



Integrated Public Alert and Warning System

IPAWS – Update and Issues

SIG Presentation

20 June 2012



FEMA

IPAWS-OPEN Status

- ▶ **IPAWS-OPEN 3.01 is operational in TDL and Production.**
- ▶ **IPAWS-OPEN 3.01 production live connection to NOAA is in place. (Use care if you have a NOAA approved COG.)**
- ▶ **CMAS distribution is in place being rolled out by the carriers.**
- ▶ **EAS is live. The EAS encoding devices are ready and mostly in place.**
- ▶ **70+ Operational COGs and 28 with Alerting Authority designation (list is growing).**
- ▶ **Developer Documentation is available.**

Agenda

- ▶ You need a new Signature and COG for SOAP Access
- ▶ Policy for Non-FCC Regulated Entity Access to the Broadcasters' EAS Feed
- ▶ .jks Signature Conversion
- ▶ Downstream CAP processing – What Breaks (and Does Not Break) an Enveloped CAP Signature.
- ▶ IPAWS Open Signature Configuration Settings
- ▶ Alert Origination Use Cases – What you can build for your users employing IPAWS-OPEN.

Have You Requested Your New Signature?

- ▶ **Required for all Alert Originators**
- ▶ **You will get a New COG ID.**
- ▶ **You Will get a new x509 cert**
- ▶ **You must return the updated Intent Form**
- ▶ **COG 999 has become “Retrieve Only” (more discussion later.)**
- ▶ **You will get only a .jks file**
- ▶ **It will have separate passwords for the keystore and for the cert (alias) itself.**

EAS Feed Access

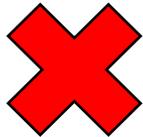
- ▶ **If you only want access to Public EAS Messages there is an Atom Feed option (easier than SOAP):**
- ▶ **Automatic access to any EAS Participant as defined in 47 CFR Part 11.2**
- ▶ **Re-Disseminators that meet the conditions and follow the rules of the iPAWS EAS Atom Feed Eligibility policy document (downloadable).**
 - **MOA required.**
 - **Your use will be reviewed and/or monitored to be sure you meet the rules.**

Converting your JKS file

- ▶ It can be converted to .PEM or .PFS
- ▶ PFS uses java keytool for translation.
- ▶ PEM requires two steps
 - Java keytool translation to PKCS12
 - openssl.exe translation to PEM
- ▶ You can also change the password of you JKS file using keytool (But not your alias/keypassword).

“Breaking” a Signature

- ▶ Any data change.
- ▶ Any change to whitespace between tags. (Simple “pretty print”)
- ▶ But name space label changes and assed namespaces have no effect on an Exclusive Signature.



```
<identifier>eg53_1234</identifier>  
<sender>abc@def.com</sender>  
TO  
<identifier>eg53_1234<identifier><sender>abc@def.com</sender>  
OR VICE VERSA
```



```
<identifier>Alert12_neg_</identifier>  
TO  
<cap:identifier>Alert12_neg_</cap:identifier>  
OR VICE VERSA
```



“Breaking” a Signature

- ▶ What is wrong with the following?

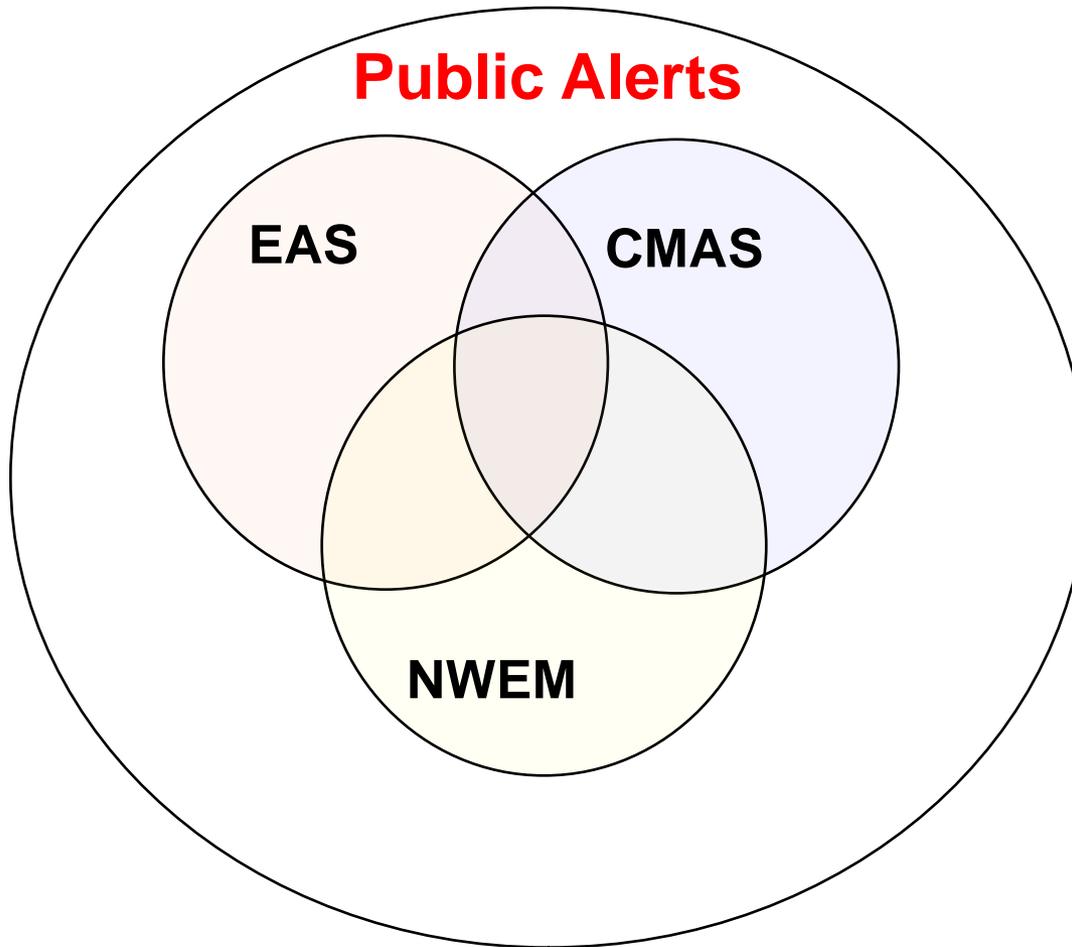
```
<identifier>eg53_1234</identifier>  
<sender>abc@def.com </sender>  
TO  
<identifier>eg53_1234<identifier>  
<sender>abc@def.com</sender>
```

- ▶ **Even trimmed whitespace will break a signature!**

CAP Signature Configuration Requirements

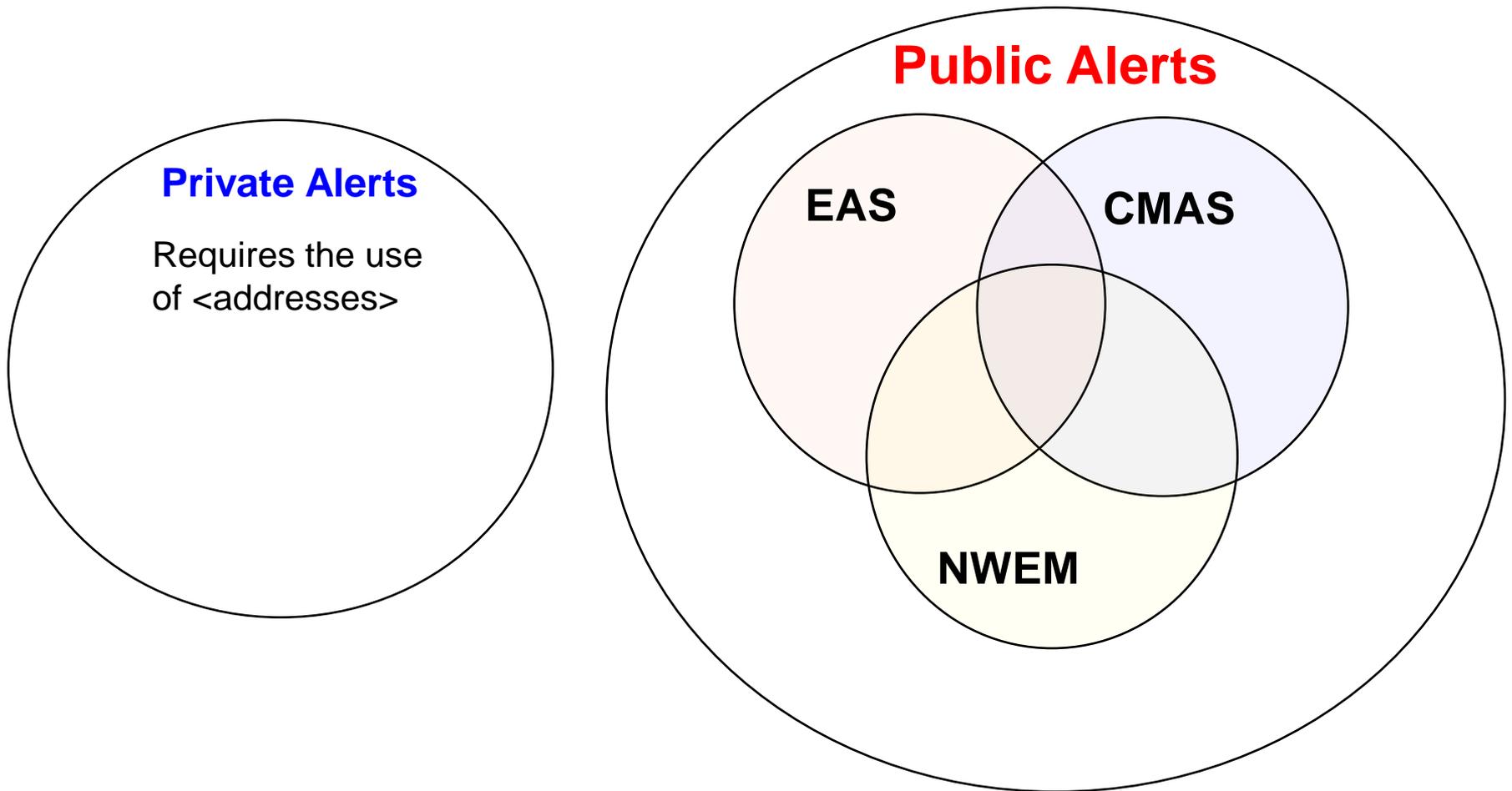
Signature Algorithm	RSA SHA-256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Canonicalization	Exclusive	http://www.w3.org/TR/xml-exc-c14n/
Digest	SHA-256	http://www.w3.org/2001/04/xmlenc#sha256
Transforms	Enveloped Signature	http://www.w3.org/2000/09/xmldsig#enveloped-signature
Certificate	X.509	http://www.ietf.org/rfc/rfc5280.txt

Public Alerting Space (IPAWS Domain)

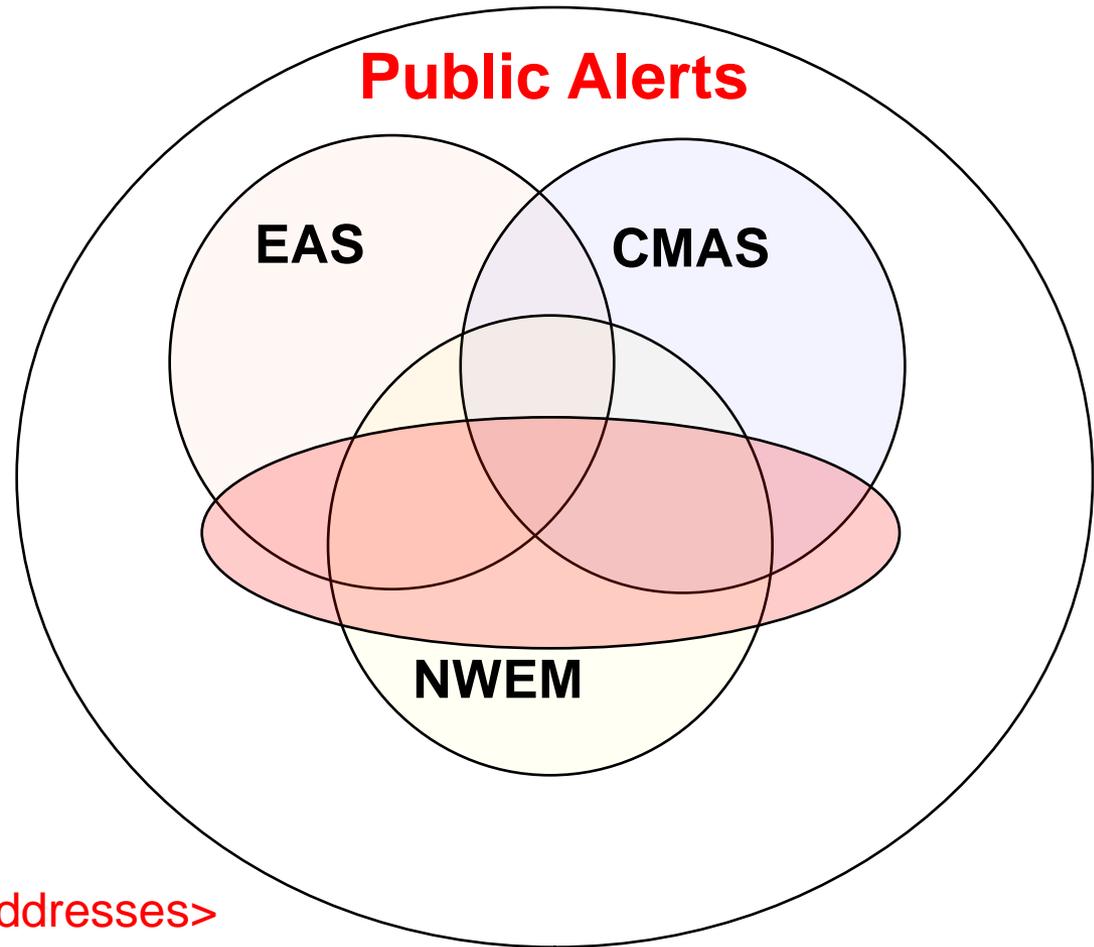
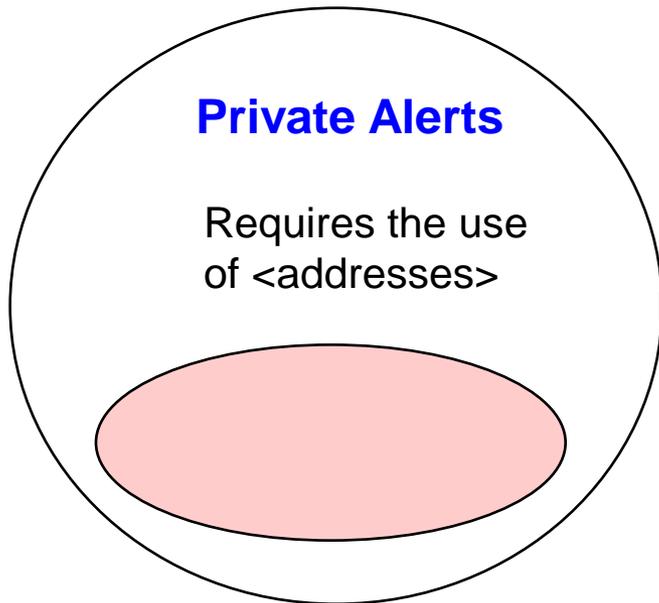


FEMA

Public and Private Alerting Space (IPAWS Domain)



Directed Alerting (IPAWS COG ID in <addresses>)



COG Directed Alerts

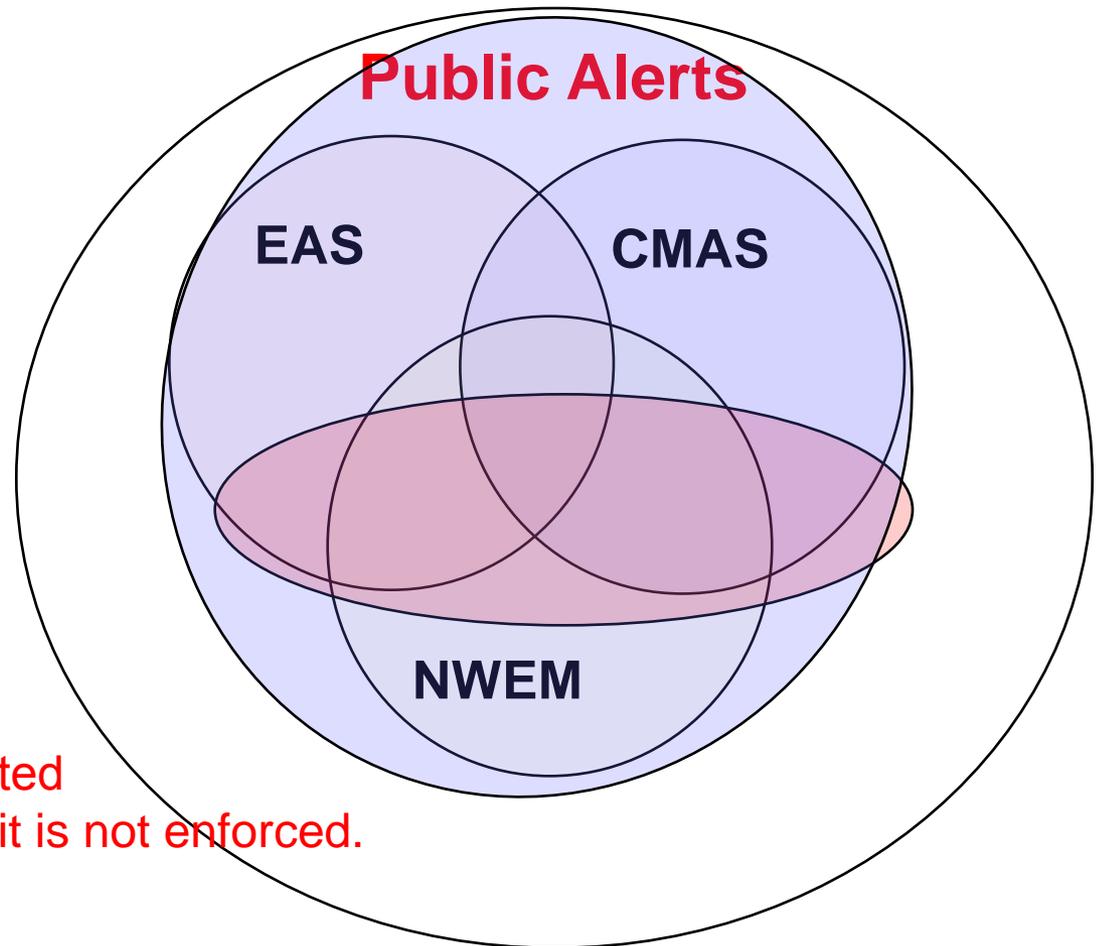
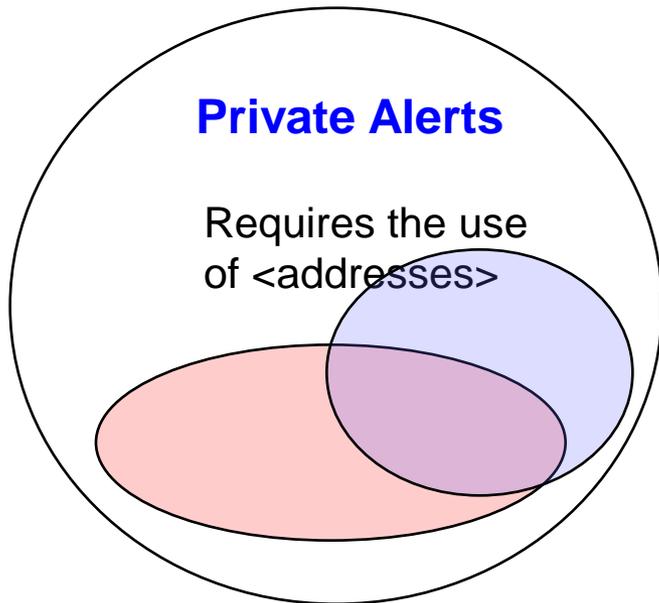
Example:

<addresses>999 100014 0</addresses>



FEMA

Digitally Signed Alerts



1. All IPAWS “push disseminated
2. Others may be signed, but it is not enforced.

Private Use Cases

<scope>Private</scope>

- ▶ **Pri 1 – Alert Within a Single Organization**
 - **<addresses>mycogID</addresses>**
- ▶ **Pri 2 - Alert to Other Known EM and Responder Organizations**
 - **<addresses>myCogID partnerCogID partnerCogID ... </addresses>**
- ▶ **Pri 3 - Alert of General Interest to All Emergency Managers, but not Appropriate for Distribution to the General Public**
 - **<addresses>0</addresses>**

Public Use Cases without IPAWS Push Dissemination

<scope>Public</scope>

- ▶ **Pub 1 – Alert Within a Single Organization – but may be sent by receivers to anyone**
 - **<addresses>mycogID</addresses>**
- ▶ **Pub 2 - Alert to Other Known EM and Responder Organizations – but without restriction on public redissemination**
 - **<addresses>myCogID partnerCogID partnerCogID ... </addresses>**
- ▶ **Pub 3 - Alert of General Interest to All Emergency Managers – left to the receiving Emergency manager whether to pass along or not.**
 - **<addresses>0</addresses>**

Public Use Cases with IPAWS Push Dissemination

<code>IPAWSv1.0</code>

<scope>Public</scope>

Digitally signed

- ▶ **IPAWS 1 – Alert Within a Single Organization – but will be sent to EAS CMAS, or NWEM locally, based on content and permissions.**
 - **<addresses>mycogID</addresses>**
- ▶ **IPAWS 2 - Alert to Other Known EM and Responder Organizations – but will be sent to EAS, CMAS, or NWEM to all public, based on content and permissions.**
 - **<addresses>myCogID partnerCogID partnerCogID ... </addresses>**
- ▶ **IPAWS 3 - Alert of General Interest to All Emergency Managers – and will be sent to EAS, CMAS, or NWEM to all public, based on content and permissions.**
 - **<addresses>0</addresses>**



CAP 1.2 Sharing Mode Summary

CAP 1.2 Options	Private	Public	Public Plus IPAWS Push
Internal	Own COG members only	Own COG members with redistribution allowed	Own COG with IPAWS Channels added depending on permissions
Exchange Partners	Exchange partners Only	Exchange Partners with redistribution allowed	Exchange Partners with IPAWS Channels added depending on permissions
All	All COGs	All COGs with redistribution allowed	All COGs with IPAWS Channels added depending on permissions



IPAWS Alerting Channels for Originators

CAP 1.2 Options	Permissions needed	Capability
COG-to-COG	Needs only an Operational COG.	Cap 1.2 post and retrieval using the IPAWS-OPEN SOAP Interface.
EAS	Added designation of COG as Public Alerting Authority	Authority to post applicable CAP messages for EAS Broadcast. (May be limited by Event Code and Geography.)
CMAS	Added designation of COG as Public Alerting Authority	Authority to post applicable CAP messages for Cellular Mobile Broadcast. (May be limited by Event Code and Geography.)
NWEM	Separately authorized by NOAA.	Authority to post applicable non weather related CAP messages for broadcast on NOAA Radio. Limited by NOAA designated Event Code and Geography.
Public Feed	TBD – Public Alerting Authority?	TBD – An internet feed of all Signed Public alerts???

Comments and Questions

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

Mark.Lucero@dhs.gov

Office (202) 646-1386

Chief, IPAWS Engineering, National Continuity Programs, DHS FEMA

Gary.Ham@associates.dhs.gov

Office: (703) 899-6241

Contractor, Systems Architect, IPAWS-OPEN

