



Integrated Public Alert and Warning System IPAWS

Get Alerts, Stay Alive

Practitioner Webinar
Improving State & Local Warnings



6 March, 2013

Audio Instructions

Thank you for joining us for this webinar. When you joined the online conference you should have been prompted to join the audio conference.

If you did not receive call in information or a call back through the instructions provided, please click on “Communicate,” “Teleconference,” “Join Teleconference,” and then follow the instructions provided.

If you have questions during the presentations, please use the chat function on the right hand panel of the WebEx screen and the IPAWS PMO will try to answer them throughout the presentation.

At the end of the presentation, if time permits, the presenters will take questions. You can use the “raise your hand” function in WebEx at the end of the presentation or you can chat your questions in.



FEMA

Introduction

Manny Centeno

EAS Test Program Manager, FEMA IPAWS

Manny Centeno began serving as a Program Manager at FEMA's Integrated Public Alert and Warning System in June of 2010. During his tenure at FEMA he led the first ever Nationwide Emergency Alert System (EAS) Test as well as the many test events and exercises leading up to it. Mr. Centeno is a frequently requested speaker with over 20 years of experience in broadcast and emergency communications as well as extensive technical experience directly working on public alert and warning systems.

Roundtable Participants

Alisia La May

Nebraska Emergency Management Agency

Jim Skinner

Nebraska's State Emergency Communications Committee (SECC)

Adrienne Abbott

Nevada's State Emergency Communications Committee (SECC)



FEMA

Security Best Practices for Originators & Disseminators

FCC's Urgent Advisory requiring immediate actions to be taken regarding CAP EAS device security:

- All EAS Participants are required to take immediate action to secure their CAP EAS equipment, including resetting passwords, and ensuring CAP EAS equipment is secured behind properly configured firewalls and other defensive measures.
- All CAP EAS equipment manufacturer models are included in this advisory.
- All Broadcast and Cable EAS Participants are urged to take the following actions immediately.
- EAS Participants must change all passwords on their CAP EAS equipment from default factory settings, including administrator and user accounts.
- EAS Participants are also urged to ensure that their firewalls and other solutions are properly configured and up-to-date.
- EAS Participants are further advised to examine their CAP EAS equipment to ensure that no unauthorized alerts or messages have been set (queued) for future transmission.
- If you are unable to reset the default passwords on your equipment, you may consider disconnecting your device's Ethernet connection until those settings have been updated.
- EAS Participants that have questions about securing their equipment should consult their equipment manufacturer.

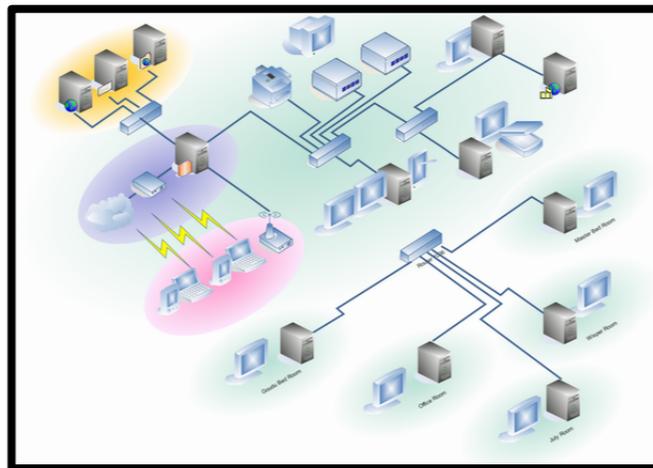


FEMA

Security Best Practices for Originators & Disseminators

- ❑ See the FCC's "Urgent Advisory Regarding Unauthorized EAS Hacks" released on February 13, 2013
- ❑ If you don't understand the terminology or concepts mentioned in these and other suggestions and best-practices, seek training or get someone that does
- ❑ Map your network to better understand how it is structured, physically and logically. Search for and identify weak links in your network, including EAS devices
- ❑ Many radio, television and cable facilities share their IT infrastructure with business operations, news and marketing. In some cases, websites and streaming services are hosted within this shared IT infrastructure

KNOW YOUR NETWORK!



FEMA

Security Best Practices for Originators & Disseminators

- ❑ Conduct a Network Vulnerability Assessment across your network. VA tools are available online and some are free or open source. These tools can help identify "open doors" which hackers may use to compromise your network
- ❑ VA tools can help identify weak links in your network that, including other devices such as servers, workstations, routers, VOIP servers, etc
- ❑ Patch your network devices, as necessary

The image displays two screenshots of security assessment tools. The left screenshot shows the Shadow Security Scanner interface, which includes a table of assets and a detailed view of a specific asset's business information.

Asset Group	IPs	Business / CVSS Info	Risk Level	Manager	Last Scan
Corporate Headquarters	192.168.1.1-192.168.1.254, 216.27.161.91		High	IT Security Manager	07/31/2006
Extranet	64.41.134.59-64.41.134.61		High	IT Security Manager	05/23/2006
FW-VPN	64.41.134.60		High	IT Security Manager	09/14/2007
Financial Systems	64.41.134.59, 64.41.134.61		Critical	IT Security Manager	12/12/2005
Firewall	216.27.161.91		High	IT Security Manager	12/12/2005
HR Systems			Critical	IT Security Manager	05/23/2006
Linux Servers					
London Map					
London S...					

The right screenshot shows the SecPoint Penetrator interface, which is a web-based tool for conducting network audits and penetration tests. It features a "Start Audit - Step 1 of 3" wizard and a sidebar with "Audit Statistics" and "Penetrator Information".

Security Best Practices for Originators & Disseminators

- Establish and understand your perimeter defense. What devices on your network "break" this defense?
 - a. Search for applications that extend through your firewall policies (exceptions)
 - b. Identify all IP-enabled devices internal to the network
 - c. Understand if mobile devices are allowed to connect to your network
 - d. Search for wireless access points that are unknowingly deployed
 - e. Identify all direct Internet access to and from other devices
- Use strong passwords on ALL your Internet facing devices. Do not use "dictionary" words for passwords
- Refresh passwords frequently
- Discuss your IT security defenses, risks and vulnerabilities with management



FEMA

Security Best Practices for Originators & Disseminators

- Disable any unused network access tools or features. For example, if you don't need to access your CAP device via the Internet, shut down the feature; if you are not a public warning originator, disable any features that allow for remote creation of warnings
- Close any telnet or command prompt services accessible via the web. Consult your manufacturer to know if any "hidden" services or "back doors" need to be patched
- If practical, isolate your CAP device from other services in your network by creating DMZs and strong firewall protection
- Ask your manufacturers which ports and services are needed for proper operation of your CAP device
- Verify that other devices on the same network are not vulnerable to intrusion
- Although this takes time, look at your network logs regularly to find any obvious intrusion attempts.
- Know your staff... Establish an appropriate credentialing process



FEMA

Security Best Practices for Originators & Disseminators

- ❑ Keeping your network secure is an on-going commitment. Be ready to defend and respond to new methods and tricks used by hackers

- ❑ Learn more about cyber security:
 - <http://www.cisecurity.org/resources-publications/>
 - <http://www.us-cert.gov/>
 - <http://msisac.cisecurity.org/resources/guides/documents/Firewall%20Guide.pdf>
 - <http://msisac.cisecurity.org/resources/guides/documents/GettingStartedGuide020808.pdf>
 - <http://www.sans.org/critical-security-controls/cag4.pdf>
 - <http://msisac.cisecurity.org/resources/state-cyber-policies.cfm>



FEMA

Public Alert and Warning Essentials

- ❑ The ability to warn the public of imminent danger has been a priority for civilizations throughout the world for thousands of years
- ❑ Years ago, ancient man would use available tools to alert and warn their groups and villages. These tools included town criers, horns, conch shells, wood sticks, smoke, bells and other devices
- ❑ As is now, in old times an effective warning required various steps to work well together. The alert and warning originator needed to have a basic process and infrastructure:
 - a. that effectively receives and shares information; and understands the emergency as it evolves
 - b. that includes a decision making process and authority to alert and warn
 - c. that provides a method or device to convey the alert and message
 - d. that provides adequate security to prevent unauthorized access or denial of service
 - e. that provides for practice and testing

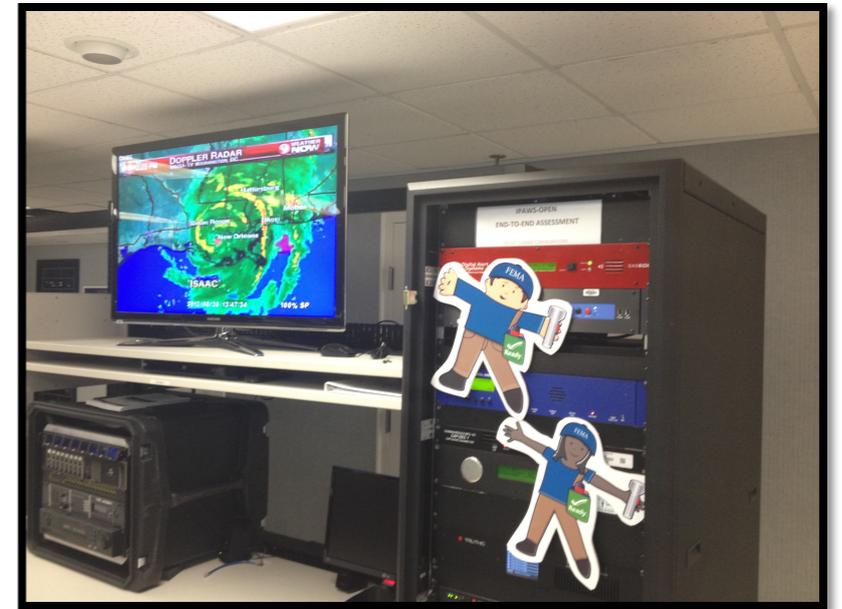


FEMA

Public Alert and Warning Essentials

To plan for a public warning program, an authority should consider the following:

1. Identify your jurisdiction's hazards to document needs and requirements
2. Identify who is authorized to originate and manage alerts
3. Identify and engage with warning partners to seek their advice and council
4. Develop clear and repeatable warning policies, guidelines, procedures, training, test and exercise plans
5. Review and frequently update public warning plans and policies in close coordination with all warning partners
6. Educate the public on the importance of being informed and the use of warning sources
7. Test and Exercise Frequently



Public A&W Essentials – Identifying Hazards

Conduct a Hazards and Vulnerability Assessment: What is the area vulnerable to?

- Understand areas that may overlap or share boundaries with other jurisdictions.
- Understand areas where your agency may be alerting citizens in another jurisdiction. For example, another State may have small towns that are close to your State's borders. These areas may not be able to support their own public warning systems, and the their State government system may be to distant to be effective there. Seek agreements with adjacent State or counties.
- Identify areas where your State may be alerting citizens of another country. Seek agreements with neighboring country with support from U.S. State Department.
- Identify Man-Made Vulnerabilities: Chemical Plants, Nuclear Plants, Fuel Depots, Trans-shipment Facilities, Cyber Attacks, Drinking Water Contamination, Shootings, Terrorist Attacks, etc.
- Identify Natural Hazards: Blizzards, Biological Threats, Severe Wind Storms, Floods, Earthquakes, Animal/Plant Diseases, Wildlife Fires, etc.



FEMA

Public A&W Essentials – Identifying Hazards

- ❑ Additionally, identify your agency's physical vulnerabilities and provide resiliency or backup facilities and components to warn the public if the main site suffers damage or destruction.
- ❑ Identify any personnel shortfalls and plan accordingly
- ❑ The Hazards and Vulnerability Assessment will assist in the development of a Public Warning Plan that:
 - a. Identifies the alert and warning codes for CAP and EAS
 - b. Provides officials with information and education to develop effective warning messages
 - c. Includes industries that may pose accidental risks to the public
 - d. Provides officials with information to educate the public for desired response
 - e. Engages and Invites all in the emergency management and emergency response community to provide input for the Vulnerability Assessment and Public Warning Plan
 - f. Provides continuity of operations in emergencies

Public A&W Essentials – Who Originates?

Identify who is authorized to originate and manage alerts (Emergency Manager, Watch Officer, Public Information Officer, etc.). How is this determined?

- ❑ Authority – Who in the organization has been granted the authority to originate public warnings? This is determined by the emergency management agency or other agency or organization as determined by the State or local government
- ❑ Trust – Public Warnings depend on and leverage the telecommunications capabilities of private-sector participants. These partners contribute willingly when their capabilities are used responsibly and effectively.
- ❑ Availability – Public Warning originators must be available at any time of day or night, everyday. Emergencies affecting the public do not occur on a schedule. Many jurisdictions use properly trained watch officers to originate public warnings. In agencies where budget does not support 24/7 personnel, web and telephone technology allows for public warning origination capabilities.
- ❑ Understanding and Training – All public warning originators must understand the incident, be trained to select the appropriate alert event codes, geo-codes, and know how to draft the right language for the warning.



FEMA

Public A&W Essentials – Public Warning Partners

Public warning programs depend on and leverage the telecommunications capabilities of private-sector participants. Other agencies and partners, such as State Police, Justice (child-abduction), military installations, chemical and nuclear plants, may also need to use these capabilities. These partners contribute willingly when their knowledge and capabilities and are happy to participate responsibly and effectively. It is important to create and maintain a Governance Structure in order to secure the permanence of effective public warning through the years.

Establish strong working relationships with the following sectors:

- ❑ Broadcast Radio, Television and Cable Providers – Most jurisdictions have already established State Emergency Communications Committees (SECCs) and Local Emergency Communications Committees (LECCs) that include these sectors.
- ❑ Cellular Service Providers – Prior to IPAWS, radio, television and cable EAS Participants would represent the private sector. Now, with the distribution of cellular alerts as part of CMAS/WEA, it is important to include cellular representatives.
- ❑ Other State, County and City Governments – These sectors should be included to provide advice and to provide planning and operational coordination of the public warning system in the area or region.

Public A&W Essentials – Policy, Guidelines, Procedures...

- ❑ Clear and concise policies, plans, procedures, and guidelines support an effective and continual public warning program at the State and local levels.
- ❑ All governments have an OBLIGATION to protect their citizens.

“Individuals, businesses, communities, organizations and governmental agencies that create, generate or hold information that can reduce risk have a fundamental moral duty to warn of impending danger.” – Partnership for Public Warning (PPW)

- ❑ Public warning policy principles can be taken from several documents:
 - Presidential Executive Order 13407
 - PPW’s A “National Strategy For Integrated Public Warning Policy and Capability”
 - PPW’s “Protecting America’s Communities – An Introduction to Public Alert and Warning”
 - IPAWS Training - IS-247.a
 - IPAWS EAS Best Practices Guide

Public A&W Essentials – Policy, Guidelines, Procedures...

- Before drafting new policy, understand alert and warning technology, nomenclature, and rules – seek support from jurisdictions that who have effective, well-exercised plans.
- Seek funding for initial deployment and sustainment.
- Communicate roles, instructions and expectations clearly.
- Create training and re-training programs for new staff and as a way to periodically “recertify” current staff.
- Develop security and accountability guidelines.
- Develop joint training opportunities with EAS, WEA, and other public warning participants.



FEMA

Public A&W Essentials – Regularly Update Policies, Guidelines, Procedures...

- ❑ Policies, guidelines, best-practices, procedures and other documentation need to be reviewed and refreshed regularly. This is necessary due to changing condition and needs, and technological advances.
- ❑ A solid stakeholder partnership and understanding of those stakeholder roles.
- ❑ An understanding of technology, and that technology requires funding.
- ❑ An understanding that no single method or technology will meet all needs.
- ❑ An understanding that no system will ever be perfect. Continual evolution and improvement is necessary in order to achieve incremental success.
- ❑ An expectation that due to the political process, leadership priorities will change. However, with strong policies, guidelines and procedures, sustainment of an enduring public warning framework is achievable.
- ❑ An understanding that regular practice and exercise supports improvement.
- ❑ An understanding that the public needs to be continually reminded that being informed is important for their safety.



FEMA

Public A&W Essentials – Educating the Public

Public education is essential in order to achieve a successful warning program...

- Being informed is a shared responsibility
- Include information on public warning systems when providing preparedness advice to the public
- Educate the public on where to seek and validate information
- Inform the public that it is unsafe to “disconnect” from information sources, especially when living or transiting through disaster prone areas
- Exercise and test public warning systems and remind the public of its importance
- Provide the public with a method for providing feedback
- Engage mass media partners to assist with informing and educating the public
- Include public warning when conducting public disaster drills and exercises

Please submit questions, ideas, and comments to:

IPAWS Website

<http://www.fema.gov/emergency/ipaws>

IPAWS Group Mailbox

IPAWS@dhs.gov

Manny Centeno

Manuel.Centeno1@dhs.gov

Program Manager, IPAWS

National Continuity Programs, DHS FEMA

Alisia LaMay

alisia.lamay@nebraska.gov

Nebraska Emergency Management Agency

Jim Skinner

Jskinner@kxvo.com

Nebraska EAS SECC

Adrienne Abbott

nevadaeas@charter.net

Nevada SECC

Caitlyn Stephenson

Caitlyn.Stephenson@associates.fema.dhs.gov

IPAWS