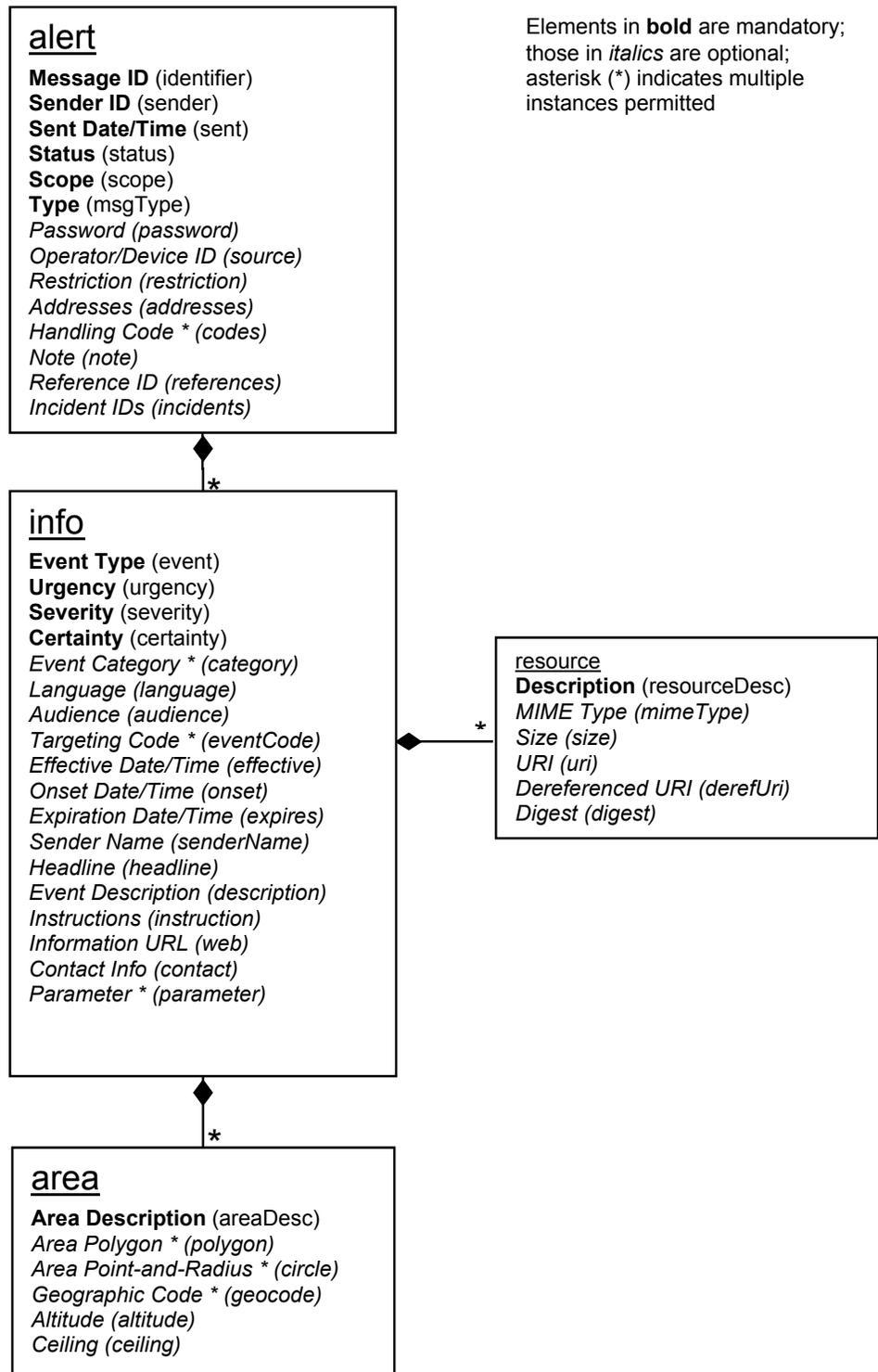
“In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also get corroboration of the alert through multiple channels, which increases the chance of the warning being acted upon.”

2.3.5. Repudiating A False Alarm

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

3. Alert Message Structure (normative)

3.1. Document Object Model



3.2. Data Dictionary

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)	<p>(1) Surrounds CAP alert message sub-elements.</p> <p>(2) MUST include the xmlns attribute referencing the CAP URI as the namespace, e.g.: <pre><cap:alert xmlns:cap="http://www.incident.com/cap/1.0"> [sub-elements] </cap:alert></pre> </p> <p>(3) In addition to the specified sub-elements, MAY contain one or more <info> blocks.</p>
identifier	cap. alert. identifier	The identifier of the alert message (REQUIRED)	<p>(1) A number or string uniquely identifying this message, assigned by the sender</p> <p>(2) MUST NOT include spaces or restricted characters (< and &)</p>
sender	cap. alert. sender. identifier	The identifier of the sender of the alert message (REQUIRED)	<p>(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name</p> <p>(2) MUST NOT include spaces or restricted characters (< and &)</p>
password	cap. alert. password. string	The string representing the password of the alert message (OPTIONAL)	Used for authenticating the sender. Note that this element should only be used on secure channels. Note also that simple password authentication schemes have numerous well-known weaknesses.
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.
sent	cap. alert. sent. time	The time and date of the origination of the alert message (REQUIRED)	The date and time is represented in ISO 8601 format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT).

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
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)
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)	Any user-defined flag or special code used to flag the alert message for special handling.

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 <reference> "Cancel" - Cancels the earlier message(s) identified in <reference> "Ack" - Acknowledges receipt and acceptance of the message(s) identified in <reference> "Error" indicates rejection of the message(s) identified in <reference>; explanation SHOULD appear in <note>
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 <i>identifier/ sender</i>) of an earlier message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.
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			
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 1766. (2) If not present, assumed value is "en-US".
category	cap. alertInfo. category. code	The code denoting the category of the subject event of the alert message (OPTIONAL)	(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 "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)	The text MAY use a specified nomenclature if available.
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

severity	cap. alertInfo. severity. code	The code denoting the severity of the subject event of the alert message (REQUIRED)	<p>(1) The “urgency”, “severity”, and “certainty” elements collectively distinguish less emphatic from more emphatic messages.</p> <p>(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</p>
certainty	cap. alertInfo. certainty. code	The code denoting the certainty of the subject event of the alert message (REQUIRED)	<p>(1) The “urgency”, “severity”, and “certainty” elements collectively distinguish less emphatic from more emphatic messages.</p> <p>(2) Code Values: “Very Likely” - Highly likely (p > ~ 85%) or certain “Likely” - Likely (p > ~50%) “Possible” - Possible but not likely (p <= ~50%) “Unlikely” - Not expected to occur (p ~ 0) “Unknown” - Certainty unknown</p>
audience	cap. alertInfo. audience. text	The text describing the intended audience of the alert message (OPTIONAL)	
eventCode	cap. alertInfo. event. code	The system-specific code identifying the event type of the alert message (OPTIONAL)	<p>(1) Code Values: Any system-specific code for event typing, in the form "code_type= code" where "code_type" is a user-assigned designator for the target system (e. g., "same=CEM"). Designators MUST NOT include spaces or XML-restricted characters (<, >, &, ',").</p> <p>(2) Multiple instances MAY occur within a single <info> block.</p>
effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	<p>The date and time is represented in ISO 8601 format (e. g., “2002-05-24T16:49:00-07:00” for 24 May 2002 at 16: 49 PDT).</p> <p>If this item is not included, the effective time is assumed to be the same as in <sent>.</p>

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 ISO 8601 format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT). (2) If this item is not included, the onset time is assumed to be the same as in <sent>.
expires	cap. alertInfo. expires. time	The expiry time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in ISO 8601 format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT). (2) If this item is not provided, each recipient is free to set its own policy as to when the message is not 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 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)	
instruction	cap. alertInfo. instruction. text	The text describing the recommended action to be taken by recipients of the alert message (OPTIONAL)	
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	The group listing of additional parameters associated with the alert message (OPTIONAL)	(1) Code Values: Parameter label / value pair(s) in the form "label=value". (2) Multiple instances MAY occur within a single <info> block.

3.2.3. "resource" Element and Sub-elements

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.
contentType	cap. alertInfoResource. contentType. 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 1521
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	Approximate size 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.

derefUri	cap. alertInfoResource. derefUri. data	The base-64 encoded data content of the resource file (conditional)	<ol style="list-style-type: none"> (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 Publication 180-1
3.2.4. "area" Element and Sub-elements			
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)	<ol style="list-style-type: none"> (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.
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)	<ul style="list-style-type: none"> (1) Code Values: The geographic polygon is represented by a whitespace-delimited list of WGS-84 coordinate values. (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)	<ul style="list-style-type: none"> (1) Code Values: The circular area is represented by a central point given as a WGS-84 coordinates value 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>.
geocode	cap. alertInfoArea. geocode. code	The geographic code delineating the affected area of the alert message (OPTIONAL)	<ul style="list-style-type: none"> (1) Code Values: Any geographically-based code to describe message target area, generally in the form "code_type=code" where "code_type" is a user-assigned abbreviation for the target system (e. g., "fips6=06003"). (2) Multiple instances MAY occur within an <area>. (3) 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)	<ul style="list-style-type: none"> (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)	<ul style="list-style-type: none"> (1) MUST NOT be used except in combination with the <altitude> element (2) The altitude measure is in feet above mean sea level per the WGS-84 datum.

3.3. Implementation Notes

3.3.1. WGS-84 Note

Geographic locations in CAP are defined using WGS 84 (World Geodetic System 1984), equivalent to EPSG (European Petroleum Survey Group) code 4326 (2 dimensions). CAP does not assign responsibilities for coordinate transformations from and to other Spatial Reference Systems. A WGS-84 coordinate value is here represented as a comma-delimited latitude/longitude pair, measured in decimal degrees (un-projected). Latitudes range from -90 to 90 and longitudes range from -180 to 180. Coordinates in the Southern and Western hemispheres are signed negative with a leading dash.

3.3.2. Coordinate Precision Note

Developers of geographic facilities are urged to exercise caution in the alignment of "precision" to "accuracy". For example, consider the possible accuracy of a world map comprising 360 degrees longitude by 180 degrees latitude. When displayed at 400 pixels wide by 200 pixels, the accuracy per pixel can be no more than a single unit of longitude and latitude. The precision of the WGS-84 values in the example should therefore be whole degrees, not some number of decimal places.

3.3.3. Security Note

Where applicable, the OASIS WS-Security framework is recommended as the basis for ensuring message authenticity, integrity and (where required) confidentiality.

3.4. XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
  targetNamespace = "http://www.incident.com/cap/1.0"
  xmlns:cap = "http://www.incident.com/cap/1.0"
  xmlns:xs = "http://www.w3.org/2001/XMLSchema"
  elementFormDefault = "qualified"
  attributeFormDefault = "unqualified">
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.0)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "identifier" type = "string"/>
        <element name = "sender" type = "string"/>
        <element name = "sent" type = "dateTime"/>
        <element name = "status">
          <simpleType name = "status">
            <restriction base = "string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "msgType">
          <simpleType name = "msgType" >
            <restriction base = "string">
              <enumeration value = "Alert"/>
              <enumeration value = "Update"/>
              <enumeration value = "Cancel"/>
              <enumeration value = "Ack"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "password" type = "string" minOccurs = "0"/>
        <element name = "source" type = "string" minOccurs = "0"/>
        <element name = "scope" minOccurs = "0">
          <simpleType name = "scope">
            <restriction base = "string">
              <enumeration value = "Public"/>
              <enumeration value = "Restricted"/>
              <enumeration value = "Private"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "restriction" type = "string" minOccurs = "0"/>
        <element name = "addresses" type = "string" minOccurs = "0"/>
        <element name = "code" type = "string" minOccurs = "0" maxOccurs =
"unbounded"/>
        <element name = "note" type = "string" minOccurs = "0"/>
        <element name = "references" minOccurs = "0">
          <simpleType name = "references">
            <list itemType = "string"/>
          </simpleType>
        </element>
        <element name = "incidents" minOccurs = "0">
          <simpleType name = "incidents">
            <list itemType = "string"/>
          </simpleType>
        </element>
        <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
          <complexType>
            <sequence>
```

```

        <element name = "language" type = "language" default = "en-US"
minOccurs = "0"/>
        <element name = "category" minOccurs = "0" maxOccurs =
"unbounded">
            <simpleType name = "category">
                <restriction base = "string">
                    <enumeration value = "Geo"/>
                    <enumeration value = "Met"/>
                    <enumeration value = "Safety"/>
                    <enumeration value = "Security"/>
                    <enumeration value = "Rescue"/>
                    <enumeration value = "Fire"/>
                    <enumeration value = "Health"/>
                    <enumeration value = "Env"/>
                    <enumeration value = "Transport"/>
                    <enumeration value = "Infra"/>
                    <enumeration value = "Other"/>
                </restriction>
            </simpleType>
        </element>
        <element name = "event" type = "string"/>
        <element name = "urgency">
            <simpleType name = "urgency">
                <restriction base = "string">
                    <enumeration value = "Immediate"/>
                    <enumeration value = "Expected"/>
                    <enumeration value = "Future"/>
                    <enumeration value = "Past"/>
                    <enumeration value = "Unknown"/>
                </restriction>
            </simpleType>
        </element>
        <element name = "severity">
            <simpleType name = "severity">
                <restriction base = "string">
                    <enumeration value = "Extreme"/>
                    <enumeration value = "Severe"/>
                    <enumeration value = "Moderate"/>
                    <enumeration value = "Minor"/>
                    <enumeration value = "Unknown"/>
                </restriction>
            </simpleType>
        </element>
        <element name = "certainty">
            <simpleType name = "certainty" >
                <restriction base = "string">
                    <enumeration value = "Very Likely"/>
                    <enumeration value = "Likely"/>
                    <enumeration value = "Possible"/>
                    <enumeration value = "Unlikely"/>
                    <enumeration value = "Unknown"/>
                </restriction>
            </simpleType>
        </element>
        <element name = "audience" type = "string" minOccurs = "0"/>
        <element name = "eventCode" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
        <element name = "effective" type = "dateTime" minOccurs = "0"/>
        <element name = "onset" type = "dateTime" minOccurs = "0"/>
        <element name = "expires" type = "dateTime" minOccurs = "0"/>
        <element name = "senderName" type = "string" minOccurs = "0"/>
        <element name = "headline" type = "string" minOccurs = "0"/>
        <element name = "description" type = "string" minOccurs = "0"/>
        <element name = "instruction" type = "string" minOccurs = "0"/>
        <element name = "web" type = "anyURI" minOccurs = "0"/>
        <element name = "contact" type = "string" minOccurs = "0"/>
        <element name = "parameter" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
        <element name = "resource" minOccurs = "0" maxOccurs =
"unbounded">

```

```

    <complexType>
      <sequence>
        <element name = "resourceDesc" type = "string"/>
        <element name = "mimeType" type = "string" minOccurs = "0"/>
        <element name = "size" type = "integer" minOccurs = "0"/>
        <element name = "uri" type = "anyURI" minOccurs = "0"/>
        <element name = "derefUri" type = "string" minOccurs = "0"/>
        <element name = "digest" type = "string" minOccurs = "0"/>
      </sequence>
    </complexType>
  </element>
  <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
    <complexType>
      <sequence>
        <element name = "areaDesc" type = "string"/>
        <element name = "polygon" minOccurs = "0" maxOccurs =
"unbounded">
          <simpleType name = "polygon">
            <list itemType = "string"/>
          </simpleType>
        </element>
        <element name = "circle" minOccurs = "0" maxOccurs =
"unbounded">
          <simpleType name = "circle">
            <list itemType = "string"/>
          </simpleType>
        </element>
        <element name = "geocode" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
        <element name = "altitude" type = "string" minOccurs = "0"/>
        <element name = "ceiling" type = "string" minOccurs = "0"/>
      </sequence>
    </complexType>
  </element>
</sequence>
</complexType>
</element>
</schema>

```

Appendix A. CAP Alert Message Example

A.1. Homeland Security Advisory System Alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/1.0">
  <identifier>43b080713727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Security</category>
    <event>Homeland Security Advisory System Update</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <senderName>U.S. Government, Department of Homeland Security</senderName>
    <headline>Homeland Security Sets Code ORANGE</headline>
    <description>The Department of Homeland Security has elevated the Homeland
Security Advisory System threat level to ORANGE / High in response to
intelligence which may indicate a heightened threat of terrorism.</description>
    <instruction> A High Condition is declared when there is a high risk of
terrorist attacks. In addition to the Protective Measures taken in the previous
Threat Conditions, Federal departments and agencies should consider agency-
specific Protective Measures in accordance with their existing
plans.</instruction>
    <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
    <parameter>HSAS=ORANGE</parameter>
    <resource>
      <resourceDesc>Image file (GIF)</resourceDesc>
      <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
    </resource>
    <area>
      <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
    </area>
  </info>
</alert>
```

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 = "http://www.incident.com/cap/1.0">
  <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>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <eventCode>same=SVR</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>fips6=006109</geocode>
      <geocode>fips6=006009</geocode>
      <geocode>fips6=006003</geocode>
    </area>
  </info>
</alert>
```

A.3. Earthquake Report

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/1.0">
  <identifier>TRI13970876.1</identifier>
  <sender>trinet@caltech.edu</sender>
  <sent>2003-06-11T20:56:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <incidents>13970876</incidents>
  <info>
    <category>Geo</category>
    <event>Earthquake</event>
    <urgency>Past</urgency>
    <severity>Minor</severity>
    <certainty>Very Likely</certainty>
    <senderName>Southern California Seismic Network (TriNet) operated by Caltech
and USGS</senderName>
    <headline>EQ 3.4 Imperial County CA - PRELIMINARY REPORT</headline>
    <description>A minor earthquake measuring 3.4 on the Richter scale occurred
near Brawley, California at 8:53 PM Pacific Daylight Time on Wednesday, June 11,
2003. (This is a computer-generated solution and has not yet been reviewed by a
human.)</description>
    <web>http://www.trinet.org/scsn/scsn.html</web>
    <parameter>EventID=13970876</parameter>
    <parameter>Version=1</parameter>
    <parameter>Magnitude=3.4 Ml</parameter>
    <parameter>Depth=11.8 mi.</parameter>
    <parameter>Quality=Excellent</parameter>
    <area>
      <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of
OCOTILLO (quarry); 1 mi. N of the Imperial Fault</areaDesc>
      <circle>32.9525,-115.5527 0</circle>
    </area>
  </info>
</alert>
```

A.4. AMBER Alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/1.0">
  <identifier>KAR0-0306112239-SW</identifier>
  <sender>KAR0@CLETS.DDJ.CA.GOV</sender>
  <sent>2003-06-11T22:39:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <source>SW</source>
  <scope>Public</scope>
  <info>
    <category>Rescue</category>
    <event>Child Abduction</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <eventCode>same=CAE</eventCode>
    <senderName>LOS ANGELES POLICE DEPT - LAPD</senderName>
    <headline>AMBER ALERT</headline>
    <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE JR. M/B
    BLK/BRO 3'0", 40 LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE
    T-SHIRT, W/BLUE COLLAR. LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S):
    KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR, BRO EYE. VEHICLE: 81' BUICK 2-DR,
    BLUE (4XXX000).</description>
    <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-
    2389</contact>
    <area>
      <areaDesc>Los Angeles County</areaDesc>
      <geocode>fips6=006037</geocode>
    </area>
  </info>
</alert>
```

Appendix B. Acknowledgments

B.1. OASIS Emergency Management Technical Committee

John Aerts, LA County Information Systems Advisory Body
Mark Benemerito, Sungard Availability Services
Dr. Arne Berre, SINTEF
Art Botterell, Partnership for Public Warning
Dr. Chris Branton, IEM
Rex Brooks
Dr. Thomas Bui, The Boeing Company
Len Bullard, Systems Analyst
Richard Carlton, Senior Partner, Consultrac
Eliot, Christian, US Department of the Interior
Jay Clark, Ship Analytics
Marc Connolly, Oracle
Robin Cover, OASIS
Jaganath Dabbi
David Danko, ESRI
Paul Denning, Mitre Corporation
Matthew Dovey, Technical Manager
Tertius Eksteen, Booz Allen Hamilton
Nasseam Elkarra
Paul Embley
Lawrence Freudinger, NASA
J Gordon, Ramsafe Technologies
David Hall, NIJ Project Manager
Gary Ham, Disaster Management Interoperability Services
Andre Hiotis, Security Officer
M Isenberg, Verisign
Stephen Jepsen, Oracle
Joyce Kern, Sungard Availability Services,
Kim Lambert, Logistics Management Institute
Steven Markman, Principal Scientist
Carl Mattocks
Maurice McGinley, Researcher
Tom Merkle, ACS
James Morentz, Science Applications International Corporation
Bona Nasution, MTG Management Consultants, LLC.
Steve Ollis, Vice President
Brian Pattinson, Unisys Corporation,
Gary Poindexter
Walid Ramadan, Product Manager
Carl Reed, OpenGIS Consortium (OGC)
Jeffrey Ricker
David Roberts, Unisys Corporation
Dave Robinson, Wells Fargo
Eleanor Robinson, Technical Manager (Anteon)
John Ruegg, LA County Information Systems Advisory Body
Barry Schaeffer
William Schroeder, ESRI
Steven Seigel, Ramsafe Technologies
Dr. John Silva
Fred Simonet, Ship Analytics
Kwasi Speede, Emergency Coordination Task Lead (Anteon)
Michael Thompson, The Boeing Company
Rob Torchon, E Team
Dr Brett Trusko, OASIS
Rick Tucker, Mitre Corporation

Jerry Weltman, IEM
Preston Wernitz, System Architect
Konstantin Wilms Senior Systems Design Engineer
Michael Wilson
Allen Wyke, Blue292 (Chair)
Jack Zhang, Beijing Harmony Technologies Co, Ltd

A.5. Common Alerting Protocol Working Group

The initial design and demonstration of the Common Alerting Protocol Alert Message was performed by the Common Alerting Protocol Working Group, an ad-hoc committee of more than 130 emergency management and technology practitioners, including:

Douglas Allport, The Allport Group
Rex Buddenberg, Naval Postgraduate School
Bill Butler, Los Angeles County Office of Emergency Management
Neil Briscoe, QinetiQ (Great Britain)
Kim Carsell, David Ford Consulting Engineers
Phillip S. Cogan, Bernstein Communications
Denis DesRosiers, CARIS-Universal Systems (Canada)
Brian Dopp, Phoenix Disaster Services
Paul Erling, Enera, Inc.
Darrell Ernst, The MITRE Corporation
John Fleming, Florida Emergency Management Agency
Kevin Farrell, Aberdeen Proving Ground
Lawrence C. Freudinger, NASA Dryden Flight Research Center
David Gillen, mobileFOUNDATIONS
Ben Green, California Office of Emergency Services
Patrick Halley, The ComCARE Alliance
Al Kenyon, Clear Channel Communications
Elizabeth Klute, Contra Costa County (CA) Community Warning System
Elden P. Laffoon, Sr., Midwest Computer Technical
Dave Luneau, Classco
Michael McGuire, Oregon Department of Human Services
Peter B. Olinger, Lockheed Martin Space & Strategic Missiles
David Oppenheimer, United States Geological Survey
Rick Paige, Mendocino County (CA) Emergency Services Authority
Darryl Parker, TFT
Efraim Petel, HormannAmerica,
David E. Price, Lawrence Livermore National Laboratory
Valerie Quigley, Lawrence Berkeley Laboratory
Bob Robinson, Business Recovery Managers Association
Don Root, California Office of Emergency Services
Ben Rotholtz, Real Networks
Richard Rudman, EAS Consultant
Van H. Schallenberg, Professional Engineer
Craig Schmidt, National Weather Service
Jeffrey Silberberg, CompuDesigns
Ingo Simonis, University of Muenster (Germany)
John Sokich, National Weather Service
Chris Warner, Earth911
Gram Wheeler, Microsoft
Theodore A. Wolf Jr., Search & Rescue Council of New Jersey

B.2. Partnership for Public Warning

The Common Alerting Protocol was sponsored into the OASIS standards process by the Trustees of the Partnership for Public Warning, a national non-profit institute devoted to the enhancement and expansion of effective public warning systems in the U.S, and internationally. Their support is gratefully acknowledged.

B.3. Additional Contributors

Kenneth Allen, Partnership for Public Warning
Peter Anderson, Simon Fraser University (Canada)
David Aylward, The ComCARE Alliance
Alan Beiagi, GeoDecisions
Ray Chadwick, Classco
Cliff Dice, Dice Corporation
Gary DuBrueler, Shenandoah County (VA) Emergency Management
Sukumar Dwarkanath, The ComCARE Alliance
Rich Eisner, California Office of Emergency Services
David Fowler, City and County of San Francisco
Daniel Gast, Orillion
Gan Wei Boon, Ministry of Home Affairs, Republic of Singapore
Sol Glassner, The MITRE Corporation
Alan Jones, USGS
Joe Jumayao, Qualcomm
John Laye, Contingency Management Consultants
Dave Liebersbach, Alaska Emergency Management
Roland Lussier, ComLabs
Lois Clark McCoy, National Institute for Urban Search and Rescue
Don Miller, Washington (state) Emergency Management
Kent Paxton, San Francisco Office of Emergency Services
Dr. Jack Potter, Winchester (VA) Medical Center
Tim Pozar, CSI Telecommunications
Tim Putprush, Federal Emergency Management Agency
Randy Schulley, California Office of Emergency Services
Alan Shoemaker, The MITRE Corporation
Dr. Peter Ward, Partnership for Public Warning
Herbert White, National Weather Service
George Whitney, California Office of Emergency Services
Tom Worden, California Office of Emergency Services

Appendix C. Revision History

Rev	Date	By Whom	What
1.0	2004-02-10	Art Botterell	Redesignated "Committee Draft" and adopted by the Technical Committee.
1.0	2004-01-20	Art Botterell	Revisions: <ul style="list-style-type: none"> • Various editorial clarifications in document. • Added optional/conditional <derefUri> within <resource> element for broadcast applications (Section 3.2 and 3.4) • Made all data types named types (Section 3.4)
1.0	2003-08-12	Art Botterell	Adopted as Committee Specification
0.9a1	2003-07-28	Art Botterell	Revisions: <ul style="list-style-type: none"> • Renamed <address> to <addresses> • Made various editorial corrections in the Context / Class / Attribute / Representation and Definition and Optionality columns of the Data Dictionary (Section 3.2) • Amended examples in Appendix A.2 and A.4 to illustrate use of <eventCode> and <geocode> for EAS/SAME codings • Edited XML schema to replace enumeration for <category> (inadvertently omitted in 0.9a)
0.9a	2003-07-21	Art Botterell	Revisions: <ul style="list-style-type: none"> • Re-designated document as Working Draft • Replaced <audio> and <image> with the <resource> complex element in Structure of the CAP Alert Message (Section 1.3), the Document Object Model (Section 3.1), the Data Dictionary (Section 3.2), and the example in Appendix A.1. • Modified definition of <polygon> in the Data Dictionary (Section 3.2) for GML conformance, and amended the examples in Appendix A. • Added Implementation Note (Section 3.3.2) warning against misleading precision in coordinate values • Substituted term "required" for "mandatory" in Data Dictionary (Section 3.2) optionality entries • Added context to ISO 11179 delineation in Data Dictionary (Section 3.2) • Created separate "alertInfo", "alertInfoResource" and "alertInfoArea" class designations in Data Dictionary (Section 3.2) • Renamed <reference> to <references>

Rev	Date	By Whom	What
			<ul style="list-style-type: none"> • Renamed <incident> to <incidents> • Redesignated <incidents> as a “group” instead of a “name” • Redesignated <polygon>, <circle> and <geocode> as “optional” instead of “conditional” • Redesignated <category> as “optional” • Updated the XML Schema (Section 3.4) to reflect above changes in Data Dictionary and Object Model • Restored prefix in XML Schema (Section 3.4) as required by some XML validators
0.9	2003-06-26	Art Botterell	Editorial corrections in Appendices A and B
0.9	2003-06-20	Art Botterell	Draft for Comment

Appendix D. 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 Executive Director.

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 Executive Director.

Copyright © OASIS Open 2004. 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 may 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.