Advice on Implementing a CAP-enabled Alerting System

Summary:

This document is intended to provide advice concerning policy and technical matters pertinent to implementing a Common Alerting Protocol (CAP)-enabled Alerting System. The advice is contributed by individuals in the role of invited experts, as listed in the Acknowledgements section. The target audience is the set of implementors who are likely to have a role in such an undertaking.

Table of Contents

1. Strategic and Policy Matters

1.1. Principles and Scope

1.1.1 Basic Principle of Alerting - Emergency alerting is widely accepted as a core responsibility of civilized societies across all cultures in the world today. In any particular national context, the emergency alerting responsibility may be rooted in various moral or ethical principles. [1] The practice of emergency alerting across different countries is typically subject to national or local laws and regulations, which may be couched in terms of civil defense, civil protection, community preparedness, emergency management, or disaster management, among others. [2]

1.1.2 All-hazards, All-Media - These notes focus specifically on meeting the emergency alerting responsibility by the implmentation of an Alerting System that helps to communicate alerts to people whose lives may be in danger. Because lives can be threatened by all manner of hazards and all communications media are potentially useful in alerting, here it is taken as given that emergency alerting should be "all-hazards" and "all-media" by design.

1.1.3 Equitable Access to Alerting - In the context of any particular Alerting System, implementors need to be clear whether the system will try to alert all people affected, and whether that also includes people who are not legal residents. A range of media must be enlisted for alerting because some media (e.g., sirens, SMS messages) can only get a person's attention while other media can more fully instruct. Also, depending on a person's activities at the moment, quite different media are needed to communicate an alert to him/her. Implementors should be very clear as well about the degree to which attempts will be made to alert people with special needs (e.g., people who are blind, deaf, cognitively impaired, or illiterate), and people who do not understand the dominant language of the area.

1.1.4 Alerting Here is Messaging Only - Any communication of alerts to people begins with the means to perceive a potential or actual hazard threat. However, those aspects are not the subject of these notes. For the purpose of these notes, alert communication starts when a message sender decides to warn people of a hazard threat by means of the Alerting System. The alert communication ends when people receive the alert message. Actions taken subsequent to receipt of the alert message are not in scope of these notes.

1.1.5 Digital Telecommunication Networks as a Backbone - Many different means are needed to accomplish effective communications for emergency alerting, depending on the particulars of the threat and the people who need to be alerted. At the end point, the alert may be communicated by a siren, an official with a megaphone, a person-to-person conversation, an e-mail, an emergency alerting app, and many other means. These notes focus on using digital telecommunication networks as a backbone infrastructure, of which the prime example today is the Internet. The Internet is now, and will likely

[1] The Universal Declaration of Human Rights, Article 3, states: "Everyone has the right to life, liberty and security of person" (see http://www.un.org/en/universal-declaration-human-rights/) Article 3 of the Declaration of Human Duties and Responsibilities asserts that States "shall take positive and effective measures to protect and enforce the right to life" and that "Individuals and non-State actors [...] have a duty to take reasonable steps to help others whose lives are threatened." (see http://globalization.icaap.org/content/v2.2/declare.html)

[2] In 2014, UNDP and IFRC conducted a comparative study of national legislation for disaster risk reduction, and they have subsequently provided a Handbook and a Checklist based on the findings of that study. These free resources are described at, and can be obtained from, http://www.drr-law.org/

remain, essential to the emergency alerting function for the great majority of hazard threats affecting groups of people in modern societies. Other networks such as cellular telephone services, radio and television broadcast, landline telephones, and more specialized networks such as "NOAA weather radio", can be viewed as end delivery mechanisms from the alert distribution perspective.

1.2. Cross-Sector Collaboration Is Essential

1.2.1 Collaboration among Government, Commerce, and NGO's - For a modern society to implement effectively and efficiently the digital telecommunication networks component of public emergency alerting, it is necessary to have collaboration across the three major sectors: government, commerce, and non-governmental organizations (NGO's). In the government sector, major actors are typically government agencies with a specific hazard threat mandate and other agencies with a civil protection mandate. In the commerce sector, major actors include telecommunications companies, news organizations, and various other actors that may help with emergency alerting for a variety of reasons. NGOs include a range of emergency preparedness and response actors, including some with a trusted and essential presence at the local community level.

1.2.2 Distinguishing Official Sources of Alerts - The Alerting System needs to distinguish official sources from other sources of alerts, both in labeling its own alerts as official and in making use of alerts that originate elsewhere. An important resource for these purposes is the international Register of Alerting Authorities, [3] maintained by the World Meteorological Organization (WMO). Because WMO is a treaty-level organization, each national assertion that a source is official has the force of law for the country making that assertion in this Register. It is noted that about 500 official sources, including all of the National Meteorological or Hydrological Services and all of the Red Cross and Red Crescent National Societies, are currently listed as alerting authorities in this international Register. For alerting sources not known to be authoritative, government might need to consider if it should, or could, restrict media and online access by such alert sources, internal to or external to the country. An additional consideration is to establish clear policy regarding the practice of "re-originating" alerts (receiving an official or unofficial alert and sending out a modified version of the alert, either officially or unofficially).

1.2.3 Private and Public Alerting - Although public alerting is the focus of these notes, the Alerting System is likely to include private messaging about hazard threats as well. Alerting authorities in different jurisdictions may send alerts privately so that the appropriate authority can send public alerts if they so decide. The initial report of an emergency situation is often a private message to the local emergency call center. [4] Private messaging is also common as experts or security personnel communicate with emergency managers about a given hazard among themselves as a threat is being evaluated. [5] Also, there are certainly private messages about suspicious activity before any public alert concerning terrorism. [6] It is a choice to what degree, if any, the Alerting System includes some

[3] The international Register of Alerting Authorities is at http://www.wmo.int/alertingorg An alerting authority can include in its records within the Register the URL of an alert news feed. For example, this feed is listed in the U.S. National Weather Service record - https://alerts.weather.gov/cap/us.php?x=0

[4] The Prefecture of Paris issued a European bid for an emergency call management system that includes CAP protocol.

[5] Pinkerton services (see 2015 presentation) supports 80 of the top 100 corporations worldwide and the company also provides security services for large events such as the Olympics. Because their alerting system is based on CAP, it is easier to connect with local emergency systems that are also based on CAP.

[6] The Government of France released, in time for the Euro 2016 football event, a free smartphone application, SAIP (Information Alert System for People) that sends French and English alerts on terrorist attacks, nuclear incidents, dam failures, or other exceptional events. SAIP will soon be CAP-enabled.

of this private messaging, but there are obvious efficiencies when relevant private alerting is deigned to be interoperable with public alerting.

1.3. Key Roles May be Voluntary

1.3.1 Voluntary Collaboration Policies - It seems certain that at least some of the actors playing a crucial role in the operational Alerting System may be executing their role on a voluntary basis. For example, in the event that cellular telephone services are not compelled to disseminate official, high-priority alerts, it may be that public policy requires the cell service provider to obtain informed consent from each customer, a positive acknowledgment that the customer understands the provider will not deliver life-critical alerts. In any case, an effective system design must take voluntary participation into account, just as it must take into account that a severe and widespread emergency might compromise many crucial components of the Alerting System, including some that are not voluntary and were mandated to remain operational.

1.4. Roles and Responsibilities Must be Clear

1.4.1 Alerting at Local to National Levels - The Alerting System may involve many actors at different levels: local community, municipality, state, national, and international. It is important to define clearly what are the respective roles and responsibilities of these actors within and across these levels. These role and responsibility definitions will affect the allocation of resources and certain details of the system design, especially the degree to which the operational system will be centralized. Here it should be noted that hazard events are far more common at the local community and municipality level. However, even if alerting for local situations is accomplished without higher-level involvement, higher-level organizations could have awareness of these local situations simply by monitoring the local news feeds that are part of the Alerting System. This capability is particularly important in those cases when a local situation evolves to the point of needing involvement by broader-scale organizations.

1.4.2 Describing a Hazard Threat as Distinct from Alerting the Public - It is important to clearly define at each level if there are distinctive roles for different alerting authorities with regard to alerting the public. For instance, the role of a scientific agency might be to characterize a hazard threat while the role of a civic authority might be to actually instruct people in how to deal with that hazard threat.

1.4.3 Roles of Alerting Collaborators Beyond Government - The Alerting System will need to be clear as to what roles are appropriate for non-government actors in emergency warning, including commercial or public news media and particular Red Cross/Red Crescent organizations, [7] among others. Some alerting services will be offered by external entities, such as Samsung [8] and Google, [9] among others. We can also expect: that radio and television could deliver alerts as Public Service Announcements, that cellular telephone services could deliver alerts through their cell broadcast capabilities, [10] that online advertisers could disseminate public warnings through the overlay of

[7] The CAP-enabled Red Cross Hazards App is described at http://preparecenter.org/content/hazard-app

[8] Samsung Geo News is described at http://www.samsung.com/ie/support/skp/faq/1061356

[9] Google Public Alerts is described at https://support.google.com/publicalerts/

[10] Cell broadcast is described at http://www.eena.org/ressource/static/files/2011_11_17_one2many.pdf
CAP-based cell broadcast in the United States is known as the Wireless Emergency Alerts system.

online ads, [11] and that billboard companies could display alerts through their digital signage resources, [12] among other possibilities.

1.4.4 Intellectual Property Rights and Attribution of Alerting Content - Clarity is needed as to the legal rules for intellectual property rights and attribution on the contents of alerts and alert services, and the manner by which rights and attribution are expressed. [13] Here consideration might be given to classifying alerts as a kind of news story, thereby allowing the Alerting System to inherit the body of existing ethical codes, laws and precedents applicable to the journalism profession and news industry.

1.4.5 Commerciality Issues in Public Alerting - It is important to consider if there is a need for specific rules applicable to the range of non-government, public alerting services. This may also require a further distinction for those entities offering emergency alerting services on a for-profit basis. For instance, there may be equitable treatment issues if companies are allowed to market alerting services on a "tiered scale" where subscribers can buy enhanced alerting or evacuation advice capabilities for a fee.

1.4.6 Privacy Issues in Public Alerting - To target alerts to people who are in the alerting area, components of the Alerting System will need to exploit geo-location information, such as subscribers in range of particular cell towers. When geo-location is very precise, personal privacy can become an issue. In this regard, the Alerting System may need a blanket prohibition against the collection of personally identifiable information, including a limit to the precision of geo-location. [14]

1.4.7 Sustaining Public Trust in Emergency Alerting - Especially in an intense emergency, it is crucial that the public has a high degree of trust in the alerting authorities who send out alerts. Obviously, trust is eroded when official authorities fail to alert. Yet, trust can be eroded by inadvertent over-warning for hazard threats that are diffuse in area and/or less than urgent, severe or certain. Trust can also be compromised if people in a given alerting area receive conflicting alerts for a given hazard threat because distinct alerting authorities characterize the threat differently or provide different instructions. Even the inadvertent issuance of duplicate alerts can cause people to wonder if their alerting authorities are collaborating as they should. The Alerting System should have processes to be informed when such conditions arise and to take corrective actions such as education, outreach, testing and exercises.

[11] CAP alerts are disseminated freely as overlays of online advertisements by the Federation for Internet Alerts, with a website at https://internetalerts.org

[12] An example of emergency alerts being displayed via highway digital signage is described at http://www.lamar.com/About/givingback/Community/EmergencyAlertSystem

[13] Creative Commons licenses are a popular mechanism for rights and attribution of electronic resources. Creative Commons licenses are described at https://creativecommons.org/

[14] A privacy issue arises when geo-location information is precise enough to identify an individual. Here It may be of interest that the Network Advertising Initiative Code of Conduct asserts "Use of Precise Geo-location Data for Interest-Based Advertising shall require a user's Opt-In Consent."
(see http://www.networkadvertising.org/2013_Principles.pdf)

1.5. Leveraging the Common Alerting Protocol (CAP) Standard

1.5.1 The CAP Standard is Essential - In the Alerting System, as in many systems already or soon-to-be implemented in societies worldwide, the Common Alerting Protocol (CAP) standard [15] should be considered essential to building an "all-hazards" and "all-media" alerting system that leverages existing digital telecommunication networks, within the country and internationally. Moreover, deploying a CAP-enabled alerting system leverages a vast array of already available and relevant alerts provided by neighboring countries and international institutions such as the WMO, the World Health Organization, and the International Federation of Red Cross and Red Crescent Societies, among others.

1.5.2 CAP Provides the Content Definition for Alert Messaging - In its essence, a CAP alert can be seen as a kind of standard business form. Like any other business form, a CAP alert defines various value selections, fill-in boxes, and check boxes that together provide key details of a specific emergency, such as the type of event, the alerting area, the headline, the sender, and so on. That set of information, the CAP-compliant content, in the form of an Extensible Markup Language (XML) file, is then communicated as a CAP alert message. This communication is typically accomplished by the sender putting the CAP alert file on a publicly accessible Internet host and updating a news feed that links to that CAP alert file. News feed subscribers then retrieve the CAP alert file as they would retrieve any other news item.

1.5.3 CAP Messaging in the Alerting System - At a functional level, an essential success factor of the Alerting System is that it facilitates CAP alerts being sent reliably and securely through digital telecommunication networks and other means, in time to warn people in the alerting area for the particular hazard threat. Already, CAP alerts can be of immediate use for alerting across virtually all sectors: civil protection, fire fighting, health, safety, law enforcement, schools/universities, transportation, hotels, embassies, intelligence, etc. Soon the applications for CAP-enabled alerting will expand dramatically as CAP alerts are increasingly generated by devices and used by devices. An example of this trend is seen in the upgrading of home smoke alarms to become all-hazard alarms simply by adding an inexpensive cell broadcast receiver. However, we should not expect legacy alerting systems to disappear quickly. CAP-enabled systems will co-exist with legacy alerting systems for the next decade or more in many communities.

[15] The CAP standard, officially designated as International Telecommunication Union Recommendation X.1303, is described in an online alerting context at https://drive.google.com/file/d/0B5FiAsl5yGbZRWxXUnYwbHNab1k/view?usp=sharing

2. Practical and Technical Matters

2.1. CAP Alert Dissemination Considerations

2.1.1 Message Distribution Constraints - A study was conducted in 2012 for Public Safety Canada concerning the distribution of CAP alert messages, focusing primarily on the effects of file size. [16] Many CAP-enabled systems distribute alert messages with only text and coded values and these messages average only one or two thousand characters. But some systems embed extra content, for example an audio file to directly support messaging over radio. Such embedded content can enlarge the CAP message to multiple millions of characters. It is clear that the larger a message, the less broadly it can be distributed unchanged. Therefore, large content should be referenced from the message rather than embedded in the message, wherever possible. Also, it may be of interest that the US Emergency Alert System (EAS) sets an alert text limit of 1,800 characters. [17]

2.1.2 Text-to-Voice and Automated Language Translation - The technologies for text-to-voice and for automated language translation recently improved very dramatically. This trend makes it much more feasible to offer emergency alerts in real time in several languages. That is especially the case with CAP messages because much of the key content is expressed in coded values, which can have associated text in any language ready for use. In this context, it is noted that unattended messaging of CAP alerts over broadcast radio and TV and online streaming can be accomplished from text-only messages. For example, OpenBroadcaster [18] is an open source product used for this purpose throughout Canada.

2.2. CAP Profile Policy

2.2.1 Specifying Alerting System Requirements - It is clear that the Alerting System needs to specify, for all actors that process CAP messages, any requirements or preferred practices applicable to the sending or receiving of CAP messages. With regard to the CAP messages per se, there are also various elements for which the Alerting System could, and in some cases should, specify a required or preferred usage. Such CAP-specific requirements are sometimes conveyed through a "CAP Profile". However, constraints specified in a CAP Profile can impede interoperability if potential actors are not sure about the rules for applying the profile. If a CAP Profile is specified, then there must also be a clear policy stating how a CAP message that is not compliant with the CAP Profile should be handled, e.g., Must it be treated as invalid? Similarly, policy should be clear on the appropriate processing when an alerting authority receives a CAP message that is not compliant with any particular CAP Profile that is supposed to be respected.

2.3. CAP Alert News Feeds

2.3.1 Preference of RSS for CAP Alert News Feeds - CAP alert feeds published on the Internet could use either of two standard XML formats for news feeds: Really Simple Syndication (RSS) or Atom. The Alerting System should specify if there is no preference between RSS and Atom, a preference for RSS, or a preference for Atom. It is noted here that: RSS is the more common format, RSS is completely adequate for the emergency alerting purpose, and RSS is frozen so that it will not change over time.

[16] The Technical Advisory Note is at https://www.oasis-open.org/committees/download.php/45483/TechnicalAdvisoryNote-v11-fina(JP).docx

[17] From section 3.6: "Constructing Alert Text from CAP V1.2 IPAWS v1.0 Profile for EAS Activations" in the Guide at http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

[18] OpenBroadcaster is described at https://alerts.pelmorex.com/lastmilesdistributors/openbroadcaster/

2.3.2 Mapping of Element Values between CAP Alerts and RSS Items - If RSS is the preferred or required Internet news feed format, it is useful to suggest how the values in an RSS item can be populated using values of the CAP alert elements, plus the CAP file URL. Here is an example mapping:

RSS channel/item/title	CAP alert/info/headline
RSS channel/item/link	CAP file URL
RSS channel/item/description	CAP alert/info/description
RSS channel/item/author	CAP alert/sender
RSS channel/item/category	CAP alert/info/category
RSS channel/item/guid	CAP alert/identifier
RSS channel/item/pubDate	CAP alert/sent

It is also noted here that the OASIS Emergency Management Technical Committee (OASIS EM TC), maintainer of the CAP specification, published a guide named "Example Practices: CAP Feeds". [19]

2.4. Validity, Encryption, and Authentication of CAP Alerts

2.4.1 Validating CAP Alerts - As mentioned earlier in these notes, a CAP alert must be packaged as a file of type XML. The XML content of the CAP alert file must be valid according to the currently adopted CAP schema version. The Alerting System should specify which version of CAP (1.1 or 1.2, as of this writing) is preferred or required, which may change over time. [20] It is noted that CAP version 1.2 is widely supported, and that it is only slightly different than version 1.1.

2.4.2 Encrypting CAP Alerts - It is likely that many, perhaps most, CAP alert messages communicated through the Alerting System will not be intended for public dissemination. To protect against unintentional disclosure of alert message content, encryption on communications links should be applied. For messaging over the Internet, such encryption is accomplished using HTTPS.

2.4.3 Authentication of CAP Alerts - Emergency alerting should be regarded as a likely target for malicious attacks, which can include attempts to disable alerting or to send deceptive alerts. The Alerting System should state if a digital signature is required to provide assurance that the CAP alert content as received is identical to the CAP alert content as sent.

2.5. High Priority Alerts Must be Easily Distinguished

2.5.1 Need to Distinguish High-Priority Alerts - The term "high priority" refers to alerting situations in which people should be alerted in a "broadcast intrusive" manner, such as sounding a siren, inserting a television "crawl text", sending a cell broadcast message, etc. This is usually reserved for situations in which people need to act: immediately or within the next hour, in response to an extraordinary or significant threat, that is already observed or is likely to occur. (These correspond to the top two values of Urgency, Severity, and Certainty in a CAP message.) Although high priority alerts are less than one percent of the alert messages typically accessible to the public, such messages are especially crucial to

[19] The OASIS EM TC guide named "Example Practices: CAP Feeds" is at http://docs.oasis-open.org/emergency-adopt/cap-feeds/v1.0/cap-feeds-v1.0.html

[20] The XML schema for CAP alerts is found in the specifications, versions 1.1 and 1.2, at http://docs.oasis-open.org/emergency/cap/

enable people to preserve life and protect property. [21] Also, given the intense nature of a high-priority alert, alerting authorities should issue an "all clear" message after the high-priority threat is over.

2.5.2 Criteria to Distinguish High-Priority Alerts - The designation "high priority" should be defined as any valid CAP alert that satisfies these six criteria for specific CAP element values:

alert/status = Actual	(not = Exercise, System, Test, nor Draft)
alert/msgType = Alert or Update	(not = Cancel, Ack, nor Error)
alert/scope = Public	(not = Restricted nor Private)
alert/info/urgency = Immediate or Expected	(not = Future, Past, nor Unknown)
alert/info/severity = Extreme or Severe	(not = Moderate, Minor, nor Unknown)
alert/info/certainty = Observed or Likely	(not = Possible, Unlikely, nor Unknown)

2.6. Suggestions for Values in Specific CAP Alert Elements

2.6.1 Example Practices for CAP Elements - The OASIS EM TC published a useful guide named "Example Practices: CAP Elements". [22] This guide contains notes on these ten topics pertinent to CAP alerts: Optimize alert areas, Include useful descriptions and instructions; Take care with XML encoding; Customize urgency, severity, certainty to event; Provide rich content by linking to resources; Prepare CAP Usage Documentation; Public Alert Aggregators Should Ignore CAP Messages with a Restriction Element; Alerts that span jurisdiction boundaries; Alert updates; and, Alert information expiration.

2.6.2 Usage of Particular CAP elements - In addition to the OASIS EM TC suggestions, the Alerting System could consider providing guidance on the usage of particular CAP elements such as are described here following.

2.6.2.1 CAP element - alert/identifier: Many countries are using CAP Object Identifiers (OIDs) that are tied to the international Register of Alerting Authorities. This identifier scheme assures that each CAP alert has a globally unique identifier that is also traceable to the particular official alerting authority which sent the alert. [23]

2.6.2.2 CAP element - alert/sender: It is considered good practice that the sender value contains an e-mail address leading to an inquiry function that can respond when necessary.

2.6.2.3 CAP elements - alert/status, alert/msgType, and alert/scope: The Alerting System could define more precisely what is regarded as appropriate use of the allowed values of the status element (Actual, Exercise, System, Test, and Draft), the msgType element (Alert, Update, Cancel, Error) and the scope element (Public, Restricted, Private).

2.6.2.4 CAP element - alert/info: The Alerting System should prohibit more than one "info" element in a single CAP alert. Although Canada, for example, uses two info elements in order to carry English and French in a single alert, this practice does not align with common practice of Internet news feeds. A news feed is expected to have one language, so the CAP alerts linked from that news feed should also

[21] The GDPC Guide for Identifying High Priority Public Warnings is at http://preparecenter.org/resources/universal-app-identifying-high-priority-public-warnings

[22] The OASIS EM TC guide named "Example Practices: CAP Elements" is available at http://docs.oasis-open.org/emergency-adopt/cap-elements/v1.0/cn01/cap-elements-v1.0-cn01.html

[23] Common questions about OID's are addressed at http://www.oid-info.com/faq.htm For example, OIDs for CAP alert messages from Mexico's CONAGUA should start with "urn:oid:2.49.0.1.484.0.", which identifies the country (484 is the code for Mexico), and an alerting authority in Mexico (0 for CONAGUA). OIDs can have any number of periods, but only positive numbers (not zero filled) between the periods.

have just one language. Also, some current EAS technology only processes the first "info block" of a CAP message.

2.6.2.5 CAP element - alert/info/language: The Alerting System should specify use of the two-character language code, rather than the five character code for a country variant of the language.

2.6.2.6 CAP element - alert/info/event: The values used in the event element should be each no more than 50 characters long. To facilitate alignment of an alert to auxiliary information that varies by type of event, this value should be taken from a widely known list of events. For example, such a list is given in Mexico's General Law for Civil Protection. [24]

2.6.2.7 CAP elements - alert/info/urgency, alert/info/severity, and alert/info/certainty: The Alerting System should prohibit use of "Unknown" value in these elements. This is necessary because many deployed CAP systems handle "unknown" incorrectly, treating the respective values as "not urgent", "not severe", and "not certain".

2.6.2.8 CAP elements - alert/info/description and alert/info/instruction: The text in the description and instruction elements should be kept fairly short to accommodate the fullest range of dissemination channels. Also, the most important information should be given first, in anticipation that the full text may be truncated or that a receiver may not take time to read all of the text.

2.6.2.9 CAP element - alert/info/web: The Alerting System should use this element to link to online information that provides practical guidance for people reacting to the alerts, such as where to find shelter. Such online information is available from Red Cross/Red Crescent resources, for example.

2.6.2.10 CAP element - alert/info/area/geocode: Although the use of geocode values is allowed by the CAP standard and is sometimes useful to distinguish an area very accurately and precisely, it should be understood that some actors in alert dissemination will not have access to the particular gazetteer function necessary to convert the given geocode values to lat/lon polygons. For this reason, the Alerting System should require that the corresponding polygon is also included in each CAP alert.

2.7. Alert Content Should be Easily Understood

2.7.1 Templates with Stock Phrases - There now appears to be broad consensus that an alert composer should incorporate "stock phrases" in emergency alert messages [25] and such phrases are often part of an "alert template". For instance, templates for 20 common emergency alert situations were developed in 2012 as part of the Regional Risk Reduction Initiative in the Caribbean. These templates, in Dutch, English, French, Spanish, and Papiamento, are feely available. [26] It should be understood, however, that stock phrases do evolve over time. For instance, for decades various hazard threats have been ranked using the terms "advisory, watch, warning" but that set of terms is likely to be retired soon.

[24] The list of events in the law as provided to the author by Rafael Marin, in Spanish and English, is available here: https://drive.google.com/file/d/0B5FiAsl5yGbZOHlOMTJ6M01lUE0/view?usp=sharing

[25] Janoske M, Brooke L, Sheppard B. Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators. Final Report. College Park, MD, USA. http://www.start.umd.edu/start/publications/UnderstandingRiskCommunicationBestPractices.pdf

[26] Templates for twenty common emergency alert situations (in Dutch, English, French, Spanish, and Papiamento) are feely available at https://docs.google.com/file/d/0B5FiAsl5yGbZUHZkWnE1Y2I5aTg/

2.7.2 Predefined Alert Areas - In some situations, the public may be already aware of areas that have a well-known risk for a particular hazard. Examples include areas near active volcanoes and the "tsunami-aware communities" that have deployed distinctive signage and other education. In a CAP-enabled alerting system, the official alerts should include polygons matched to these pre-defined areas.

2.7.3 Communicating Uncertainty - An ongoing challenge for alerting authorities is to communicate uncertainty in a way people understand and different techniques have been employed for different kinds of hazard threats. [27] Given that every person is potentially faced with hazards of many different types, the communication of uncertainty ought to be approached from an all-hazards perspective.

2.7.4 Impact-Based Alerting - A current trend in making alerts more understandable is to focus more on the impact of a hazard on people and what actions they need to take, as distinct from describing the hazard itself. The CAP standard facilitates this trend to some degree because the CAP instruction element is distinct from the CAP description element, in contrast to traditional free text alerts wherein instructions are mixed with descriptions in a narrative crafted in a bulletin or press release style. [28]

Acknowledgments

This document is a generalized version of the 2016 report titled "Toward a CAP-enabled National Alert System: Some Notes for the Government of Mexico" [29] The contributors to that report are gratefully acknowledged: Cyrille Honore, Efraim Petel, Eliot Christian, Elizabeth Klute, Elysa Jones, and Norm Paulsen. Additional contributors to this document specifically are listed in the table below.

Glossary of Terms

alerting authorities - organizations designated by nations as authoritative in the context of alerting

Atom (Atom Syndication Format) - Atom is an XML format used for web feeds, alternative to RSS

CAP (Common Alerting Protocol) - an XML-based data format for exchanging public warnings and emergencies between alerting technologies

EAS (Emergency Alert System) - the national public warning system of the United States

FIA (Federation for Internet Alerts) - a facilitator for Internet technology and services collaboration among companies, non governmental organizations, and alerting authorities

IFRC (International Federation of Red Cross and Red Crescent Societies) - the world's largest humanitarian organization, with 190 member National Societies

GDPC (Global Disaster Preparedness Center) - an IFRC resource center that promotes innovation in disaster preparedness and knowledge sharing amongst disaster preparedness practitioners

[27] Gill J. Guidelines on Communicating Forecast Uncertainty (PWS-18). Technical Document. Geneva, Switzerland; World Meteorological Organization, Public Weather Services; 2008. WMO/TD No. 1422. http://www.wmo.int/pages/prog/amp/pwsp/documents/GuidelinesonCommunicatingUncertainty_TD-4122.pdf.

[28] see WMO Guidelines on Multi-hazard Impact-based Forecast and Warning Services / Directrices de la OMM sobre servicios de predicción y aviso multirriesgos que tienen en cuenta los impactos

[29] The Report is available at http://preparecenter.org/resources/cap-mexico-notes

HTTPS (Hypertext Transfer Protocol Secure) - the use of Hypertext Transfer Protocol (HTTP) with Secure Socket Layer (SSL)

NWR (NOAA Weather Radio) - The U.S. National Weather Service maintains NWR to broadcast weather and other messages (e.g. national security, environmental and public safety) through EAS

OASIS EM TC - OASIS (Organization for the Advancement of Structured Information Standards), Emergency Management Technical Committee

OID (Object Identifier) - a hierarchically-assigned identifier expressed using the ASN.1 (Abstract Syntax Notation) standard, X.690, defined by the International Telecommunication Union

Red Cross and Red Crescent National Societies – National Societies are the independent members of the IFRC, typically having a formal auxiliary role to their national governments

RSS (Really Simple Syndication) - RSS is an XML format used for web feeds, alternative to Atom

Register of Alerting Authorities - an online facility maintained by the maintained by the World Meteorological Organization and the International Telecommunication Union

URL (Uniform Resource Locator) - an Internet address usually consisting of the access protocol, the host domain name, and optionally the path to a service or resource accessible on that host

SMS (Short Message Service) - a text messaging service component of phone, Web, or mobile communication systems

SSL (Secure Socket Layer) - encrypts data being transmitted so that a third party cannot understand it

UNDP (United Nations Development Program) - a UN agency very active in developing countries

WEA (Wireless Emergency Alerts) - emergency messages sent by authorized U.S. government alerting authorities through mobile carriers

web feed (or news feed) - a data format used for providing users with frequently updated content

XML (eXtensible Markup Language) - a set of rules for encoding documents in a format that is both human-readable and machine-readable