Guidance for IPAWS Common Alerting Protocol (CAP) Elements and Sub-element Data

Sean Donelan – sean@donelan.com

This guidance attempts to follow the Common Alerting Protocol philosophy -- one CAP message is intended to be distributed by multiple alerting channels. The guidance is intended to improve the consistency of CAP messages across all IPAWS distribution channels. Some items improve interoperability with different implementations, such as specifying case-sensitive versus case-insensitive values. Other items would improve the public presentation of alerts, but don't affect the operation of the alert system.

The guidance does not favor a particular IPAWS distribution channel. Nevertheless, this guidance does recognize some CAP elements are used for specific IPAWS distribution channels. For example, general CAP elements such as Headline, Description and Instructions used by multiple IPAWS distribution channels, should use mixed case text with normal punctuation according to the Info block language. But CMAMtext and CMAMlongtext Parameter elements, used only for WEA, should use only characters which can be transformed into the GSM 7-bit character set. Finally, some poorly specified CAP elements could be used by new IPAWS distribution channels, such as Internet and future alerting systems, if better specified. Geo-location elements and Resource blocks are examples.

Interoperability items are always the most difficult to reach agreement, because multiple choices are possible. Different choices may be correct but may not be interoperable. This guidance intentionally makes some choices which are different than individual alerting origination software, but I believe improve the overall alerting ecosystem across all stakeholders. That does not mean those vendors were incorrect. I hope those vendors and customers will consider making compatible changes.

CAP Alert Element and Sub-elements Details

CAP v1.2 standard	Liberal accept	Conservative send	Notes
Alert <alert> The container for all component parts of the alert message. (Required)		Required.	
Message ID <identifier> The identifier of the alert message. (Required)	Must be unique (case-sensitive) within same Sender ID.	Automatically generate Message ID when sent.	Must be something unique for each message. Suggestion: A Universally Unique Identifier (UUID) or

	Must not include spaces, commas or restricted characters (< and &). An identical Message ID could be used with multiple Sender IDs. Message IDs are not universally unique, only unique with the same Sender ID.	Use only URL and Filename Safe Alphabet (RFC4648) [A-Za-z0-9], hyphen and underscore. Avoid case-sensitive values, i.e., use all upper or lowercase. When used in Reference ID, could be treated as case-sensitive. Maximum 64 characters. Do not reuse Message IDs with the same Sender ID.	(GUID), e.g., "123e4567-e89b-12d3-a456-426655440000." Use database or include workstation hash to avoid ID collisions. Alternative: A structured string used to order and group events in other systems, such as used by IPAWS tests, NWS and NCMEC.
Sender ID <sender> The identifier of the sender of the alert message. (Required)	Assigned globally unique (case-sensitive) name for alert originator. Must not include spaces, commas or restricted characters (< and &). Verify (Message ID and Sender ID) is not a duplicate Alert.	Automatically populate based on alerting organization. Use only Internet domain name alphabet (RFC1035) [A-Za-z0-9], hyphen and period. Avoid mixed case names, i.e., use all upper or lowercase. When used in Reference ID, could be treated as case-sensitive. Maximum 64 characters.	Avoid personally identifiable information, such as operator email addresses. "<name>@" portion usually unnecessary. Suggest using organization fully qualified domain name: "fema.dhs.gov" "mshp.dps.missouri.gov" "oem.nyc.gov" Organization domain should be consistent with COG. The Sender ID is always the actual originator, even if the Sender Name is a different

			agency name. The Sender ID element is not intended to be rendered as part of the public alert.
Sent Date/Time <sent> The time and date of the origination of the alert message. (Required)	Must have valid date / time / offset format "CCYY-MM-DDThh:mm:ssXzh:zm". Verify the Sent Date/Time is recent, i.e., not older than the expiration time interval for the distribution channel.	Automatically populate with the current time when sending the CAP message. Sent Date/Time must be within +/- two minutes of current time.	Use local time and time zone offset of intended alert area or community. If a nationwide alert, use Eastern time zone offset. See notes below.
Message Status <status> The code denoting the appropriate handling of the alert message. (Required)	CAP v1.2 code values Allowed values Actual, Exercise, System, Test or Draft.	**"Actual"**	Required for Public alerts.
Message Type <msgType> The code denoting the nature of the alert message. (Required)	CAP v1.2 code values Allowed values Alert, Update, Cancel, Ack or Error.	**Alert**, **Update** or **Cancel**	Alert, Update and Cancel message types used for Public alerts.
Source <source> The text identifying the source of the alert message. (Optional)		Omit, if not used. Automatically populate based on alert origination point.	May appear as the signature line in the alert message in some CAP distribution channels. Should be treated as metadata, not normally rendered as part of the public alert.

			See notes below.
Scope <scope> The code denoting the intended distribution of the alert message. (Required)	CAP v1.2 code values Allowed values Public, Restricted or Private.	**"Public"**	Required for Public alerts. Public alerts are assumed to be appropriate for immediate public release.
Restriction <restriction> The text describing the rule for limiting distribution of the restricted alert message. (Conditional)	Required when Scope is Restricted. May be present even when Scope is not Restricted.	Omit, if not used. Must not be present in Public alerts.	CAP public distribution channels should NOT render CAP messages containing a Restriction element, even if the Scope element is Public. Alert Originators should not rely on (public) exchange partners obeying the contents of the Restriction element.
Addresses <addresses> The group listing of intended recipients of the alert message. (Conditional)	Required when Scope is Private, optional when Scope is Public or Restricted. Space delimited string of all COG-ID(s) that the message will be posted to.	Omit, if not used.	Not used by CAP public distribution channels. May be used for CAPEXCH, even when Scope is Public, to notify other COGs.
Handling Code <code> The code denoting the special handling of the alert message. (Optional, multiple occurrences allowed)		**"IPAWSV1.0"**	Required for Public alerts.
Note <note> The text describing the purpose or significance of the alert message. (Optional)		Omit, if not used. If present, should contain plain text, without control	Not used by Public CAP distribution channels. A Note element should be present when Message Status

		codes or formatting characters.	is Exercise or Message Type is Error.
Reference IDs <references> The group listing identifying earlier message(s) referenced by the alert message. (Optional)	Required when Message Type is Update, Cancel, Ack or Error. May be present when Message Type is Alert. If present, must reference earlier CAP message or messages and structured as "sender,identifier,sent" with 3 data elements and 2 commas. If multiple CAP messages are referenced, each reference ID structure must be separated by whitespace.	Cancel, Update, Ack or Error should automatically populate from unexpired, previous CAP message(s). Preserve exact element values from original CAP message, including case.	All related messages that have not yet expired must be referenced for Update and Cancel messages. Do not include Reference IDs of expired CAP message(s). Alerting organizations should not Update or Cancel messages with different Sender IDs, except in extraordinary circumstances. CAP exchange partners should check for exact match, including case-sensitive. If no previous message found, may check for case-insensitive match.
Incident IDs <incidents> The group listing naming the referent incident(s) of the alert message. (Optional)	If multiple incident identifiers are referenced, they shall be separated by whitespace. Incident names containing whitespace shall be surrounded by double-quotes.	Omit if not used.	Not used by Public CAP distribution channels. May be used for CAPEXCH.

Notes on Sent Date/Time element:

All time elements (Sent, Effective, Onset, Expires) in CAP message should use the local time zone of the alerting area of responsibility. If an alerting organization's area of responsibility spans multiple time zones, choose a consistent local convention. For example, statewide Amber alerts could use the local time and time zone offset of the state capital. Avoid using Coordinated Universal Time (-00:00), in public CAP Messages. An agency may use UTC for internal processing, but public alerts should use a local time zone to minimize any public confusion.

If daylight saving time changes during alert, use time zone offset in effect at the time in the element. For example, Sent Date/Time uses 12:45 a.m. EDT (-04:00) and Expiration Date/Time uses 3:45 a.m. EST (-05:00) when daylight saving time ends at 2 a.m. between the sent and expiration times.

Notes on Source element:

Avoid using personally identifiable information, such as operator names or initials. When the specific alert origination point is not relevant to the public e.g., distinguishing between a primary and backup emergency operation center, the Source element can be used to track where a problem alert originated. Alert system audit logs are also be used to trace alerts when a problem occurs. But it can take longer to check audit logs in multiple locations, especially when the source of a problem is an infrequently used location.

When the alert origination point is relevant to the public, use the Info block Sender Name element for different alert origination points, e.g., local Weather Forecast Offices.

Single source alerting organization:
Optional, omit.

Multiple source alerting organization:
Acronym or short name (max 10 characters) for different alert origination points in an agency, usually different locations. Because the Source element appears in public CAP messages, it should not identify the individual operator or workstation within those different locations. For example (not actual):

- "FOC" – FEMA Operation Center
- "FAOC West" – FEMA Alternate Operation Center West
- "IPAWS" – FEMA IPAWS program office
- "TEST" – JITC Lab

CAP Info Element and Sub-elements Details

CAP v1.2 standard	Liberal accept	Conservative send	Notes
Info <info> The container for all component parts of the info sub-element of the alert message. (Optional, multiple occurrences allowed)	All Info block instances shall be appropriate for immediate public release. All Info blocks in a single alert must relate to a single incident or update, with the same event category and event code values. Incident metadata could differ within groups of Info block Language sequences. IPAWS does not use groups of Info block Language sequences but can occur with CAP systems designed for other nations. At least one Info block instance required when Message Type is Alert or Update. Info blocks instances are optional when Message Type is Cancel, Ack or Error.	At least one Info block instance when Message Type is Alert, Update as well as Cancel. No Info block instance required when Message Type is Ack or Error. All Info blocks in a CAP alert or update or cancel message must contain consistent metadata information with the same event category and event code values. Groups of Info block Language sequences are not supported in IPAWS. For IPAWS, each unique Language identifier value should have only one Info block instance.	Some Exchange partners may process only the first Info block encountered in a language they support. In case exchange partners missed an earlier message, a Cancel message should include at least a minimal, courtesy Info block instance with the same metadata information, i.e., Event Categories, Event Codes and Areas, from the most recent referenced message. In any case, a Cancel message cancels all referenced messages, regardless of the presence or absence of any Info blocks.

Language <language> The code denoting the language of the info sub-element of the alert message. (Optional, if absent or null, default "en-US")	Code Values: Natural language identifier per [RFC 3066] is NOT case-sensitive and may contain a tag with multiple sub-tags of 1 to 8 characters each. For example, "en" for English, "en-US" for US English, "en-US-MA" for Massachusetts English dialect or "sgn-US" for American Sign Language. If null or absent, "en-US" is assumed as the default value. Multiple Info block instances may be used for the same alert with content in different languages. Multiple Info block instances containing the same Language identifier should be treated as a group.	The first Info block occurrence should use the default (omitted) or mandatory Language identifier value. Each language identifier should contain one language code and one country code, e.g., "en-US" or "es-US" The Language identifier should match (upper/lowercase) the relevant code tables. [ISO 639] recommends that language codes are written in lowercase. [ISO 3166] recommends that country codes are capitalized.	Some exchange partners may ignore a CAP message, when no Info blocks contain a Language identifier they support. Additional Info block instances with other Language identifier values should be after the default or mandatory Language Info block.
Event Category <category> The code denoting the category of the subject event of the alert message. (Required, Multiple occurrences allowed)	All Info block instances must have the same Event Category values. Allowed values Geo, Met, Safety, Security, Rescue, Fire, Health, Env, Transport, Infra, CBRNE or Other.	At least one Event Category code required. A Cancel or Update message should automatically populate the same Event Category(ies)	Some Exchange partners may process only the first Event Category occurrence in an Info block.

		from the most recent referenced message.	
Event Type <event> The text denoting the type of the subject event of the alert message. (Required)	If present, could contain line breaks, white space and control codes.	Should use a controlled vocabulary in the Info block language containing text limited to 35 characters, without control codes or formatting characters. A Cancel or Update message should automatically populate the Event Type from the Info block with the same Language identifier in the most recent referenced message.	The Event Type text should be synchronized with the Event Code(s). Info Blocks with different Language identifiers may use a different Event Type text for each language.
Response Type <responseType> The code denoting the type of action recommended for the target audience. (Optional, Multiple occurrences allowed)	If present, allowed values are Shelter, Evacuate, Prepare, Execute, Avoid, Monitor, Assess, AllClear or None.	Strongly recommended. Initial alert (emergency, watch or warning) messages should use Shelter, Evacuate, Prepare, Execute, Avoid or Monitor. Administrative and test messages should use Assess, AllClear or None. Update and Cancel messages may use any allowed Response Type values.	If Response Type exists, and is not None, a corresponding Instructions element should be present. Required if the message is intended for WEA distribution and “CMAMtext” Parameter is null.
Urgency <urgency> The code denoting the urgency of the subject event of the alert message.	Allowed Values Immediate, Expected, Future, Past or Unknown.	Required.	The Alert Originator can change the Urgency in Update and Cancel Messages.

(Required)			WEA Imminent Threat messages require Immediate or Expected. The WEA message will canceled if a WEA Imminent Threat message Update uses other values.
Severity <severity> The code denoting the severity of the subject event of the alert message. (Required)	Allowed Values Extreme, Severe, Moderate, Minor or Unknown.	Required.	The Alert Originator can change the Severity in Update and Cancel Messages. WEA Imminent Threat messages require Extreme or Severe. The WEA message will canceled if a WEA Imminent Threat message Update uses other values.
Certainty <certainty> The code denoting the certainty of the subject event of the alert message. (Required)	Allowed Values Observed, Likely, Possible, Unlikely or Unknown.	Required.	The Alert Originator can change the Certainty in Update and Cancel Messages. WEA Imminent Threat messages require Observed or Likely. The WEA message will cancel if a WEA Imminent Threat message Update uses other values.
Audience <audience> The text describing the intended audience of the alert message. (Optional)	"All" and "Public" sometimes appear as filler text.	Omit if not used.	Not used by Public CAP distribution channels.

Event Code <eventCode> A system- specific code identifying the event type of the alert message. (Optional, Multiple occurrences allowed)	All Info block instances must have the same Event Code values. The content of "valueName" identifies the assigned domain of the event code. Values of "valueName" are NOT case-sensitive, but acronyms should be in all capital letters without periods. The content of "value" is a case-sensitive string and should match the domain-specific code table.	All Info block instances must have the same Event Code values. The content of "valueName" should exactly match the assigned string for the domain, including upper/lower casing. The content of "value" should exactly match the value in the domain-specific code table, including upper/lower casing. A Cancel or Update message should automatically populate the same Event Code(s) from the most recent referenced message.	The Event Type text should be synchronized with the Event Code(s).
<valueName> = "SAME" (Optional)		Required for EAS. Each Info block instance must contain one and only one Event Code with the "valueName" element containing the uppercase value "SAME" and the "value" element containing an uppercase three-letter code.	All three-letter values for SAME Event Code are passed, even if the Event Code value is not shown in FCC Part 11.31, as long as the value is three-letters. For example, "NWS" is used as a placeholder with extended weather phenomena and significance codes.
<valueName> = Other values (Optional, Multiple occurrences allowed)	Multiple event codes, with "valueName" other than SAME, may be present.		For example, "NationalWeatherService" (exact case) is used with weather phenomena and

			significance codes not covered by SAME event codes.
Effective Date/Time <effective> The effective time of the information of the alert message. (Optional, if absent, assumed to be the same as Sent Date/Time)	IPAWS CAP messages are always in effect when issued. If present, must have valid date / time / offset format "CCYY-MM-DDThh:mm:ssXzh:zm".	When Message Type is Alert, by default, automatically populate with the current time, usually the same as Sent Date/Time. A Cancel or Update message should automatically populate the same Effective Date/Time from the most recent referenced message.	The Effective Date/Time value must be the same or earlier than the Sent Date/Time value. It may be rounded down to a whole minute or adjusted by the alert originator. When present, the Effective Date/Time should take precedence over the Sent Date/Time for the purposes of rendering a public alert. The Effective time still must be the same or earlier than the Sent Date/Time value. This assumes the CAP message is composed shortly before being sent, but the Effective timestamp may differ (earlier) from the Sent timestamp by a few minutes to better synchronize with other alerting systems timestamps. See Sent Date/Time for Time Zone Offset handling.

Onset Date/Time <onset> The expected time of the beginning of the subject event of the alert message. (Optional)	IPAWS CAP messages are always in effect when issued. If absent, assumed to be the same as Effective Date/Time value. If present, must have valid date / time / offset format "CCYY-MM-DDThh:mm:ssXzh:zm".	When Message Type is Alert, by default, omit the Onset Date/Time element. A Cancel or Update message should automatically populate the same Onset Date/Time from the most recent referenced message.	The Onset Date/Time value may be adjusted by the alert originator. See Sent Date/Time for Time Zone Offset handling.
Expiration Date/Time <expires> The expiry time of the information of the alert message. (Optional, if absent, recipient may use its own expiration policy.)	Required. Must be later than the Sent Date/Time value. IPAWS CAP messages must not expire before or at issuance. If present, must have valid date / time / offset format "CCYY-MM-DDThh:mm:ssXzh:zm".	When Message Type is Alert, by default, automatically populate with the Effective Date/Time value plus a default expiration time interval. A Cancel or Update message should automatically populate the same Expiration Date/Time from the most recent referenced message.	The Expiration Date/Time value must be the later than the Sent Date/Time value. The default expiration time interval should be a multiple of 15 minutes. The Expiration Date/Time may be rounded up in whole expiration time intervals, i.e., 15 minutes, or adjusted by the alert originator. IPAWS distribution partners may further round up the expiration time by a distribution channel acceptable interval or have a distribution channel maximum expiration time limit. For

			example, NWEM (Six hours), WEA (24 hours) and EAS (99:30 hours). See Sent Date/Time for Time Zone Offset handling.
Sender Name <senderName> The text naming the originator of the alert message. (Optional)	If present, could contain line breaks, white space and control codes.	Automatically populate based on alert origination agency. Sender Name should contain plain text limited to 64 characters, without control codes or formatting characters. Backup alert origination agencies should be able to choose alternate Sender Names when sending alerts on behalf of other agencies. The Sender Name should not be manually typed by the operator.	The proper name including jurisdiction of the responsible agency on behalf the alert message is being issued, which may be different from the originator in the Sender ID. The first 11 characters of the Sender Name are used in the default CMAS alert text. The default is not used when the Parameter “CMAMtext” exists. The Sender Name element may be used as the display text with the web link or the posting “From” line in Social media and internet apps. The Sender ID in the Alert block is always the actual originator, even if the Sender Name is a different agency name. Normally the Alert block/Sender ID is not

			rendered as part of the public alert. See notes below.
Headline <headline> The text headline of the alert message. (Optional)	If present, could contain line breaks, white space and control codes.	Optional, but strongly recommended. The Headline should contain plain text in normal sentence case limited to 140 characters, without control codes or formatting characters. The Headline text and Event Description text should not be the same. The Headline should be a summary, and Event Description should provide more detail than the Headline. If not used, should be omitted instead of filler characters.	The Alert Originator must be able to customize the Headline text, even if the system generates draft Headline text from a template or other Info block elements. The Headline element may be used as the display text for the posting "Subject" line in Social media or pop-up text in internet apps. Note: Most IPAWS distribution channels do NOT render Cancel messages for the public. A Cancel message STOPS the rendering of any referenced alert messages. This recommendation is for robustness, in case a Cancel message is accidently rendered to the public: Cancel messages should NOT populate the Headline from earlier referenced messages. A

			Cancel message should automatically generate a draft cancellation headline which the Alert Originator can customize, for example: "Canceled: <previous headline>"
Event Description <description> The text describing the subject event of the alert message. (Optional)	If present, could contain line breaks, white space and control codes.	Required. The text should be relevant and useful for the audience in the alert area. The text should not be duplicated in the Headline or Instructions. The Event Description should contain plain text in normal sentence case. Suggest limiting the Event Description plus Instructions to about 200 words (less than 1,000 characters) to fit within two minutes when using Text-to-Speech. The length of the Event Description and Instructions must be less than 1800 bytes. Depending on UTF-8 encoding that may be less than 1800 characters.	The Alert Originator must be able to customize the Event Description text, even if the system generates draft Event Description text from a template or other Info block elements. Note: Most IPAWS distribution channels do NOT render Cancel messages for the public. A Cancel message only STOPS the rendering of the referenced alert messages. This recommendation is for robustness, in case a Cancel message is accidently rendered to the public: Cancel messages should NOT populate the Event Description from earlier referenced messages. A Cancel message should automatically

		Update messages should verify before posting that they are different to avoid accidently reposting duplicate messages.	populate the Event Description with a draft cancellation statement which the Alert Originator can customize. For example: "The <Event Type> has been canceled by <Sender Name> on <Date> at <Time>."
Instructions <instruction> The text describing the recommended action to be taken by recipients of the alert message. (Optional)	If present, could contain line breaks, white space and control codes.	Optional, but strongly recommended if Response Type exists, and is not None. Instructions may be present even if Response Type is None or absent. The Instructions text and Event Description text should not be the same. If present, Instructions text should be actionable and should focus on appropriate protective action to be taken by the public or the specified audience of the alert. The Instructions should contain plain text in normal sentence case. Suggest limiting the Event Description plus Instructions	The Alert Originator must be able to customize the Instructions text, even if the system generates draft Instructions text from a template or other Info block elements. Note: Most IPAWS distribution channels do NOT render Cancel messages for the public. A Cancel message only STOPS the rendering of the referenced alert messages. This recommendation is for robustness, in case a Cancel message is accidently rendered to the public: Cancel messages should NOT populate the Instructions from earlier referenced messages. The Instructions element

		to about 200 words (less than 1,000 characters) to fit within two minutes when using Text-to-Speech. The length of the Event Description and Instructions must be less than 1800 bytes. Depending on UTF-8 encoding that may be less than 1800 characters. If not used, should be omitted instead of filler characters.	usually should be omitted from Cancel messages, unless customized by the Alert Originator. If draft cancellation Instructions are created, they should NOT presume a canceled alert message means the hazard is all-clear.
Information URL <web> The identifier of the hyperlink associating additional information with the alert message. (Optional)	If present, must be a well-formed, but not necessarily valid, URL.	Optional, but strongly recommended. If present, must be a well-formed URL. Should be valid and publicly accessible. Avoid using unsafe and percent-encoded characters in URIs. If not used, should be omitted instead of filler characters.	This URL should link (or re-direct) to the most current update of the alert accessible on the web. Not an old copy of the alert. Alternative: A static link to the Alert Originator's website.
Contact Info <contact> The text describing the contact for follow-up and confirmation of the alert message. (Optional)	If present, could contain line breaks, white space and control codes.	Omit if not used. If present, Contact Info should be plain text limited to 64 characters, without control codes or formatting characters.	Avoid personally identifiable information, such as operator names, email addresses, etc. No format is specified. If used, suggest including only public "mailto:" or "tel:" links. Not supported by EAS or WEA, but

			some internet browsers will automatically detect.
Parameter <parameter> A system- specific additional parameter associated with the alert message. (Optional, multiple occurrences allowed)	The content of "valueName" identifies the assigned domain of the Parameter code. Values of "valueName" are NOT case-sensitive, but acronyms should be in all capital letters without periods. The content of "value" varies by the type of domain, either a text string or a coded value. If a coded domain, the content of "value" is a case-sensitive string and should match the domain-specific code table. If a text string, the content of "value" is a free-text string, and could include arbitrary line breaks, white space and control codes.	The content of "valueName" should exactly match the assigned string for the domain, including upper/lower casing. If a coded domain, the content of "value" should exactly match the domain-specific code table, including upper/lower casing. If a text string, the content of "value" should contain plain text, without control codes or formatting characters.	A Cancel or Update message should automatically populate the same Parameter(s) coded values with updated information or from the most recent referenced message. If a text strings, see the guidance for each text Parameter for Cancel and Update processing. Note: Most IPAWS distribution channels do NOT render Cancel messages for the public. A Cancel message STOPS the rendering of any referenced alert messages. Including copies of the Parameter(s) in the Cancel message is for the convenience of exchange partners which may have missed some of the referenced messages.
<valueName> = "BLOCKCHANNEL" (Optional, multiple occurrences allowed)		Omit, unless intentionally blocking specific IPAWS distribution channels.	Parameter instances, each with one of the following four values will restrict that message distribution channel: CMAS, EAS, NWEM or PUBLIC.

<valueName> = "CMAMtext" (Optional)	Could contain UTF-8 encoded characters not available in the GSM 7-bit alphabet, line breaks, white space and control codes.	Strongly recommended. Should be present to avoid generating unexpected default WEA text by the IPAWS WEA channel transformation. Each Info block should contain one and only one instance of the Parameter with <valueName> of "CMAMtext" (exact text and upper/lower casing). The <value> element should contain plain text limited to 90 characters, encoded in UTF-8 with characters also available in GSM 7-bit default alphabet.	Only the first Info block occurrence for each Language element equal to "en-US" or "es-US" are processed by the IPAWS WEA distribution channel. Any characters not supported by the GSM 7-bit default alphabet (3GPP TS 23.038/GSM 03.38) may be removed or replaced when transformed by the WEA (CMAC) distribution channel.
<valueName> = "CMAMlongtext" (Optional)	Could contain UTF-8 encoded characters not available in the GSM 7-bit alphabet, line breaks, white space and control codes.	Strongly recommended, should include to avoid generating unexpected default WEA text by the WEA channel transformation. Each Info block should contain one and only one instance of the Parameter with <valueName> of "CMAMtext" (exact text and upper/lower casing). The <value> element should contain plain text limited to 360 characters, encoded in UTF-8 with characters also	Only the first Info block occurrence for each Language element equal to "en-US" or "es-US" are processed by the IPAWS WEA distribution channel. Any characters not supported by the GSM 7-bit default alphabet (3GPP TS 23.038/GSM 03.38) may be removed or replaced when transformed by the WEA (CMAC) distribution channel.

		available in GSM 7-bit default alphabet.	
<valueName> = "EAS-ORG" (Optional)		Required for EAS and NWEM distribution channels. Each Info block should contain one and only one instance of the Parameter with the valueName of "EAS-ORG" (exact text and uppercase). The value contains a three-letter uppercase code equal to EAS, CIV, WXR or PEP.	Must match the Alerting Organization's IPAWS profile. The EAS-ORG code value must be one of the following three-letter codes: ▪ PEP – Primary Entry Point System ▪ EAS – Broadcast station or cable system ▪ WXR – National Weather Service ▪ CIV – Civil authorities
<valueName> = "timezone" (Optional)		Required for NWEM distribution channels. Each Info block should contain one and only one instance of the Parameter with the valueName of "timezone" (exact lowercase). The value contains a three-letter/four-letter uppercase time zone code equal to AST, EST, CST, MST, PST, HST, AKST, SST or CHST.	The originator's timezone code must be one of the following three-letter/four-letter codes for both standard and daylight saving time: ▪ AST – Atlantic time zone ▪ EST – Eastern time zone ▪ CST – Central time zone ▪ MST – Mountain time zone ▪ PST – Pacific time zone ▪ HST – Hawaii time zone ▪ AKST– Alaska time zone ▪ SST– Samoa time zone ▪ CHST– Chamorro time zone
<valueName> = "WEAHandling"			"Child Abduction" "Imminent Threat"

(Optional)			"Presidential" "Public Safety" "WEA Test"
<valueName> = other (Optional, Multiple occurrences allowed)			A wide-variety of other Parameter codes are used. Mostly ignored, except for proprietary systems.

Notes on Sender Name element:

The Sender Name is used primarily by the PUBLIC distribution channel for internet and social media. WEA may use the first 11 characters as part of the default CMAS alert test, only when the Parameter "CMAMtext" is missing. Since its almost always better to use CMAMtext, concern about truncation of the Sender Name in WEA messages should be less of an issue. EAS can, but seldom does, use the Sender Name. NWEM used Sender Name structured as "COG Name, City, State" but is currently disabled. The NWEM channel transformation process probably should use IPAWS metadata, such as COG ID, for machine processing and to lookup the responsible agency instead of a text field.

if IPAWS is used for next-generation alerting channels, the Sender Name text could be a powerful part of the public's assessment of an alert's source and importance. But only if the Sender Name is meaningful to the public.

Use a proper name for the agency which will be clear, concise and recognizable to the public. The name does not need to be the agency's formal, legal name or COG name; and often is not. Joint communication centers should adopt a consistent, meaningful public name for joint warning operations. Unless multiple department offices issue warnings within the same jurisdiction or agency, a long name specifying intradepartment offices or branches is unnecessary.

Do not assume all alert recipients will be local or will recognize local agencies. Alerts are often distributed outside the intended local area or posted on global social media.

The full proper name should indicate the nation, state, county, city, etc. of the agency's jurisdiction. The Sender Name should avoid confusion with the names of other agencies or jurisdictions. For example, there are multiple Springfield Police Departments; use Springfield Police Department IL instead. Likewise, instead of Metropolitan Police Department use Metropolitan Police Department of Washington DC. Local agencies could join together to create a new consolidated joint

county, multicounty or multistate alerting authority name, e.g., Washington DC National Capital Region Emergency Operation Center (does not actually exist). Avoid abbreviations, with a few nationally known exceptions, such as NWS forecast offices and USPS state abbreviations. Even if an agency believes they are better known by their abbreviation, infrequent alert originators should include their proper name after the abbreviation. Such as, FBI – Federal Bureau of Investigation or FEMA – Federal Emergency Management Agency.

Some federal agencies use distinct local alerting authority names, such as weather forecast offices and some military bases.

Alerting authorities should coordinate naming policies with their state emergency management agency. If your state has no naming policy, The Associated Press Stylebook may be a useful reference.

Because the Sender Name element is in the Info block with a Language identifier, the text value in different blocks may be in different languages. Such as President of the United States and Presidente de los Estados Unidos.

National examples (not actual, with National, Federal, etc.):

- President of the United States
    - Spanish: Presidente de los Estados Unidos
- Federal Emergency Management Agency
- National Earthquake Information Center
- U.S. Department of Homeland Security
- U.S. Tsunami Warning Center

State examples (not actual, with full state name):

- California Highway Patrol
- California Office of Emergency Services
- Port Authority of New York and New Jersey
- New York State Police
- Virgin Islands Territorial Emergency Management Agency

Local examples (not actual, with full city or county, and state abbreviation):

- City of Los Angeles CA

- Los Angeles County CA
- NWS Baltimore MD/Washington DC
- Pasco County Sheriff's Office FL
- U.S. Army Fort Knox KY
- Saint Louis County MN
- Saint Louis City MO
- Saint Louis County MO
- NWS Buffalo NY
- New York City Office of Emergency Management NY
- Pentagon Force Protection Agency Arlington VA
- University of Wisconsin-Madison Police Department WI

A little redundancy in names is better than a lot of confusion caused by names.

CAP Resource Element and Sub-elements Details

CAP v1.2 standard	Liberal accept	Conservative send	Notes
Resource <resource> The container for all component parts of the resource sub-element of the info sub- element of the alert element. (Optional, Multiple occurrences allowed)		Link to recorded audio file strongly recommended for EAS. Not required for CMAS.	Only needed if audio file or stream is linked or embedded. May be used with other resource types, e.g., images and video.
Description <resourceDesc> The text describing the type and content of the resource file. (Required)	Required, could contain line breaks, white space and control codes.	For EAS audio content use "EAS Broadcast Content" in the first Resource block instance. Should use a controlled vocabulary in the Info block	Some exchange partners may process only the first Resource block occurrence in an Info block.

		language containing text limited to 35 characters, without control codes or formatting characters.	See notes on resource description.
MIME Type <mimeType> The identifier of the MIME content type and sub-type describing the resource file. (Required)	Required, could contain line breaks, white space, control codes and arbitrary strings.	For EAS audio content, use: audio/x-ipaws-audio-mp3	MP3 is the most widely supported audio type. The MP3 patent has expired, so all CAP creators should be able to use. See notes on Mime type.
File Size <size> The integer indicating the size of the resource file (Optional)		Value in bytes of the raw file size retrieved from the <uri> or <derefUri> (not after base64 encoding or HTTP compression).	Omit if unknown or indefinite, do not use 0 or MAXINT.
URI <uri> The identifier of the hyperlink for the resource file. (Optional)	The absolute URL location should be publicly accessible over the internet. A relative URL should contain only a filename and file type extension. It can be used as the suggested filename for the derefUri element.	For EAS audio use the full absolute URL of the audio file on internet. CAP producers should verify the resource file URL is accessible on the public internet, i.e., not a private IP address or blocked by firewalls. Omit if not publicly accessible. Avoid using unsafe and percent-encoded characters in URIs.	If both <derefUri> and a full absolute <uri> occur in the same Resource block, first attempt to retrieve and use the resource file from the absolute <uri>. For security reasons, relative URIs are not used. CAP consumers should generate their own temporary storage filenames.
Dereferenced URI <derefUri>		Not recommended with IPAWS. Can be used with state	If a full absolute <uri> is not present or could not be

The base-64 encoded data content of the resource file (Conditional)		systems and systems in other countries.	retrieved, then decode and use the resource file from the base-64 derefUri.
Digest <digest> The code representing the digital digest (“hash”) computed from the resource file (Optional)	Poorly defined.	Calculate using the Secure Hash Algorithm (SHA-1) of the raw file. Value stored as 28 characters in base64 for a 160-bit hash.	Should be prepared for longer SHA digests if the CAP standard or IPAWS profile is updated with the latest FIPS Secure Hash standards.

Notes on Resource Description and MIME Type

Resource Description should use a controlled vocabulary to identify the Resource blocks for a specific IPAWS distribution channel, i.e., “EAS Broadcast Content” or as simple text for a public caption or hyperlink anchor in general-purpose Resource blocks. The <web> URL is better for complex interactive resources such as HTML pages or browsers selecting alternative video encodings.

General-purpose Resource blocks are typically used for simple internet/Social Media hyperlinks but could be used by any IPAWS distribution channel. Possible simple hyperlinks could include pictures (image/gif, image/jpeg, image/png) used with the Resource Description: Missing Person, Subject, Victim, Vehicle, Location Map or Evacuation Routes. General-purpose Resource Descriptions should in the Info block language.

In the future, not yet standardized, Resource Descriptions could identify which Resource blocks contain extended Advanced Emergency Alerting packages in the CAP message to pass to advanced warning and alerting systems.

URI file names should use URL and filename safe alphabet (RFC4648) “[_A-Za-z0-9-]+”, plus the recommended file type extension. Avoid using unsafe characters and percent-encoded characters in URIs.

Resource Description	Resource mimeType	Suggested encoding parameters	Notes
CMAS * EAS * NWEM * PUBLIC *			Resource block Descriptions beginning with IPAWS channel names should be reserved for future

			standardization with those distribution channels.
EAS Broadcast Content	audio/x-ipaws-audio	Unspecified audio codec not recommended.	Use a specific audio codec type identifier for EAS.
	Audio/x-ipaws-audio-mp3	Human recording: 96 kbps CBR, Mono, (16-bit), 48 kHz. Loudness -16 LUFS (LKFS), -1 dB FS. Max file size: 1.5MB (Two minutes) Computer generated text-to-speech: 64 kbps CBR, Mono, (16-bit), 22.05 kHz. Loudness -16 LUFS (LKFS), -1 dB FS. Max file size: 1MB (Two minutes)	Content-Type: audio/mpeg File type extension: .mp3 Note: mono is actually mixed at -19 LUFS, but most loudness meters adjust and display -16 LUFS for both mono/stereo.
	Audio/x-ipaws-audio-wav	Not recommended.	Content-Type: audio/vnd.wave, audio/wav, audio/wave, or audio/x-wav File type extension: .wav Mono, 16-bit, 22.05 kHz Loudness -16 LUFS (LKFS), -1 dB FS. Note: mono is actually mixed at -19 LUFS, but most loudness meters adjust for mono/stereo and display -16 LUFS for both. Max file size: 5.5MB (Two minutes)
	audio/x-ipaws-streaming-audio	None standardized.	
	Video/x-ipaws-video	None standardized.	

	Video/x-ipaws-streaming-video	None standardized.	
Other resource types must have an appropriate Description text.	audio/mpeg audio/vnd.wave (wav, wave or x-wav) image/gif image/jpeg image/png	If it's not accepted according to the Internet Advertising Bureau (IAB) Standards, Guidelines and Best Practices, it's likely a bad idea.	Use IPAWS MIME types only with resourceDesc "EAS Broadcast Content." Use IANA MIME types with other resource descriptions.

CAP Area Element and Sub-elements Details

CAP v1.2 standard	Liberal accept	Conservative send	Notes
Area <area> The container for all component parts of the area sub- element of the info sub- element of the alert message. (Optional, Multiple occurrences allowed)		At least one Area block must be present in each Info block. Area blocks should be consistent across Info block instances with different Language identifier values.	Some exchange partners may process only the first Area block in an Info block. When multiple Area blocks exist within an Info block, the alert area of the Info block is the geospatial union of the associated Area blocks. See notes on alerting areas.
Area Description <areaDesc> The text describing the affected area of the alert message. (Required)	Required, could contain line breaks, white space and control codes.	Required. Should use a controlled vocabulary in the Info block language containing text limited to 35 characters if	The Area Description text should describe, and be synchronized with, the area represented by Area Polygon(s), Area Circle(s), Area

		multiple Area blocks each with a separate area or 256 characters if a single Area block with all the areas combined, without control codes or formatting characters.	Geocode(s), Altitude and Ceiling in this Area block. Other national CAP profiles use keywords in the Area Description to include/exclude alert areas.
Area Polygon <polygon> The paired values of points defining a polygon that delineates the affected area of the alert message. (Optional, Multiple occurrences allowed)	Structured string.	Optional.	When multiple Area Polygons exist within an Area block, the polygon area for that Area block is the geospatial union of all the Area Polygons in the same block.
Area Circle <circle> The paired values of a point and radius delineating the affected area of the alert message. (Optional, Multiple occurrences allowed)	Structured string.	Optional.	When multiple Area Circles exist within an Area block, the circle area for that Area block is the geospatial union of all the Area Circles in the same block.
Area Geocode <geocode> The geographic code delineating the affected area of the alert message. (Optional, Multiple occurrences allowed)	The content of "valueName" identifies the assigned domain of the Area Geocode. Values of "valueName" are NOT case-sensitive, but acronyms should be in all capital letters without periods. The content of "value" is a case-sensitive string and	The content of "valueName" should exactly match the assigned string for the domain, including upper/lower casing. The content of "value" should exactly match the value in the domain-specific code table, including upper/lower casing. A Cancel or Update message should automatically populate the same Geocode(s) from the	Some exchange partners may process only one type of Geocode. When multiple Area Geocodes exist within an Area block, the geocode area for that Area block is the geospatial union of all the Area Geocodes in the same block.

	should match the domain-specific code table.	most recent referenced message.	
<valueName> = "SAME" (Optional, Multiple occurrences allowed)	Area blocks may contain multiple Area Geocodes with the "valueName" element containing the uppercase value "SAME" and the "value" element containing an a SAME 6-digit location (extended FIPS) code.	At least one SAME Geocode must be present in each Info block language.	Only the first 31 SAME Geocodes for an entire Info block are used by EAS. Other CAP distribution channels may process more, or fewer SAME Geocodes.
<valueName> = Other values (Optional, Multiple occurrences allowed)	Multiple Area geocodes with "valueName" other than SAME may be present.		For example, NOAA's Universal Geographic Code (UGC).
Altitude <altitude> The specific or minimum altitude of the affected area of the alert message (Optional)		Omit if not used.	Not currently used in IPAWS.
Ceiling <ceiling> The maximum altitude of the affected area of the alert message (Conditional)	May only occur when Altitude is also present.	Omit if not used.	Not currently used in IPAWS.

Notes on alerting areas

When an individual Area block contains a combination of Area Polygons, Area Circles and Area Geocodes, some exchange partners use only one type of area, i.e., only polygons, circles or geocodes, to create an effective alerting area. This means GIS enabled exchange partners usually alert a small geographic area, based on polygons or circles. And usually non-GIS exchange partners alert larger geographic areas, based on geocodes. However, sometimes Alert Originators create polygons

/ circles larger than the associated geocode area. In that case, GIS exchange partners alert a larger geographic area, and non-GIS exchange partners alert a smaller geographic area.

Alerting is even more inconsistent when the polygon / circle areas and geocode areas are disjoint.

A suggested alternative is make the geospatial intersection of the area types (i.e., polygons, circles, geocodes) within each Area block and then combine that area in the geospatial union with other Area blocks. In other words, make a union of all the polygons in the same block, make a union of all the circles in the same block, and make a union of all the geocodes in the same block. Then take the intersection of those three (non-null) area types in the same block to create the joint overlapping area result for that Area block. Elevation and Ceiling is not currently used in IPAWS. But if used, Elevation and Ceiling would create a 3-Dimensional geospatial area result for that Area block. That block's result is then combined in the union with other Area blocks. The final result is a consistent and specific alerting area.

CAP creators should coordinate with adjacent alerting authorities. Natural hazards rarely respect geopolitical borders. And alerting systems have significant bleed-over beyond specified alert boundaries. If multiple jurisdictions are impacted, consider creating a single, joint CAP alert covering the entire affected area instead of multiple alerts for each jurisdiction.

CAP alert origination software should warn the alert originator when specifying very small or very large alert areas for different IPAWS distribution channels. The effective area alerted by different exchange partners will vary depending on each partner's dissemination policies and technical capabilities. The suggested minimum alert areas are:

- The polygon area should be greater than 2.5 square kilometers or approximately 1 square mile.
- The circle radius should be greater than 0.9 kilometers; approximately 2.5 square kilometers or 1 square mile.
- The SAME geocode should be greater than 1/9 of the county, which is the minimum size of a SAME geocode.

These are warnings, not errors. An Alert Originator may intend to alert a very small or very large area, but often it's a typing or interface error. These suggested minimum sizes should be configurable.

IPAWS channel	Suggested minimum alert area	Suggested maximum alert area
CAPEXCH	No minimum area	Depends on IPAWS authorization
CMAS	25 square kilometers; 10 square miles	Depends on IPAWS authorization
EAS	200 square kilometers; 77 square miles	Depends on IPAWS authorization

NWEM	50 square kilometers; 19 square miles	Depends on IPAWS authorization
PUBLIC	2.5 square kilometers; 1 square mile	Depends on IPAWS authorization

Notes on geospatial data types (from EDXL standards):

Values for latitude and longitude are expressed as decimal fractions of degrees conforming to the WGS84 coordinate reference system. Whole degrees of latitude are represented by a decimal number ranging from 0 through 90. Whole degrees of longitude are represented by a decimal number ranging from 0 through 180. When a decimal fraction of a degree is specified, it is separated from the whole number of degrees by a decimal point (the period character, "."). Decimal fractions of a degree are expressed to the precision intended, with trailing zeros being used as placeholders if required. A decimal point is optional where the precision is less than 1 degree.

Some effort should be made to preserve the apparent precision when converting from another datum or representation, for example 41 degrees minutes should be represented as 41.22 and not 41.21666, while 41° 13' 11" may be represented as 41.2197.

Latitudes north of the equator MAY be specified by a plus sign (+), or by the absence of a minus sign (-), preceding the designating degrees. Latitudes south of the equator MUST be designated by a minus sign (-) preceding the digits designating degrees. Latitudes on the equator MUST be designated by a latitude value of 0.

Longitudes east of the prime meridian shall be specified by a plus sign (+), or by the absence of a minus sign (-), preceding the designating degrees. Longitudes west of the prime meridian MUST be designated by a minus sign (-) preceding the digits designating degrees. Longitudes on the prime meridian MUST be designated by a longitude value of 0. A point on the 180th meridian shall be taken as 180 degrees West and shall include a minus sign.

Caution: EDXL standards do not specify how alert areas cross -180 and 180 degrees. The two typical alternatives are:

1. Use two Area blocks with adjacent alert areas on their respective sides of the 180-degree meridian.
2. Use bounding box coordinates with longitudes extending over 180 or -180, e.g., 183 West (-) is the same as 177 East (+); and 183 East (+) is the same as 177 West (-). This connects the coordinates across the 180-degree meridian, instead of connecting the coordinates across the prime (0-degree) meridian on the other side of the globe.

CAP producers should use alternative #1. CAP consumers should be prepared to handle both alternatives.

Sean Donelan – sean@donelan.com

Signature Element and sub-elements

<Signature>			
<SignedInfo>			
<CanonicalizationMethod>			
<SignatureMethod>			
<Reference>			
<Transforms>			
<Transform>			
<DigestMethod>			
<DigestValue>			
<SignatureValue>			
<KeyInfo>			
<X509Data>			
<X509SubjectName>			
<X509Certificate>			

Notes on Signature

See IPAWS-OPEN Interface Design Guidance document for digital signature requirements.