



# Web Services and the Common Alerting Protocol (CAP)

```
<alert>  
<msg_id>43b08071-3727-41b4-  
<sender_id>U.S. Federal Gover  
<sent>2003-04-02T14:39:01-05:0  
<msg_status>Actual</msg_status  
<msg_scope>Public</msg_scope>  
<msg_type>Alert</msg_type>  
<info>  
<language>en-US</language>  
<event_cat>Security</event_ca  
<event_type>Homeland Securiti  
<urgency>Forecast</urgency>  
<severity>Severe</severity>  
<certainty>High</certainty>  
<info_url>http://www.dh  
<info_url>http://www
```

# ○ ● ● Outline

---

- Web Services
- The Common Alerting Protocol
- Applications

# ○ ● ● Web Services

- Using web servers (HTTP) and XML for computer-to-computer communications
- Avoids most firewall and interoperability problems
- Services are self-documented; interfaces can self-program
- Microsoft, Sun et al. agree (!)

# An XML Message

```
<alert>
  <identifier>43b08071-3727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <scope>Public</scope>
  <type>Alert</type>
  <info>
    <language>en-US</language>
    <category>Security</category>
    <event>Homeland Security Advisory System</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <from>U.S. Federal Government, Department of Homeland Security</from>
    <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
    <image>http://www.dhs.gov/dhspublic/getAdvisoryImage</image>
    <parameter>HSAS=orange</parameter>
    <area>
      <areaDesc>U.S. nationwide</areaDesc>
    </area>
  </info>
</alert>
```

# An XML Message

```
<alert>
  <identifier>43b08071-3727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <scope>Public</scope>
  <type>Alert</type>
  <info>
    <language>en-US</language>
    <category>Security</category>
    <event>Homeland Security Advisory System</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <from>U.S. Federal Government, Department of Homeland Security</from>
    <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
    <image>http://www.dhs.gov/dhspublic/getAdvisoryImage</image>
    <parameter>HSAS=orange</parameter>
    <area>
      <areaDesc>U.S. nationwide</areaDesc>
    </area>
  </info>
</alert>
```

# ○ ● ● Web Service Technology

## ● Standard protocols (XML / SOAP)

- Cross-platform data transfer
- Encryption and digital signature standards

## ● Service descriptions (WSDL)

- Defines messages and transaction sequences

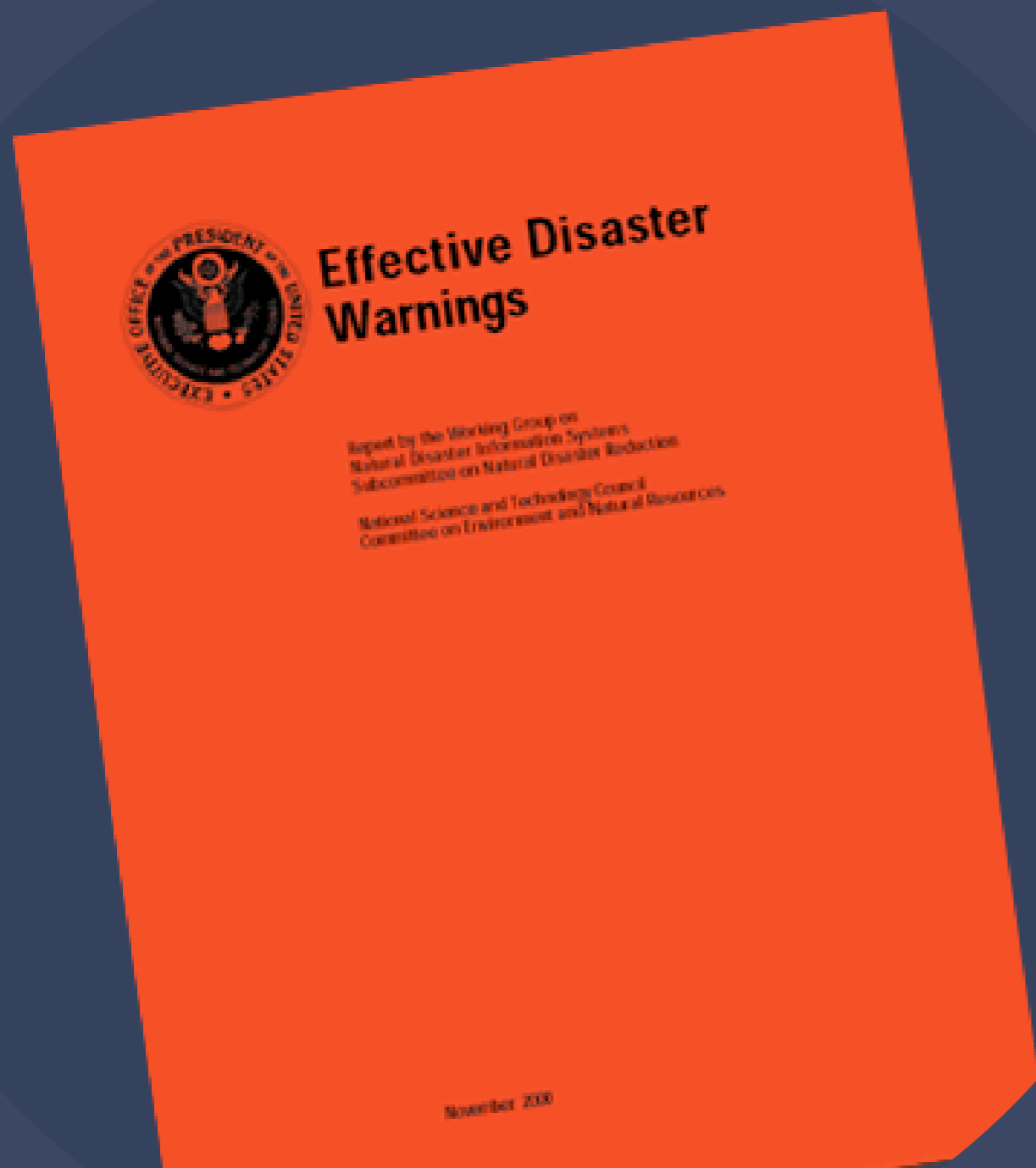
## ● Registries (UDDI / ebXML)

- “Yellow pages” for Web services

# ○ ● ● The Common Alerting Protocol

- An open, non-proprietary standard for Web services
- All-hazard notification and alerting
- Flexible and comprehensive
- Can reference parameters, images, audio

# ● ● ● CAP History - 2000



National Science  
and Technology  
Council releases its  
"Red Book" report  
on "Effective  
Disaster Warnings"

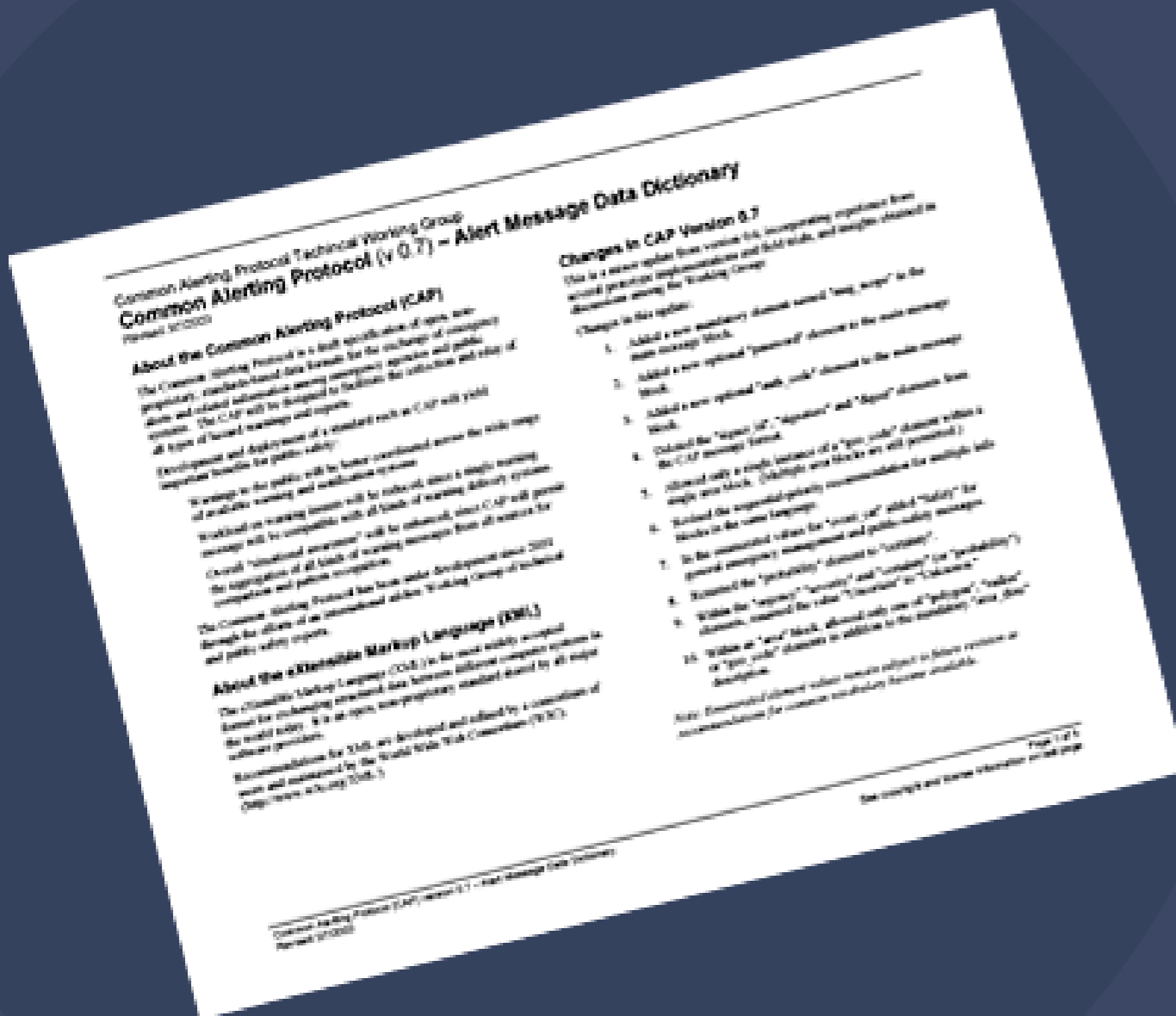
# ○ ● ● CAP History - 2001

Formation of:

- Partnership for Public Warning
- CAP Ad-Hoc Working Group

# CAP History - 2002

## Draft CAP Format



# CAP History - 2002

- Draft CAP Format
- Prototype Applications

The screenshot displays two overlapping web browser windows. The background window is titled "Message Entry Form - Microsoft Internet Explorer" and shows a "CAP Message Input Form" for the Northern Shenandoah Valley ITS Public Safety Initiative. The form includes fields for "User ID:", "Password:", and "Message Type:" (set to "Test"). Below these are fields for "Source Description:", "Event Category:" (set to "Weather"), "Urgency:" (set to "Immediate"), and "Affected Area (I)". A "Draw Area" button is visible. The foreground window is titled "Draw Polygon - Microsoft Internet Explorer" and shows a map of the Shenandoah Valley region with a red polygon drawn over a central area. A scale bar at the bottom of the map indicates 2.0 km and 1.5 mi. Below the map are "Finished" and "Reset" buttons.

**Common Alerting Protocol**

This is a test input form for the Northern Shenandoah Valley ITS Public Safety Initiative.

A Java application for monitoring CAP demonstration messages can be [downloaded here](#).

Information about the Common Alerting Protocol project is [available here](#).

**CAP Message Input Form**  
(Required elements are labeled in RED.)

User ID:  Password:  Message Type:

Source Description:

Event Category:

Urgency:

Affected Area (I):

Draw Area

Headline:

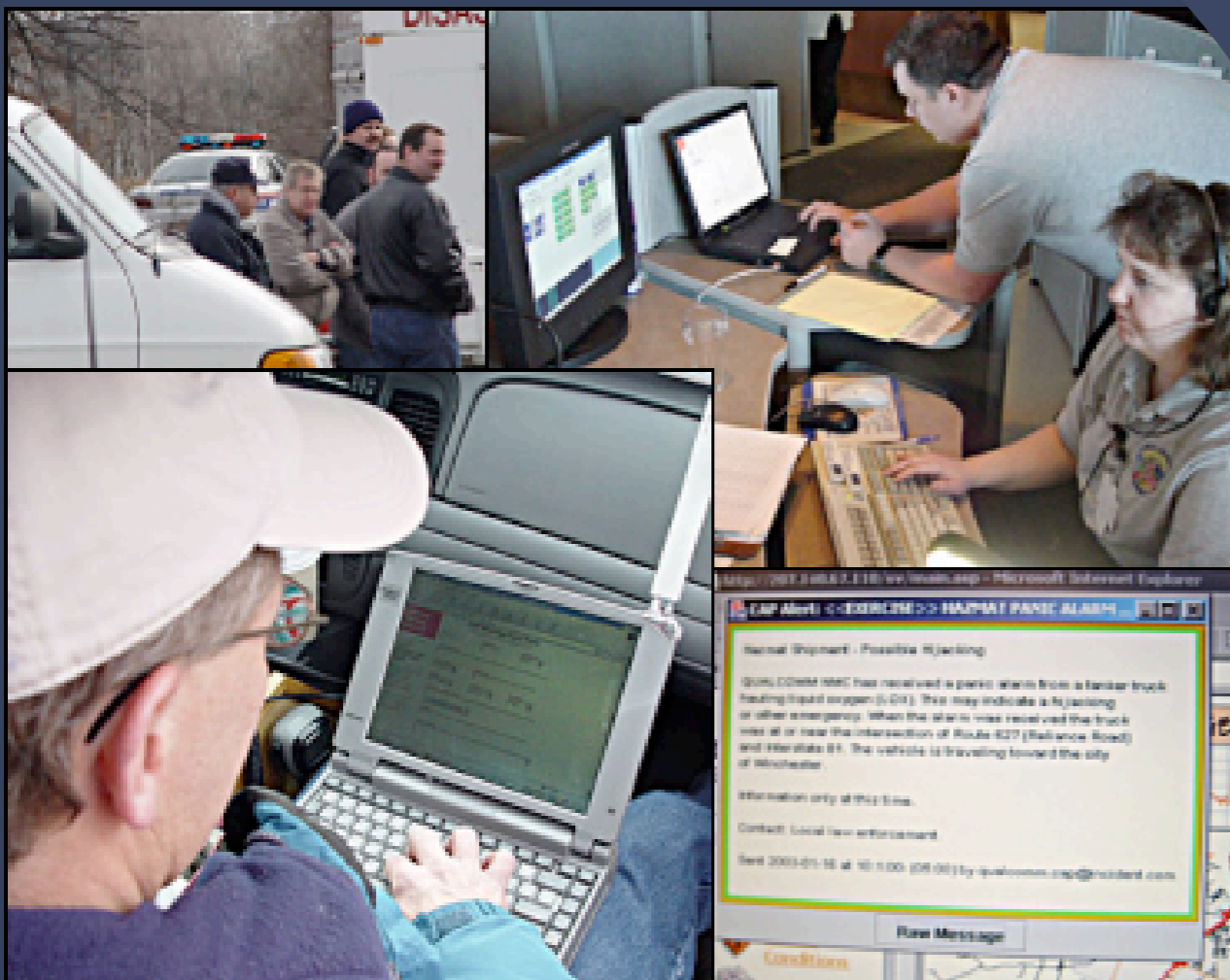
Event Description:

Now click 'Finished' to proceed or 'Reset' to clear and redraw.

Finished Reset

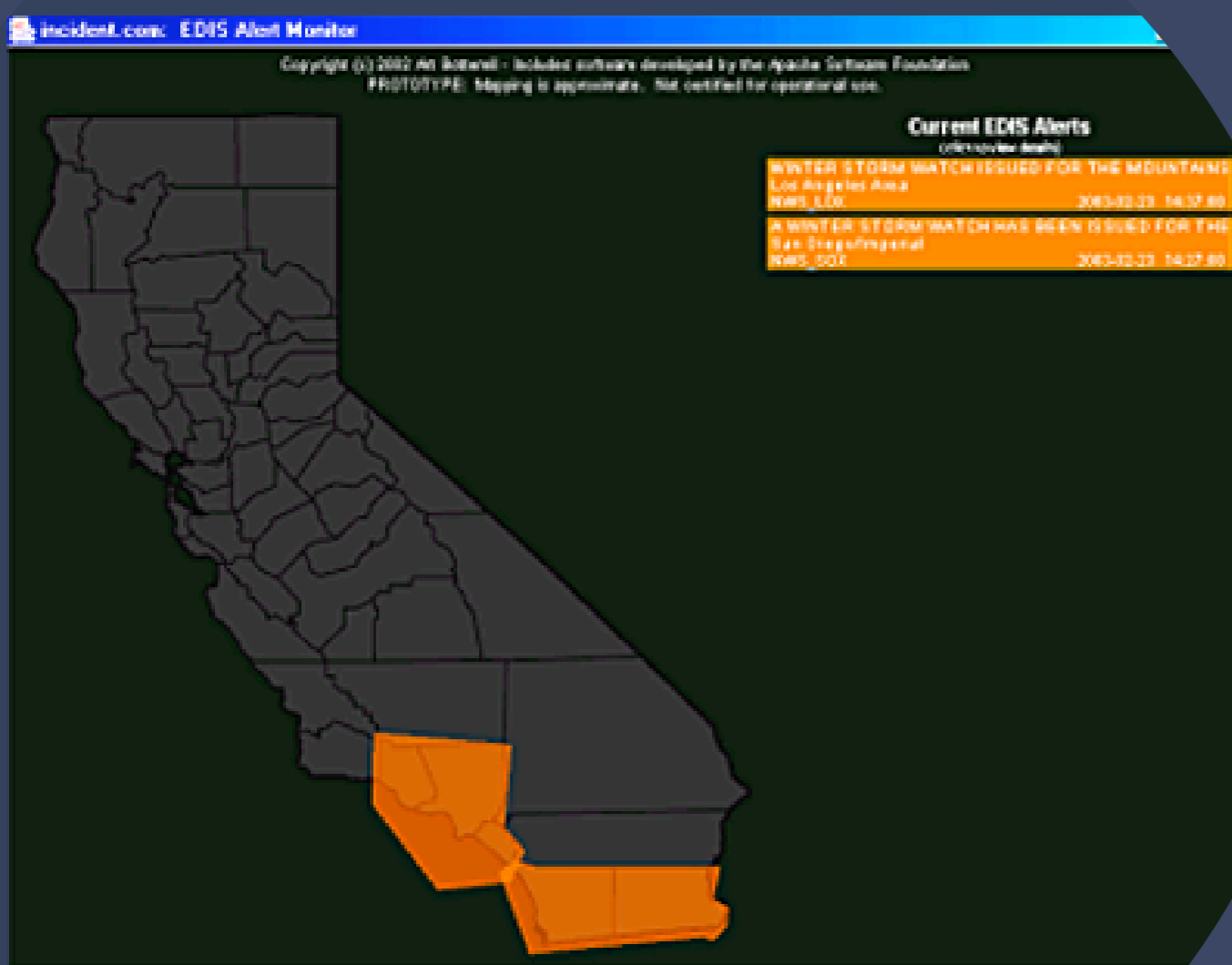
# ● ● ● CAP History - 2002

- Draft CAP Format
- Prototype Applications
- Virginia Field Trials (ComCARE Alliance)



# ● ● ● CAP History - 2002

- Draft CAP Format
- Prototype Applications
- Virginia Field Trials (ComCARE Alliance)
- California Field Trial (California EDIS)



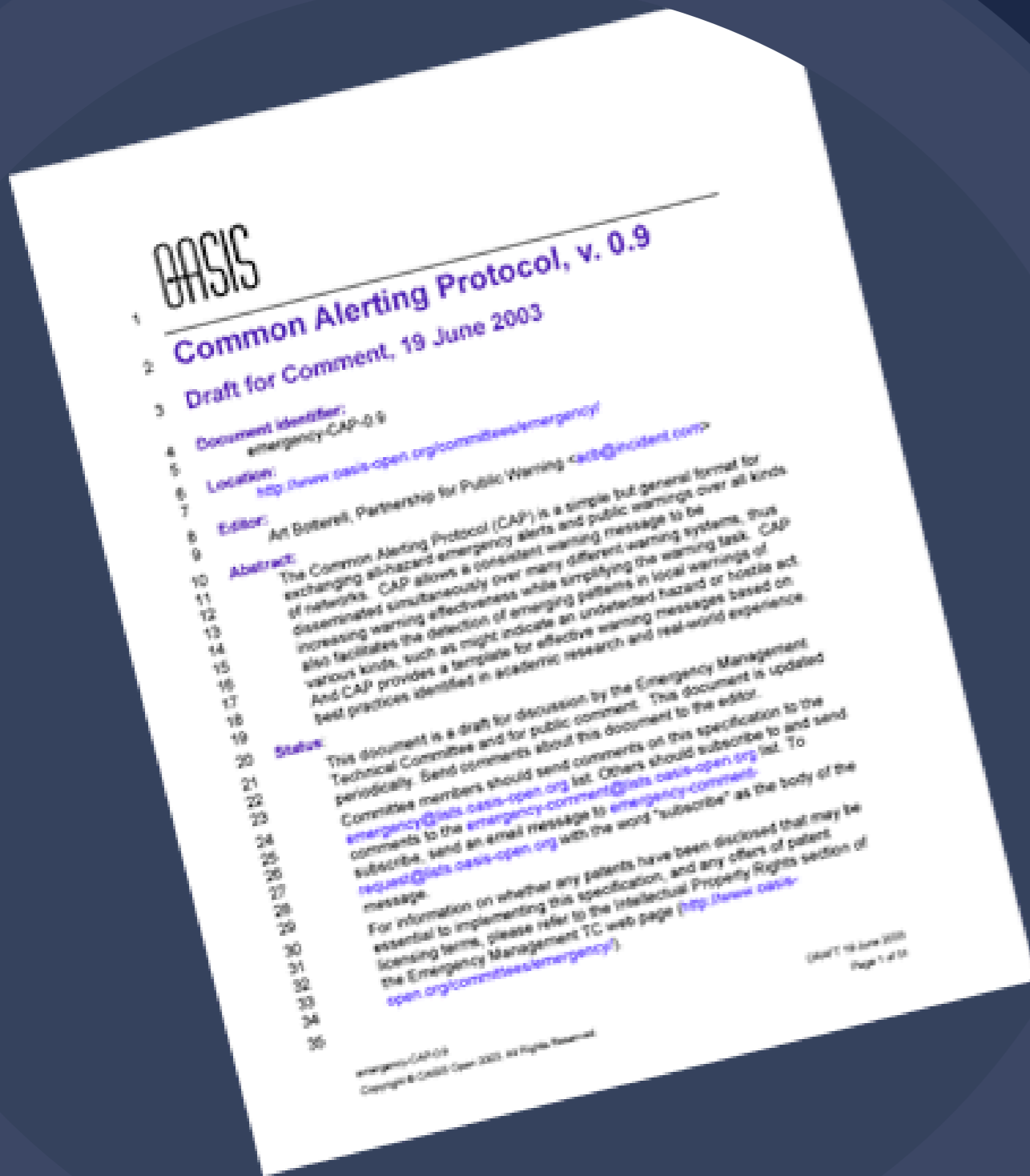
# ○ ● ● CAP History - 2003

- OASIS standards organization forms "Emergency Management XML Technical Committee"
- EM TC selects CAP as its first standards-track project
- CAP draft released for public review and comment

# ● ● ● The OASIS draft

For your review  
and comment:

*[http://  
www.oasis-  
open.org/  
committees/  
emergency/](http://www.oasis-open.org/committees/emergency/)*





# The CAP Message

(As of draft version 0.9)

- Alert Block - information about this message *which may contain...*
- Info Block(s) - information about the event or hazard *which may contain...*
- Area Block(s) - information about the affected area(s)

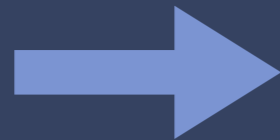


# The CAP Message

(As of draft version 0.9)

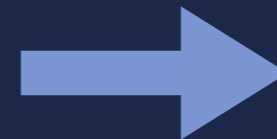
## alert

**Message ID**  
**Sender ID**  
**Date/Time Sent**  
**Alert Status**  
**Alert Type**  
*Password*  
*Operator ID*  
*Alert Scope*  
*Restriction*  
*Address*  
*Handling Code*  
*Note*  
*Reference ID*  
*Incident ID*



## info

**Event Category**  
**Event Type**  
**Urgency**  
**Severity**  
**Certainty**  
*Language*  
*Audience*  
*Target Code*  
*Date/Time Effective*  
*Date/Time Onset*  
*Date/Time Expires*  
*Sender Name*  
*Headline*  
*Event Description*  
*Instructions*  
*Information URL*  
*Image URL*  
*Audio URL*  
*Contact Info*  
*Parameters*



## area

**Area Description**  
*Polygon*  
*Circle*  
*Geocode*  
*Altitude*  
*Ceiling*

# ○ ● ● The Alert Block

Basic information about this message:

- Date/Time
- Sender
- Message Type & Status
- Distribution Scope

# ● ● ● Message Type

Describes the general purpose of this message:

<b>Alert</b>	Initial information about an event or hazard
<b>Update</b>	New information updating an earlier message
<b>Cancel</b>	Cancels an earlier message
<b>Ack</b>	Acknowledges receipt and acceptance of a message
<b>Error</b>	Indicates rejection of a message (with explanation)

# ○ ● ● Message Status

Describes the appropriate use of this message:

<b>Actual</b>	Refers to actual hazards or events
<b>Exercise</b>	Refers to simulated hazards of events, for exercise participants
<b>Test</b>	Technical testing, not actionable
<b>System</b>	Network internal messages, updates, etc.

# ○ ● ● Message Scope

Describes the appropriate dissemination of this message:

<b>Public</b>	For general delivery to unrestricted audience and the public
<b>Restricted</b>	For delivery only according to a specified rule.
<b>Private</b>	For delivery only to specified addresses.

# ○ ● ● The Info Block

---

## Specifics of an event or a threat:

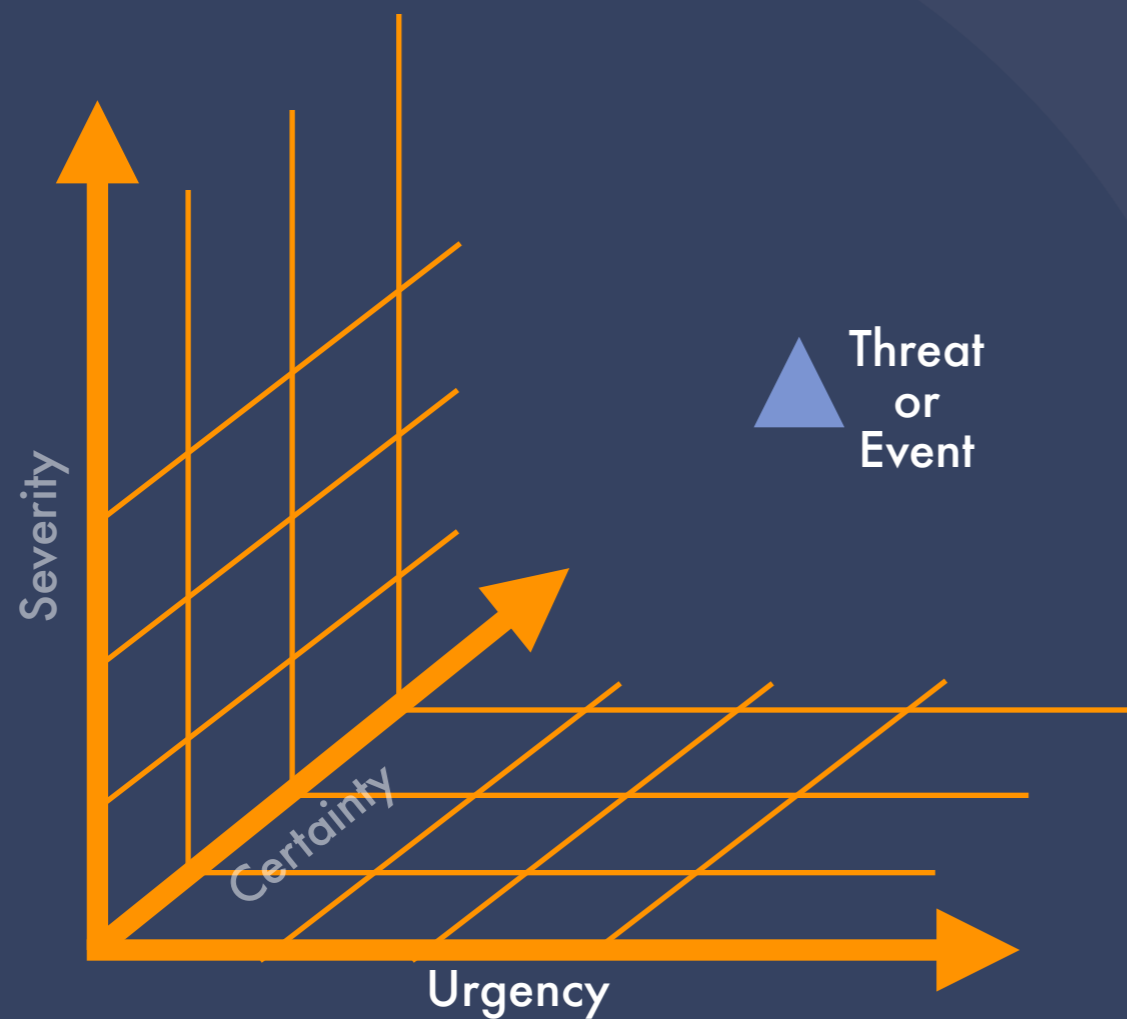
- Category and description
- Urgency / Severity / Certainty
- Timeframes
- Recommended action
- Links to additional information

# Event Category

*(A perfect list is hard to find!)*

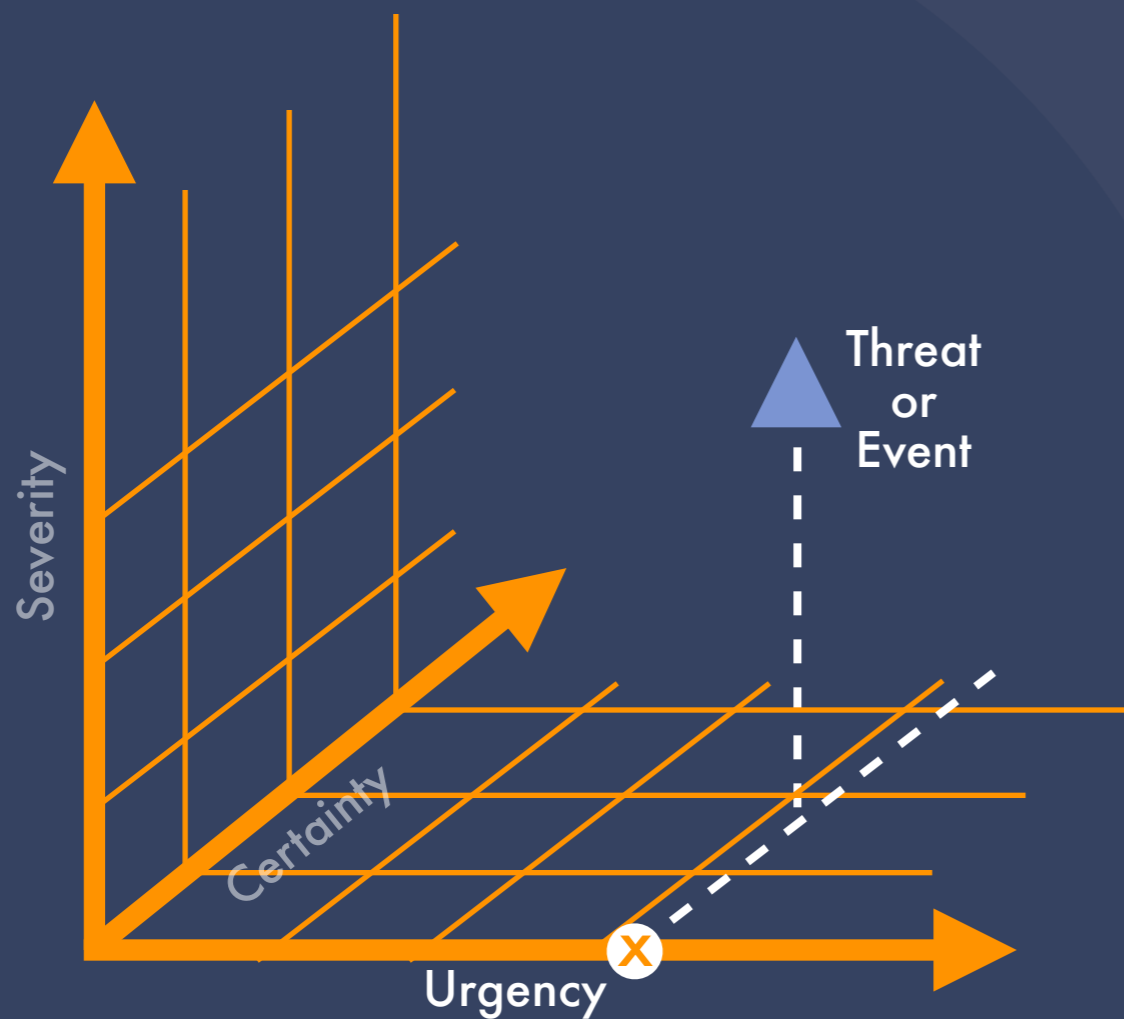
<b>Geo</b>	Geophysical
<b>Met</b>	Meteorological
<b>Safety</b>	General emergency and public safety
<b>Security</b>	Law enforcement, military, homeland and private security
<b>Rescue</b>	Rescue and recovery
<b>Fire</b>	Fire suppression
<b>Health</b>	Public health and medical
<b>Env</b>	Hazmat, pollution and other environmental
<b>Transport</b>	Public and private transportation
<b>Infra</b>	Utility, telecommunications, other infrastructure
<b>Other</b>	Not otherwise categorized

# ○ ● ● The U/S/C Model



- Traditional one-dimensional model of "priority" is expanded into a "3D" model that expresses:

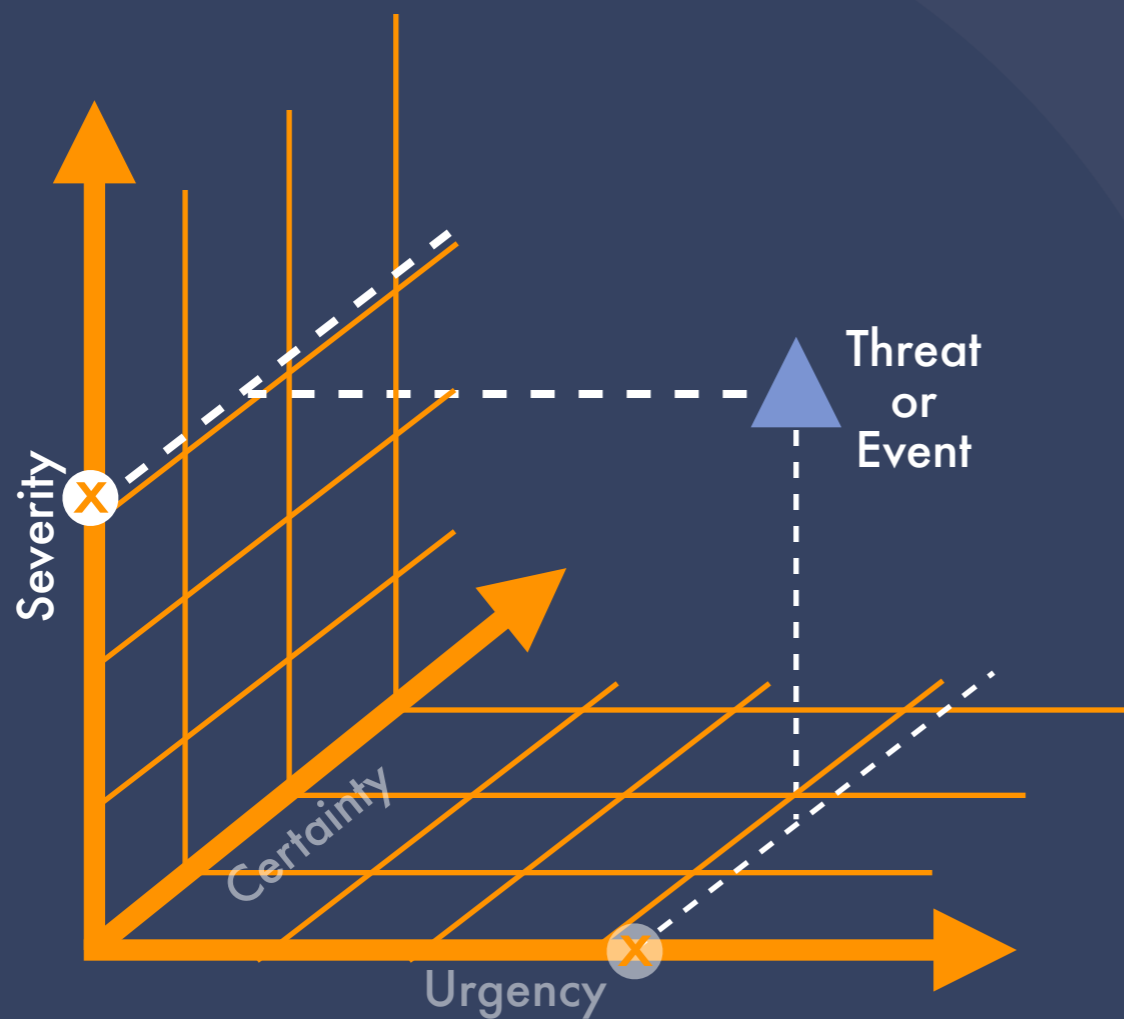
# ○ ● ● The U/S/C Model



● Traditional one-dimensional model of “priority” is expanded into a “3D” model that expresses:

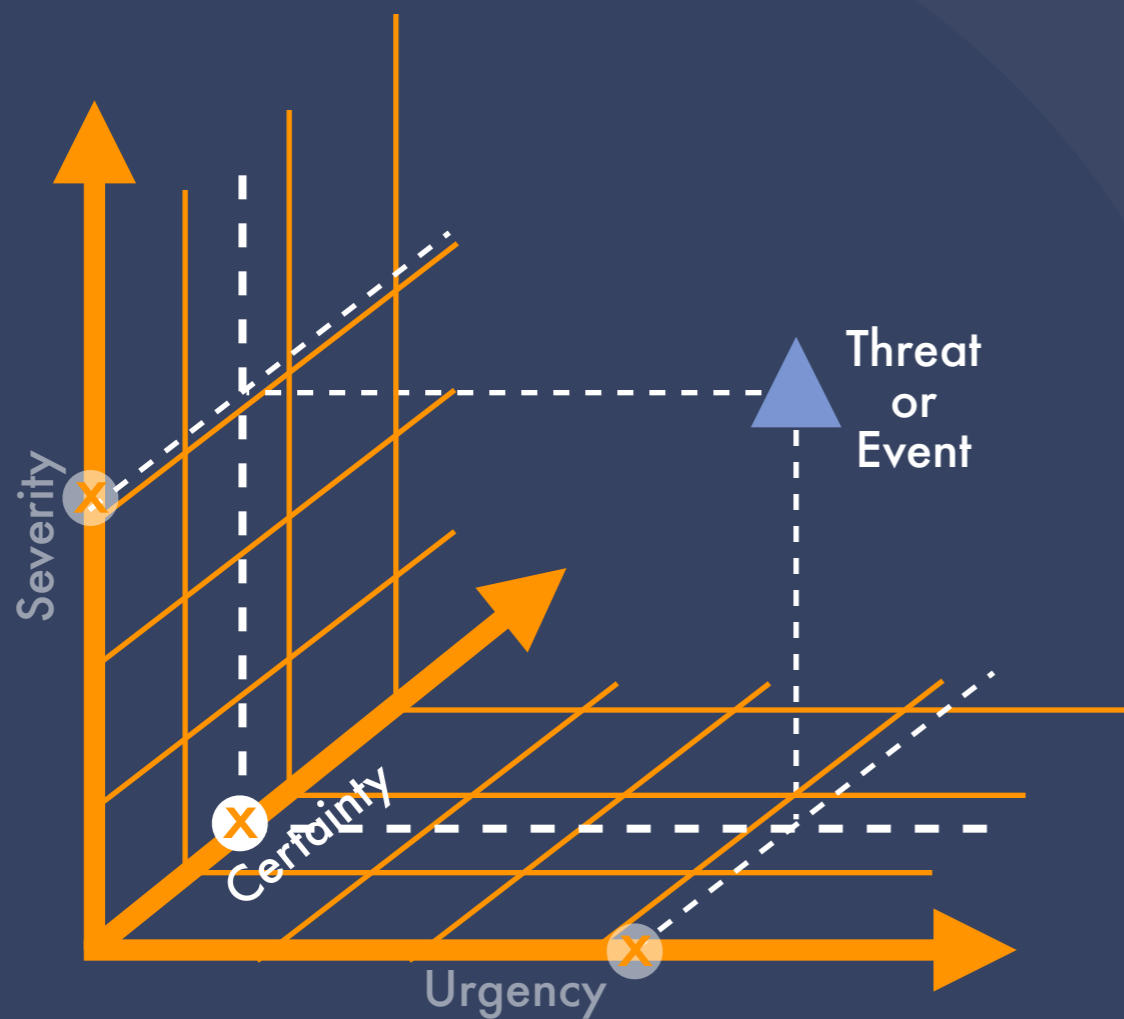
○ Urgency (time)

# ○ ● ● The U/S/C Model



- Traditional one-dimensional model of "priority" is expanded into a "3D" model that expresses:
  - Urgency (time)
  - Severity (impact)

# ○ ● ● The U/S/C Model



- Traditional one-dimensional model of “priority” is expanded into a “3D” model that expresses:
  - Urgency (time)
  - Severity (impact)
  - Certainty (probability)



# Urgency

In the U/S/C model

Describes the time available to prepare:

<b>Immediate</b>	Responsive action should be taken immediately
<b>Expected</b>	Action within next hour
<b>Future</b>	Action in near future (typically 6-24 hours)
<b>Past</b>	Past, no preparatory action required
<b>Unknown</b>	Not known



# Severity

In the U/S/C model

Describes the intensity of impact (if it occurs):

<b>Extreme</b>	Extraordinary or large-scale threat to life and property
<b>Severe</b>	Significant threat to life and property
<b>Moderate</b>	Potential threat to life and property
<b>Minor</b>	Limited threat to live and property
<b>Unknown</b>	Not known

# ○ ● ● Certainty

In the U/S/C model

Describes the issuer's confidence that the event will occur or has occurred as described:

<b>Very Likely</b>	Highly likely or certain ( $p > 85\%$ )
<b>Likely</b>	Likely, although not highly likely ( $p > 50\%$ )
<b>Possible</b>	Possible but not likely ( $p < 50\%$ )
<b>Unlikely</b>	Not expected to occur
<b>Unknown</b>	Not known

# ○ ● ● <parameter> element

- Any application-specific values

- In the form:

`key=value`

- Example:

`<parameter>M1=5.2</parameter>`

- Multiple instances permitted

# ○ ● ● <image> and <audio>

- For binary attachments
- URI may refer to asset on a separate server ("binary pull") or to SOAP attachment transmitted with message ("binary push")

# ○ ● ● The Area Block

Geographic target area:

- Text description and combo of:
  - GIS Polygon (area)
  - Point and Radius
  - Geographic Code (FIPS, ZIP, etc.)
- Optional altitude and ceiling

# ○ ● ● Applications of CAP

- Dissemination of forecasts, event data and updates
- Reporting sensor data
- Aggregation and correlation
- Archiving and reconstruction

# Contacts

for the Common Alerting Protocol project

## OASIS EM TC

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

## Partnership for Public Warning

<<http://www.ppw.us/>>

## CAP Working Group

<<http://www.incident.com/cap/>>

Workshop presented by

**Art Botterell**

<[acb@incident.com](mailto:acb@incident.com)>

copyright (c) 2003 Art Botterell

```
<alert>
<msg_id>43b08071-3727-41b4-
<sender_id>U.S. Federal Gover
<sent>2003-04-02T14:39:01-05:
<msg_status>Actual</msg_status>
<msg_scope>Public</msg_scope>
<msg_type>Alert</msg_type>
<info>
<language>en-US</language>
<event_cat>Security</event_ca
<event_type>Homeland Securiti
<urgency>Forecast</urgency>
<severity>Severe</severity>
<certainty>High</certainty>
<info_url>http://www.dh
<info_url>
```

