SCTE · ISBE

STANDARDS

Network Operations Subcommittee

SCTE OPERATIONAL PRACTICE

SCTE 179 2020

Recommended Practice

Upgrading EAS to CAP Compliance

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

TABLE OF CONTENTS

1.0 SCOPE

This document is identical to SCTE 179 2012 except for informative components which may have been updated such as the title page, NOTICE text, headers and footers. No normative changes have been made to this document.

The 2012 release of this standard mentions a deadline that is now past. This 2020 release of the standard maintains mention of this past date for historical reference.

This document is intended to provide general background information concerning Cable operators' adoption of the Common Alerting Protocol (CAP) and a generic technical and operational checklist to assist in preparing for the carriage of CAP messages.

Cable operators are encouraged to develop a technical checklist for each Emergency Alert System (EAS) Decoder location. The enclosed checklist represents an outline of the key issues that need to be identified and addressed. The checklist should be expanded to include any system or MSO specific issues. This tool will help ensure that the necessary tasks are completed before June 30, 2012 .[1]

2.0 INTRODUCTION

Since 1999, all Multi-channel Video Program Distributors (MVPDs), including cable operators, have been required to participate in the Federal Communication Commission's (FCC) Emergency Alert System. EAS was created to give the US President the ability to quickly communicate with the country in the event of a national emergency. More commonly, the system is put to use for state and local emergency events including weather related, hazardous spills, AMBER[2] alerts, etc.

On September 30, 2010, the Federal Emergency Management Administration (FEMA) announced its adoption of the CAP standard for EAS.[3] This announcement triggered the FCC requirement that all EAS participants be able to support CAP within 180 days.[4] Since that time, an extension was granted to one year.[5] The FCC and FEMA have now established June 30, 2012 as the date when all EAS participants are required to support the CAP standard.

---

[1] June 30, 2012 is the deadline established by the Federal Communications Commission (FCC)

[2] AMBER alerts -- The AMBER Alert™ Program is a voluntary partnership between law-enforcement agencies, broadcasters, transportation agencies, and the wireless industry, to activate an urgent bulletin in the most serious child-abduction cases. http://www.amberalert.gov/

[3] FEMA Announces Adoption Of New Standard For Emergency Alerts, Common Alerting Protocol Key in Developing America's Next Emergency Alert and Warning Network, Release Date: September 30, 2010, Release Number: HQ-10-192 http://www.fema.gov/news/newsrelease.fema?id=52880

[4] 47 CFR 11.56 EAS Participants receive CAP-formatted alerts, Nov. 2, 2007

[5] EB Docket No. 04-29, Released November 23, 2010

By that date all EAS participants must have purchased and installed FEMA *Integrated Public Alerting and Warning System (IPAWS)* conformance hardware and software verified by manufacturers' Supplier's Declaration of Conformity (SDOC) notice to be able to attach to the IPAWS server and process CAP messages[6].

3.0 ACTIONS

The CAP upgrade project can be broken down into eight key tasks.

1. Develop an inventory of all EAS equipment presently installed.
2. Determine State and Local requirements.
3. Evaluate existing EAS network connectivity and decoder placement.
4. Determine which EAS equipment is upgradeable and which is not.
5. Upgrade or replace legacy EAS equipment, as necessary.
6. Install and test of upgrades and/or new EAS equipment.
7. Test Components and Systems.
8. Monitor updates in CAP requirements and accommodate changes.

Each step is detailed below:

1. Develop an inventory. Create a spreadsheet listing details of equipment for each EAS decoder. The Appendix "CAP Upgrade Checklist" may serve as a template. Include make and model of EAS equipment, software version, LP1 and LP2 monitoring assignments, and note the availability of Internet access at the location where the equipment is located. This step should be performed for each EAS decoder location. Set-tops supported at each site should be noted. The interface between the EAS equipment and each set-top control system is unique and may require consideration. The EAS vendor must be aware of deployed set top box types and/or EAS-compatible consumer premises equipment (CPE) in order to determine how they can be supported.

---

[6] As referenced in a report by the FCC's Communications Security, Reliability and Interoperability Council (http://www.fcc.gov/pshs/docs/advisory/csric/WG_5A-CAP_Introduction_Final_Report_Readout.ppt and http://transition.fcc.gov/pshs/docs/csric/CSRIC%205A%20Working%20Group.pdf)

2. Determine State and Local requirements. Review the State Emergency Communications Committee (SECC) plans for any unique or CAP specific requirements that need to be accommodated.

In addition, each SECC should designate a 'Cable Co-chair'. Contact this individual and determine any unique state or local requirements that may apply. Verify the monitoring assignments. Coordinate next generation EAS activities with the SECC and Local Emergency Communication Committees (LECCs) as appropriate.

> *Note: As of publication date no states have approved up-to-date CAP-compliant state plans, and a few states still have no approved state plans in place. However, up to 20 states have already deployed some form of CAP or IP-based EAS relay system.*

3. Evaluate existing EAS network connectivity and decoder placement. . It is anticipated that CAP messages will be made available using Internet Protocol (IP) via an Internet connection. More specifically, the IPAWS aggregator (server) will publish CAP messages on a FEMA CAP/IPAWS feed.[7] If appropriate connectivity is not available to the decoder, modifications to either the connectivity or decoder placement may be necessary.

> *Note: State CAP alerting architectures are more diverse, including Internet, satellite and/or wireless distribution of CAP XML data and audio files. Some networks utilize "push" technologies, while others relay on passive "polling" methods. Operators will need to carefully evaluate the CAP data systems in place or under development in each of the states in which they operate regarding: (1) how does their CAP EAS equipment support data interoperability with each respective state or local CAP source, and (2) what additional hardware/software – if any – may be required to physically interface with these state/local networks.*

4. Determine EAS Equipment Upgradeability. Some legacy EAS equipment may not be upgradeable. Check with manufacturers to determine which equipment on the inventory list can be upgraded and which must be replaced. FEMA is responsible for testing and certifying manufacturers' CAP equipment and will publish periodically updated lists of conforming equipment. Review this list to verify that the equipment or upgrade being purchased is on the FEMA approved list.[8]

There are generally two methods used by CAP EAS products for handling CAP messaging. One method is using a separate CAP-to-EAS protocol translating device, functioning in tandem with an existing EAS encoder/decoder. The second is an integrated CAP capability, using an

---

[7] As of date of publication, FEMA is using ATOM RSS. Several methods have been used and implementers should confirm the current publishing protocol.

[8] See https://www.rkb.us/

integrated CAP processor and EAS encoder/decoder. This second approach is available in both an integrated single unit package and as well as in a multi-device configuration.

When choosing your CAP compliance solution, either a CAP to EAS protocol converter or a CAP processing EAS device, select a system that has passed FEMA IPAWS conformance testing. A non-conforming product might not support all of the requirements for compliance to FCC Part 11 (EAS), including any future requirements for "Gubernatorial Must-Carry".

The selection process for CAP compliance solutions should incorporate a number of fundamental questions:

Does the solution meet FCC Part 11 requirements for EAS equipment?	*Part 11 covers both the encoding and decoding of EAS protocol messages including allowing intermediary devices.*
Does the specific piece of equipment hold (1) an IPAWS Conformity Assessment Test Report and (2) a Suppliers Declaration of Conformity?	*IPAWS Conformity test results relate to specific product designation, model number and version/sub-version numbers. Anything other than the specific product referenced in the test results may be deemed ineligible to connect with the IPAWS aggregator).*
Does the solution readily support potential state and local sources of CAP messaging?	*(As of date of publication,, there are no known requirements to monitor state and local CAP alert resources. Some jurisdictions require monitoring state EAS.*
Does the solution support carriage of the additional detail provided in CAP messaging?	*If providing the additional detail to your subscribers is important, an intermediary device may not support this requirement.*

Table 1 – Selection Process

5. Upgrade and Replacement plans. Based on the requirements identified above, work with EAS manufacturers to determine whether EAS upgrades or replacement equipment is most appropriate to facilitate CAP support. Ensure that the EAS manufacturer is aware of any network changes that may be required to facilitate reception of CAP messages. Also, determine if the EAS manufacturer has an upgrade path to facilitate state and local requirements once

adopted by the FCC and FEMA. Note that in some cases EAS equipment may be obsolete or not upgradable, thereby requiring replacement.

Create the bill of materials, determine the budget, prepare purchase orders and procure the necessary equipment or upgrades.

6. Install and Test. Following the manufacturer's recommendations and instructions, install the new equipment and upgrade the existing equipment and/or software, bringing the individual components and the EAS system into CAP compliance. DO NOT DISABLE THE CURRENT EAS SYSTEM, as it will continue to be used to deliver emergency alerts, whether received via the current EAS distribution network or via the to-be-determined CAP delivery methodology. At the completion of this exercise EAS locations should be back to operational status and CAP compliant.

7. Test Components and Systems. Since CAP upgrades are being applied to the existing EAS platform it is possible that existing EAS functionality is affected by modifications to the current EAS hardware, software, network, or delivery platforms. Monitor the EAS platform during subsequent alerts, such as weekly and monthly tests, to ensure that the EAS network is functioning as required. Engage with engineering or EAS manufacturers as appropriate to troubleshoot, diagnose and repair EAS or CAP equipment as required. As of August 25, 2011, the delivery methodology for CAP-compliant messages is not yet defined. As such, CAP compliance testing will be limited to EAS manufacturer provided CAP test procedures.

8. Monitor updates in CAP requirements and accommodate changes. Monitor developments at the FCC and FEMA related to updates and changes in CAP requirements, especially as it relates to the methodology adopted to deliver CAP messages. Work with your EAS manufacturer to develop and execute test plans that ensure end-to-end delivery of emergency alert messages from CAP reception to EAS distribution.

As mentioned above, as of publication date most states do not have defined CAP plans approved. As state plans become available, review them to determine the CAP input and distribution requirements. Develop a plan to adapt the recently upgraded or replaced EAS equipment to accommodate those state and local plans. Review the State Emergency Communications Committee (SECC) plans for any unique requirements that need to be accommodated.[9] Coordinate with the SECC (and LECC (Local Emergency Communication Committee), if any) as appropriate.

> *Note: The deadline for implementing CAP is June 30, 2012. Develop an expedited timeline that ensures all tasks above can be facilitated in the time allotted, especially as it relates to gathering requirements as well as ordering, receiving, installing and testing the new components and the full EAS network.*

[9] The FCC and FEMA adopted CAP after a handful of states had already implemented their own version of CAP. The CAP implementation in your state may be different from the national version so special accommodations may be required.

4.0 ABBREVIATIONS AND ACRONYMS

ANSI – American National Standards Institute

ATOM – Atom Syndication Format

CAP – Common Alerting Protocol

EAS – Emergency Alert System

FCC – Federal Communications Commission

FEMA – Federal Emergency Management Administration

FIPS – Federal Information Processing Standard

IPAWS – Integrated Public Alerting and Warning System

LECC – Local Emergency Communications Committee

LP – Local Primary

MVPD – Multi-channel Video Program Distributor

NWS – National Weather Service

OPEN – Open Platform for Emergency Messaging

SDOC – Suppliers' Declaration of Conformity

SECC – State Emergency Communications Committee

SOAP – Simple Object Access Protocol

XML – Extensible Markup Language

5.0 CAP UPGRADE CHECKLIST

Fill out for each EAS Decoder:

Location _____

EAS Vendor _____

Web site _____

Vendor Rep (name)_____

Phone _____

Email address _____

Model _____

Software version _____

Is this version the most up to date for the applications? Y/N ___

CPE supported devices (set top box or other receivers) _____

Set-Top Box controller Software version _____

Is this version the most up to date for the applications? Y/N ____

Other EAS processing equipment:

QAM Devices_____

Edge Devices (e.g., decoders, D/A) _____

Multiplexers _____

Is SCTE 18 (ANSI J-STD 042) in use? Y/N ____

Local franchise override requirement? Y/N ____

Stations monitored (Call letters and frequencies):

LP1 _____ per state plan Y/N ____

LP2 _____ per state plan Y/N ____

NWS _____ per state plan Y/N ____

Other _____ per state plan Y/N ____

Input Source for CAP signal _____

Counties / FIPS codes covered:

_____

_____

_____

Event codes programmed for response:

EAN, EAT, RMT _____

EAN Detailed Channel location: (SCTE 18 entry)_____

Steps required to upgrade EAS system:

_____

_____

_____

Special requirements for this site:

MSO Specific requirements:

_____

_____

_____

Is internet connectivity available at this site? Y/N ___

Attach -- Bill of Materials

Date Ordered _____

Purchase Order(s) number(s) (attach) _____

Date Received _____

Date installed and configured _____

Date Tested: _____

Provisioning for CAP source _____

Date tested _____

Verify that EAS protocol still functions ____

Verify reception of test signal from CAP source ____

Continue logging EAS messages and begin logging CAP messages received and transmitted.

6.0 BIBLIOGRAPHY

(Not intended to be an all-inclusive list)

47 CFR Part 11 http://ecfr.gpoaccess.gov/cgi/t/text/text-dx?c=ecfr&tpl=/ecfrbrowse/Title47/47cfr11_main_02.tpl

CAP EAS Implementation Guide, EAS CAP Industry Group - ECIG

EAS-CAP Implementation Guide Subcommittee Version 1.0, 17 May 2010: http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

CAP cookbook http://www.incident.com/cookbook/index.php/Welcome_to_the_CAP_Cookbook

http://www.incident.com/cookbook/index.php/Welcome_to_the_CAP_Cookbook*Detailed technical specifications for CAP* http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf.

EASALERT Broadcasters' Forum http://www.easalert.org/

EAS Approved Vendors http://www.fcc.gov/pshs/services/eas/vendors.html

EAS CAP Industry Group http://eas-cap.org/

EAS State plan database http://www.fema.gov/about/programs/disastermanagement/haz/eas.shtm

Federal Communications Commission http://www.fcc.gov

FEMA IPAWS Home page http://www.fema.gov/emergency/ipaws/

FEMA Responder Knowledge Base https://www.rkb.us/

Monroe Electronics http://www.monroe-electronics.com/EAS_pages/eas_cap.htm

Meeting report by Gary Timm http://www.awareforum.org/

National Association of Broadcasters http://www.nab.org

National Cable and Telecommunications Association http://www.ncta.com

National Cable Television Cooperative http://www.nctconline.org

Slides from the FEMA webinars http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=4659

Society of Broadcast Engineers http://www.sbe.org

Society of Broadcast Engineers webinar http://www.sbe.org/WebinarsbySBE-TheNewEAS.php

Society of Cable Telecommunications Engineers http://www.scte.org

Trilithic http://www.trilithic.com/Emergency%20Alert%20Systems

7.0 FAQ

Is it better to buy a new EAS, upgrade my current system, or buy or a CAP converter?

A converter is not necessarily a better option. Upgrading currently installed equipment may provide more features. A CAP to EAS protocol converter can drop all of the additional data that CAP supports and EAS does not. This may be particularly important for an AMBER alert. Also, it is uncertain how a translation will show a message from a governor as being mandatory.

Older EAS equipment may not be upgradeable. Some manufacturers who produced EAS equipment are no longer in business. In these cases, a new system may be the best alternative.

Where will the CAP messages come from?

CAP messages will be delivered over a yet to be determined data path. Indications are that the Internet may be a source. This is an unresolved issue that FEMA and state plans will need to address.

Anticipation is that transmission from FEMA to EAS participants will be via the existing IPAWS (Integrated Public Alert and Warning System)[10] SOAP interface using the IPAWS-OPEN (Open Platform for Emergency Networks)[11] as an aggregator.

What about messages from the Governor?

FCC Part 11 rules require EAS participants to pass all CAP alerts originated by state governors, or their designee.

What hasn't been determined?

What will participants do when they receive CAP messages?

- What sources do I monitor for CAP messages?
- If the CAP messages are sent using the public Internet, what about remote headends with no Internet availability?
- What happens if an emergency brings down my internet access?
- What security measures will be used so that hackers won't be able to take control of emergency networks?
- How will governors send their messages to participants?
- How will state plans be changed?

---

[10] http://www.fema.gov/emergency/ipaws/

[11] http://www.fema.gov/emergency/ipaws/projects.shtm#6