Integrated Public Alert and Warning System (IPAWS) Guide for Independent Testing of Emergency Alert System Equipment

June 2012

FEMA

Table of Contents

List of Figures

List of Tables

Introduction

This document provides an orientation to the Integrated Public Alert and Warning System (IPAWS) Conformity Assessment (CA) Program that was concluded August 2011. The CA Program was designed to assess vendor product adherence to, and the appropriate application of the Organization for the Advancement of Structured Information Standard (OASIS) Common Alerting Protocol (CAP) v1.2 Standard; OASIS CAP v. 1.2 USA Integrated Public Alert and Warning System (IPAWS) Profile Version 1.0; CAP EAS Implementation Guide Version 1.0[1]; and Federal Communications Commission (FCC) Title 47 of the Code of Federal Regulations (CFR) Part 11, herein referred to as the program requirements. This document describes the testing requirements for any Independent Testing Authority (ITA) who wishes to provide testing services for the manufacturers of Emergency Alert System decoder equipment for purposes of meeting FCC equipment certification requirements.

Initial IPAWS CA testing activities were managed by the Federal Emergency Management Agency (FEMA) IPAWS Program Management Office (PMO), herein referred to as PMO. FEMA IPAWS provides the Nation's next generation of alert and warning infrastructure, expanding upon the traditional audio-only radio and television Emergency Alert System (EAS). This allows the President and other authorized officials at the federal, state, local, and tribal levels to effectively provide alerts to local and state Emergency Operations Centers (EOCs) and the public by providing one message over multiple media before, during, and after a disaster.

On May 31, 2007, the FCC published the Second Report and Order that directs EAS participants to accept messages using CAP v1.1[2]. FCC Title 47 of the CFR Part 11 contains rules and regulations providing for EAS and methods to deliver alerts and

[1] IPAWS CA recognizes this Implementation Guide as per FEMA's memorandum of concurrence, http://www.eas-cap.org/.

[2] FEMA adopted the latest version of CAP, version 1.2, for use with IPAWS on September 30, 2010, http://www.fema.gov/news/newsrelease.fema?id=52880.

warnings. The program requirements are used by FEMA IPAWS to facilitate the rapid delivery of alert and warnings via analog and digital television, radio, digital cable television, Digital Audio Broadcast (DAB), telephone, cell phone, pagers, computers, Direct Broadcast Satellite (DBS), Satellite Digital Audio Radio System (SDARS), and other communications methods.

On March 22, 2012, the FCC published its Fifth Report and Order addressing EAS equipment certification, among other topics. (See http://www.gpo.gov/fdsys/pkg/FR-2012-03-22/pdf/2012-6601.pdf.) In paragraph 164, the FCC concluded:

> *We conclude that EAS equipment must be certified as CAP compliant because we are amending Part 11 to require CAP-to-SAME conversion in conformance with the ECIG Implementation Guide, and thus, as part of the required Part 11 functions, it necessarily falls under Part 11's certification requirements. While we agree with commenters that FEMA's IPAWS CA program has served as a useful mechanism for determining EAS device conformance with the ECIG Implementation Guide, this program cannot by itself serve as a substitute for the Commission's certification procedures. Accordingly, we will require that any EAS device that performs the functions of converting CAP-formatted messages into a SAME-compliant message, including integrated CAP-capable EAS devices and, as detailed below, intermediary devices, be certified under our Part 11 rules.*

The report describes the manner in which certification requirements may be satisfied:

165. ...any integrated CAP-capable EAS devices that have passed the conformance testing performed under FEMA's IPAWS CA program may use the Supplier's Declaration of Conformity (SDoC) issued under that program to demonstrate CAP-to-SAME conversion in conformance with the ECIG Implementation Guide.

166. Integrated CAP-capable EAS devices that have not already passed the conformance testing performed under FEMA's IPAWS CA program, and thus do not have an IPAWS CA program-authorized SDoC, must independently show conformance with the ECIG Implementation Guide to update their existing FCC certification or obtain FCC certification, as applicable. There are two methods for demonstrating such conformance. The SDoC issued under the NIMS CAP testing program *[now P-TAC STEP]* can be used to update an existing FCC certification or obtain a new FCC certification, as described above for SDoCs issued under the IPAWS CA program.

167. The second method for demonstrating compliance with the ECIG Implementation Guide involves the manufacturer arranging for testing and submitting a copy of the test report in lieu of the SDoC to complete the process discussed above. We again observe that the test procedures developed and utilized in FEMA's IPAWS CA program constitute the most logical basis for demonstrating compliance.

To support independent third party testing, FEMA has released this Program Guide to the public for use by accredited independent testing authorities in support of the option described in the paragraph above.

Testing will take place at the independent testing authorities' (ITA) designated facilities. In order for any ITA to conduct the testing described below, the ITA must execute a Memorandum of Agreement (MOA) with FEMA for the purpose of gaining secure access to the IPAWS Test and Development Laboratory (TDL). Accreditation to test for emergency response information technology must be issued by a nationally-recognized U.S. accreditation body. (See http://www.standardsportal.org/usa_en/resources/USaccreditation_bodies.aspx)

To achieve and maintain accreditation status, the laboratory must met general requirements for the competencies of testing and calibration laboratories, as provided in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025:2005. To begin the process of requesting an MOA, download the application from http://www.fema.gov/pdf/emergency/ipaws/moa_ipaws_open_app.pdf, complete, and return to IPAWS@dhs.gov.

Specifications

CAP is a "general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks"[3]. The CAP v. 1.2 USA IPAWS Profile Version 1.0, herein referred to as the Profile, "describes an interpretation of OASIS CAP v1.2 standard necessary to meet the needs of IPAWS"[4]. The CAP EAS Implementation Guide "is intended to further reduce the areas of uncertainty in how an alert will be presented to

[3] OASIS CAP v1.2 Standard, Abstract.

[4] OASIS CAP v. 1.2 USA IPAWS Profile Version 1.0, Abstract.

the public via CAP/EAS"[5]. These documents form a sequence in which each successive document clarifies, refines, and adds to the previous one.

Scope

The IPAWS CA Program was designed to ensure that vendors seeking to provide hardware or software solutions meet program requirements. These solutions were categorized into Message Originators, Message Managers, CAP-to-EAS Converters, EAS Encoder/Decoders, and Other Alerting Devices. **Figure 1** illustrates how the product categories generally fit within the CAP alert dissemination framework. The scope of this document is currently limited to CAP-to-EAS Converters and EAS Encoder/Decoders. Independent Testing Authorities will utilize the Test Cases and Objectives outlined in **Appendix A: Test Cases and Objectives** for testing product conformance to program requirements.

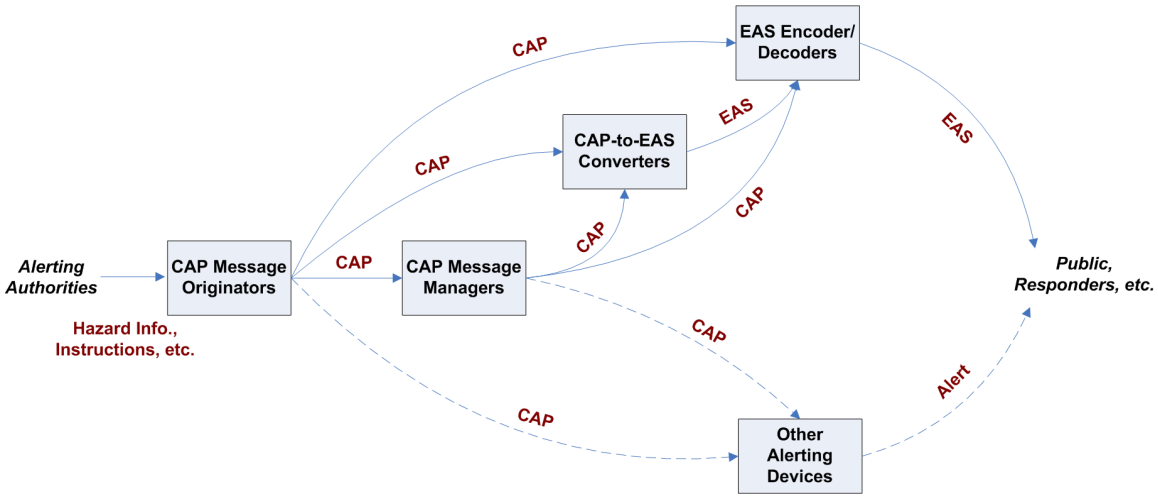

Figure 1: CAP Alert Dissemination

Program Description

The IPAWS CA Program provided an objective test of commercial and government software and hardware products (e.g., Encoder/Decoders) to assist in the implementation of IPAWS. Testing activities were designed to provide FEMA an objective process to

[5] CAP EAS Implementation Guide Version 1.0, Section 1.1.

verify conformance of software and hardware solutions, including EAS products as well as other alert and warning products that may not be bound by FCC Part 11 rules. The current FCC equipment certification requirements are limited to validating the following at 47 CFR 11.56 (a) (2):

> *Converting EAS alert messages that have been formatted pursuant to the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol Version 1.2 (July 1, 2010), and Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0 (Oct. 13, 2009), into EAS alert messages that comply with the EAS Protocol, such that the Preamble and EAS Header Codes, audio Attention Signal, audio message, and Preamble and EAS End of Message (EOM) Codes of such messages are rendered equivalent to the EAS Protocol (set forth in §11.31), in accordance with the technical specifications governing such conversion process set forth in the EAS–CAP Industry Group's (ECIG) Recommendations for a CAP EAS Implementation Guide, Version 1.0 (May 17, 2010) (except that any and all specifications set forth therein related to gubernatorial "must carry" shall not be followed, and that EAS Participants may adhere to the specifications related to text-to-speech on a voluntary basis).*

Benefits to Vendors

A test report may assist vendors in making future product improvements and/or meeting FCC equipment certification requirements. It also allows vendors to improve the marketing of their products for integration into other CAP-based alert and warning solutions at the community level.

Once the product has been determined to meet testing requirements, test reports and vendor's signed SDoC may be submitted to the Responder Knowledge Base (RKB) website for posting. The RKB is where state and local IPAWS users are directed to view a list of qualified products when considering alert and warning system purchases or upgrades.

Disclaimer

Test results and use of trade names on the IPAWS CA and RKB websites do not constitute a Department of Homeland Security (DHS) or FEMA certification or endorsement of the use of such commercial products.

Test Process

Test Conduct

An appropriate set of test cases and procedures will be performed by the test engineer. Test cases are included in **Appendix A: Test Cases and Objectives**.

Reporting

Test reports will include a description of the product and events that occurred during the test, and results regarding conformance.

Supplier's Declaration of Conformity

The information in this section is in accordance with ISO/IEC-17050-1:2004 and ISO/IEC-17050-2:2004.

The purpose of the Supplier's Declaration of Conformity (SDoC) is to give assurance of conformity of the vendor's product to which the declaration refers, and to clarify who is responsible for that conformity and declaration. Alert and warning product providers may release test reports and SDoCs based on independent testing from recognized laboratories. This will assure broadcasters and the public that equipment complies with applicable standards and guidance. Once the product qualifies, independent test authority staff may provide an SDoC template to the vendor to complete and sign (See **Appendix B: Sample Supplier's Declaration of Conformity** Format).

The product supplier's authorized signatory to the SDoC bears full responsibility for the content, completeness, and accuracy of the SDoC. FEMA, DHS, and program staff are not responsible for incomplete or inaccurate statements within an SDoC. Furthermore, it is the vendor's responsibility to re-evaluate the validity of the declaration of conformity in the following situations:

- There are changes that affect the product's design or specification.
- There are changes to the specified requirements (including standards) that relate to the product of the declaration.
- There are changes in the ownership or management of the vendor.

- There is any relevant information which indicates the product no longer fulfills the specified requirement.

Results from test events may be posted on the RKB website (https://www.rkb.us)

Roles and Responsibilities

The following table, **Table 1: Participating Organizations**, describes the roles and responsibilities of the participants.

Table 1: Participating Organizations

Participant	Roles and Responsibilities
FEMA IPAWS PMO	FEMA IPAWS PMO is responsible for the overall guidance and for setting the appropriate levels of conformity assessment in coordination with program staff. FEMA IPAWS PMO is also responsible for the Profile description and for publishing any potential updates and changes to the conformity assessment program policies or procedures, and any/all information that may impact either the broadcast or vendor community.
ITA	The laboratory supports tests that aim to verify that systems conform to IPAWS requirements. ITA refers to personnel directly involved in the CA testing process.
Vendors	Vendors are responsible for selecting an ITA, and agreeing to the ITA's unique rules, roles, and responsibilities.

Appendix A: Test Cases and Objectives

IPAWS CA Test Cases and Objectives

Test Case Summary

IPAWS CA test cases are grouped into suites based on (1) the product's category and (2) the particular program requirement on which the test is based. The following is relevant to current FCC equipment certification requirements:

Table 2: Product Category for EAS Testing

Categories / Descriptions	CAP Version 1.2	CAP v1.2 USA IPAWS Profile Version 1.0	CAP EAS Implementation Guide, Version 1.0
EAS Encoder/Decoders and **CAP-to-EAS Converters** consume CAP messages and produce EAS alerts. EAS Encoder/Decoders are certified by the FCC to broadcast those alerts to the public; CAP-to-EAS Converters depend on downstream EAS Encoder/Decoders to broadcast those alerts to the public.	Test Suite 20	Test Suite 21	Test Suite 22

Note: Test Suite 00 falls outside of this categorization, and applies to all products.

Test Suite 00 - Production Ready

Objective

The purpose of the single test case in this suite is to determine whether the product under test is Production Ready and can be installed, configured, and operated according to vendor-supplied documentation. During this test, test engineers configure the product in accordance with the objectives of the remaining test cases.

Table 3: Test Suite 00, Test Cases and Objectives

Test Case Identifier and Title	Test Case Objective
IPAWS_CA_0000 Production Ready Status	Verify that the product under test is production ready. Ensure proper turn-on and communication functionality.

Test Suites 20, 21, and 22 - EAS Devices Test Suites

Overview

These are the primary "CAP message consumer" suites. They cover both EAS Encoder/Decoders and CAP-to-EAS Converters, recognizing that CAP-to-EAS Converters can emit EAS alerts that would not be allowed by FCC Part 11 (because the emitted alerts are designed to be further processed by an EAS Encoder/Decoders). For example, a CAP-to-EAS Converter may choose to emit an expired EAS alert knowing that downstream EAS Encoder/Decoders will not relay such an alert to the public.

The results of test cases with an "observe" objective do not impact product conformity.

Approach

Test engineers will present various messages to the products under test, and observe the actions and resulting alerts of those products.

Test Suite 20: CAP Version 1.2 Tests

Table 4: Test Suite 20, Test Cases and Objectives

Test Case Identifier and Title	Test Case Objective
IPAWS_CA_2000 Baseline EAS Alert	Establish basic message consumption and alert production.
IPAWS_CA_2001 Message Type	Determine whether the product under test recognizes "Update", "Error", and "Ack" messages.
IPAWS_CA_2002 Language	Observe the product's performance when presented with English and non-English <language> elements.
IPAWS_CA_2003 Message Importance	Determine whether the product under test alerts regardless of the content of the <urgency>, <severity>, and <certainty> elements of a Profile message.
IPAWS_CA_2004 Queuing	Observe the product's performance when presented with input more quickly than it can produce output.

Test Suite 21: CAP v. 1.2 USA IPAWS Profile Version 1.0 Tests

Table 5: Test Suite 21, Test Cases and Objectives

Test Case Identifier and Title	Test Case Objective
IPAWS_CA_2100 Event Code	Determine whether the product under test recognizes and handles event codes as defined by the <eventCode> specification in the Profile.
IPAWS_CA_2101 Geocode Handling - National Political	Determine whether the product under test recognizes national alerts in incoming Profile messages.
IPAWS_CA_2102 Geocode Handling - Local Political	Determine whether the product under test recognizes its assigned political location information in incoming Profile messages.
IPAWS_CA_2103 EAS Duplicates	Determine whether the product under test recognizes different Profile messages that resolve to duplicate EAS output.
IPAWS_CA_2104 CAP Duplicates	Determine whether the product under test recognizes that different Profile messages with the same <identifier>, <sender>, and <sent> elements are duplicate messages.
IPAWS_CA_2105 Degenerate Messages	Observe the product's performance when presented with messages that conform to the Profile but are in some way nonsensical and/or non-EAS-triggering.

Additional Information for Test Suite 21:

IPAWS_CA_2101, Geocode Handling - National Political: FCC Part 11 does not recognize “000000” as a valid FIPS code. However, this test case tests against the <geocode> specification in the OASIS CAP v. 1.2 USA IPAWS Profile Version 1.0.

IPAWS_CA_2102, Geocode Handling - Local Political: Results of this test case are reported as pass/fail for EAS Encoder/Decoders and as an observation for CAP-to-EAS Converters.

IPAWS_CA_2103, EAS Duplicates: Results of this test case are reported as pass/fail for EAS Encoder/Decoders and as an observation for CAP-to-EAS Converters. FCC Part 11.33(10) prohibits duplicate EAS output.

IPAWS_CA_2104, CAP Duplicates: Results of this test case are reported as pass/fail for EAS Encoder/Decoders and as an observation for CAP-to-EAS Converters. FCC Part 11.33(10) prohibits duplicate EAS output.

IPAWS_CA_2105, Degenerate Messages: Products under test are subjected to Profile messages suffering the following conditions: no <info> element; <msgType> of "Update" or "Cancel," but no <references> element; event codes of "nic," "qqq," "WYYZ," and "NICX"; no SAME event code; EAS originators of "civ" and "QQQ"; and <area> elements not containing location information.

Test Suite 22: CAP EAS Implementation Guide, Version 1.0 Tests

Table 6: Test Suite 22, Test Cases and Objectives

Test Case Identifier and Title	Test Case Objective
IPAWS_CA_2200 Text-To-Speech	Observe whether the product under test creates speech from text as described by §3.6 of the CAP EAS Implementation Guide.
IPAWS_CA_2201 <area> Element	Determine whether the product under test handles <area> elements as described by the <area> entry in §6.7 of the CAP EAS Implementation Guide.
IPAWS_CA_2202 Remote Resources	Determine whether the product under test handles remote audio resources as described by §3.5 of the CAP EAS Implementation Guide.
IPAWS_CA_2203 Duration	Determine whether the product under test handles <expires> elements as described by the <expires> entry in §6.7 of the CAP EAS Implementation Guide.
IPAWS_CA_2205 Message Type	Determine whether the product under test handles "Cancel" messages as described in §3.8.3 of the CAP EAS Implementation Guide.
IPAWS_CA_2206 EAS Originator	Determine whether the product under test handles the EAS-ORG <parameters> as described by the EAS-ORG Special EAS parameter entry of §6.7 of the CAP EAS Implementation Guide.
IPAWS_CA_2207 Target Audience	Determine whether the product under test suppresses non-public Profile messages.
IPAWS_CA_2208 Expired Messages	Determine whether the product under test recognizes expired Profile messages as described by the <expires> entry in §6.7 of the CAP EAS Implementation Guide.

Additional Information for Test Suite 22:

IPAWS_CA_2200, Text-To-Speech: There are inconsistencies between the algorithm and the flowchart in §3.6.4.4 of the EAS CAP Industry Group (ECIG) Guide (in the case

that the length of the <description> is less than half and the length of the <instruction> is not); this test case is based on the flowchart.

IPAWS_CA_2201, <area> Element: The CAP EAS Implementation Guide requires that "[s]econd or more <area> blocks will not be processed." This constrains the OASIS CAP v1.2 Standard's specification for the <area> element, which says "[m]ultiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks."

IPAWS_CA_2202, Remote Resources: Remote audio resources in this test were collected from public domain sources and re-encoded to conform to the guidelines in §3.5.2 of the CAP EAS Implementation Guide: MP3, mono, 64 kbit/s data, sampled at 22.05 kHz or 44.1 kHz.

IPAWS_CA_2203, Duration: §6.7 of the CAP EAS Implementation Guide contains an error in its description of the <expires> element. Specifically, the Guide says, "[the <expires> element is] used to derive the EAS Valid Time Period (TTTT) by subtracting from <sent> to derive a duration ...." Subtracting in the prescribed manner will give negative TTTT values, and then that same paragraph goes on to describe rounding and ignoring rules based on the arithmetic sign of the derived duration. This test case assumes that the word "from" is extraneous.

IPAWS_CA_2207, Target Audience: Results of this test case are reported as pass/fail for EAS Encoder/Decoders as well as CAP-to-EAS Converters.

IPAWS_CA_2208, Expired Messages: Results of this test case are reported as pass/fail for EAS Encoder/Decoders and as an observation for CAP-to-EAS Converters. See also the additional information for Test Case IPAWS_CA_2203, above.

Appendix B: Sample Supplier's Declaration of Conformity Format

Supplier's Declaration of Conformity (SDoC)

SDOC-*[Product Name]-[4 or 5 digit test report number]*

*[**Company Name**]*
[department]
[address]
Customer Contact: *[customer's contact name]*
Phone: *[999-999-9999]*, Fax: *[999-999-9999]*
[company's web address]
[e-mail address of the customer contact]

Product Name: *[product name, product version number, and/or model number]*

FCC ID (if applicable): *[FCC ID]*

Product Category: *[product category]*

Product Description: *[product description]*

Installed Options: *[installed options include version numbers]*

Vendor-Provided Products Tested with *[product name]*: *[manufacturer, product name, model and/or version number(s), product definition, unique ID, and installed options]*

Additional Information (if necessary): *[additional information]*

[Company name] hereby declares that *[product name] [version #]* product(s) conform(s) to the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) v1.2 Standard (1 July 2010) and the OASIS CAP v1.2 USA IPAWS Profile v1.0 (13 October 2009) and passed the test cases in their entirety without exclusions.

The report for the test performed at_____, located at_____, is identified as follows:

Test Report Identification: *TR-[product name]-[or test report number]* issued by *[Testing lab conducting assessment]* on *[Month Day, Year]*.

Issue Date	*Supplier's Authorized Representative Signature*
	Supplier's Authorized Representative Printed Name

This information contained herein has been provided by the vendor of the product with permission to make the information publicly available. The U.S. Department of Homeland Security (DHS) is making this information available as a public service; however, DHS IS PROVIDING THE INFORMATION "AS IS." DHS MAKES NO EXPRESS OR IMPLIED WARRANTIES AND SPECIFICALLY, DHS MAKES NO WARRANTIES OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ACCURACY OR USE OF THIS INFORMATION. Reference to any specific commercial products, processes, or services by trade name, trademark, vendor, or otherwise does not constitute an endorsement by or a recommendation from DHS.

Appendix C: References

1. A2LA, http://www.a2la.org/
2. EAS CAP Industry Group, EAS-CAP Implementation Guide Subcommittee, CAP EAS Implementation Guide, Version 1.0, 17 May 2010, http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf
3. Federal Communications Commission (FCC) Code of Federal Regulations (CFR), Title 47, Part 11, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=47:1.0.1.1.11&idno=47
4. IPAWS, http://www.fema.gov/emergency/ipaws/
5. ISO/IEC 17025: 2005, http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883
6. ISO/IEC 17050: 2004 (part 1 and 2), http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29373 and http://www.iso.org/iso/catalogue_detail.htm?csnumber=35516
7. OASIS Common Alerting Protocol Version 1.2, OASIS Standard, 01 July 2010, http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.pdf
8. OASIS Common Alerting Protocol (CAP) Version 1.2 Schema, http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd
9. OASIS Common Alerting Protocol (CAP) v1.2 USA Integrated Public Alert and Warning System Profile Version 1.0 – Committee Specification 01, 13 October 2009, http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cs01/
10. RKB website, https://www.rkb.us/

Appendix D: Acronyms and Abbreviations

CA	Conformity Assessment
CAP	Common Alerting Protocol
CFR	Code of Federal Regulations
DAB	Digital Audio Broadcast
DBS	Direct Broadcast Satellite
DHS	Department of Homeland Security
EAS	Emergency Alert System
ECIG	EAS CAP Industry Group
EO	Executive Order
EOC	Emergency Operations Center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
IANA	Internet Assigned Numbers Authority
IEC	International Electrotechnical Commission
IPAWS	Integrated Public Alert and Warning System
ISO	International Organization for Standardization
IT	Information Technology
ITA	Independent Testing Authority
MIME	Multipurpose Internet Mail Extensions
NDA	Non-Disclosure Agreement
OASIS	Organization for the Advancement of Structured Information Standards
PMO	Program Management Office
QC	Quality Control
RKB	Responder Knowledge Base
SAME	Specific Area Message Encoding
SDARS	Satellite Digital Audio Radio System
SDoC	Supplier's Declaration of Conformity
TCB	Telecommunications Certification Body
URL	Uniform Resource Locator