

SCTE • ISBE[®]

S T A N D A R D S

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>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2020
140 Philips Road
Exton, PA 19341

TABLE OF CONTENTS

1.0	SCOPE	4
2.0	INTRODUCTION	4
3.0	ACTIONS	5
4.0	ABBREVIATIONS AND ACRONYMS	9
5.0	CAP UPGRADE CHECKLIST	10
6.0	BIBLIOGRAPHY	15
7.0	FAQ	16

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, AMBER² 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 messages⁶.

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>)