



# **Integrated Public Alert and Warning System**

## **IPAWS-OPEN Security Configuration for Operational Use**

**SIG Presentation**

**22 June 2011**



**FEMA**

# IPAWS-OPEN Status and Time Line

- ▶ Current status/timeline presented by FEMA Program Manager, Charles McCobb



## Operational MOA Guidance

- ▶ MOA is required for all operational COGs on a per COG basis.
- ▶ Will be executed only with organizations that have emergency management responsibilities (not to product vendors).
- ▶ Will be used as a prerequisite for issuance of an operational digital certificate for the COG.
- ▶ System permissions with IPAWS will be COG based. Different permission sets will require different COGs.
- ▶ EMA users and vendors should be aware of MOA w/ROB
- ▶ EMA must educate end users on ROB and attain signature
- ▶ Responsible for managing end user communities



## Vendor Support to Customer for Operational MOA

- ▶ May want to help your customer with the system details for his MOA. (see form)
- ▶ Vendors should review the possibility of automating the ROB process.
- ▶ Vendors should be sure that their product is compatible with the ROB.

## Signature Management (Operational MOA Holder)

- ▶ EMA's will receive sensitive information
  - Digital cert
  - Associated credentials (password and alias)
- ▶ EMA must safeguard received digital signatures
- ▶ Responsibility does not go away with delivery to vendor
- ▶ This should be included in any contractual agreement
- ▶ Detection of unauthorized use will cause access to IPAWS-OPEN to be removed.

## Signature Management (Vendor to Operational MOA Holder)

- ▶ You might want to consider making security “user configurable” for a EMA super user.
- ▶ Or you must be sure that your system maintains absolute security with regard to the clients credential.
- ▶ **YOU CANNOT SHARE AN OPERATIONAL CREDENTIAL!!!!!!**
- ▶ One COG, one signature, one set of permissions. They do not mix. Your customer/client will be held responsible. They will hold you responsible!

# Permission Management

- ▶ Right now only NWEM messages are “permission managed” in the sense that COGs have restricted capability (e.g. isCogAuthorized and getNwemAuxData).
- ▶ IPAWS-OPEN has structures internally to associate permissions with digital signatures for:
  - Event Code
  - SAME (FIPS) code
  - Distribution Method
  - Other factors
- ▶ As time goes by, Vendors may want to make it possible for for users to “see” their IPAWS permissions. (They will not be able to set them.)

# IPAWS-OPEN Vendor Implementation Intent

- ▶ Right now only your MOA is identified.
- ▶ Need to identify specific aspects of IPAWS-OPEN you intend to build to (or have already built to (see the attached form):
- ▶ Will eventually identify software use operationally:
  - Used by a customer with an operational COG.
  - Identified as using one or more of the functions in the intent registration form.
  - You do not have to reply. Usage will be defined as “Unidentified.”

# Comments and Questions

▶ **IPAWS Website** - <http://www.fema.gov/emergency/ipaws>

[Mark.Lucero@dhs.gov](mailto:Mark.Lucero@dhs.gov)

Office (202) 646-1386

Chief, IPAWS Engineering, National Continuity Programs, DHS FEMA

[Gary.Ham@associates.dhs.gov](mailto:Gary.Ham@associates.dhs.gov)

Office: (703) 899-6241

Contractor, Systems Architect, IPAWS-OPEN

