Integrated Public Alert and Warning System (IPAWS) Conformity Assessment (CA) Program Test Report (TR)

Communications Laboratories (Comlabs), Inc.
EMnet CAP-to-EAS Converter (software version 4.0.1.36)

TR-EMnet-12920

July 2011

FEMA

Table of Contents

List of Tables

1.0 Introduction

This report presents the results from a test of the EMnet CAP-to-EAS Converter, software version number 4.0.1.36, referred to herein as the product[1], developed by Communications Laboratories (Comlabs), Inc., which was conducted as part of the Integrated Public Alert and Warning System (IPAWS) Conformity Assessment (CA) Program.

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) National Continuity Programs Directorate is sponsoring the IPAWS CA Program to assist in the implementation of Executive Order (EO) 13407, "Public Alert and Warning System," as well as to fulfill Homeland Security Presidential Directive (HSPD)-20, which establishes a comprehensive national policy on the continuity of the federal government. FEMA IPAWS provides the Nation's next generation public alert and warning capability expanding upon the traditional audio-only radio and television Emergency Alert System (EAS). This allows the President of the United States 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.

IPAWS CA is designed to ensure the vendors who wish to provide hardware or software solutions to meet Federal Communications Commission (FCC) and FEMA requirements conform to the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) Version 1.2; OASIS CAP v. 1.2 USA IPAWS Profile Version 1.0; CAP EAS Implementation Guide Version 1.0[2]; and FCC Title 47 of the Code of Federal Regulations (CFR) Part 11, herein collectively referred to as the program requirements. The term Profile message(s) is used in this document to describe Extensible Markup Language (XML) formatted messages that comply with the program requirements. To support testing, FEMA awarded a contract to Eastern Kentucky University (EKU) in August 2009. EKU teamed with Science Applications International Corporation (SAIC) to develop and operate the IPAWS CA Program.

The SAIC location in Somerset, KY includes the Incident Management Test and Evaluation Laboratory (IMTEL), where this test took place. The intent of this test was to determine the system's conformance to the program requirements. This report provides an overview of the product, followed by the test results. Note that the test results and use of trade names in this report do not constitute a DHS or FEMA certification or endorsement of the use of such commercial products.

[1] System and product are used interchangeably in this document.

[2] IPAWS CA recognizes the CAP EAS Implementation Guide as per FEMA's memorandum of concurrence; see http://www.eas-cap.org/.

IMTEL is accredited through the American Association for Laboratory Accreditation (A2LA). To maintain accreditation status, the laboratory meets general requirements for the competencies of testing and calibration laboratories, as provided in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025:2005. The current scope of accreditation and associated certifications are available on A2LA's website for ISO/IEC 17025:2005. Test results in sections **2.1 Detailed Test Results** and section **2.2 Summarized Test Results** are within IMTEL's ISO/IEC 17025:2005 scope of accreditation. Any opinions contained within this report are derived from guidance provided by FEMA.[3] Other individual findings, observations, and results that fall outside the scope of accreditation are marked with an asterisk (*).

1.1 System Description[4]

EMnet is a privately managed messaging network for the Emergency Management Community which conveys messages as well as documentation for use by its customers.

1.2 Test Objective

The objective of this CA test was to determine conformance to the program requirements. This product is a CAP-to-EAS Converter. Test engineers executed the test procedures of the test cases outlined in section **2.2 Summarized Test Results** and scored each test step as Pass, Fail, or Not Applicable (NA) based on the category and the performance of the system. Additional information based on the test results is listed as key findings.

1.3 Test Setup

Test engineers used vendor-provided documentation for product installation, setup, and configuration as detailed in section **2.1 Detailed Test Results**.

1.3.1 Laboratory Environment

The IMTEL setup for the IPAWS CA test environment consisted of workstations with Local Area Network (LAN) connectivity and supporting hardware/software tools. Other resources included vendor-provided hardware, software, and documentation necessary to conduct IPAWS CA testing.

---

[3] IPAWS CA Program Guide, http://www.fema.gov/emergency/ipaws/.

[4] The vendor provided the majority of information within this section. IMTEL staff did not verify all of the system's capabilities during the test, only those associated with the program requirements.

Table 1: Supporting Tools

Tool	Version
SUNOS 5.11	8.0.6001.18702
SeaTTY	2.30.0.480
Windows XP	2002 sp3

1.4 Test Schedule

IMTEL staff conducted testing on the system on 30 - 31 July 2011.

1.5 Limitations

Table 2: Limitations identifies issues that impacted the test and the approach to mitigating them.

Table 2: Limitations

Limitation	Impact	Mitigation Strategy
The product under test operates in a client/server environment with Comlabs' centralized server. Comlabs' centralized server product is managed internally by Comlabs and is not available to the customer.	Comlabs' centralized server is required for testing the product under test.	Comlabs provided a server to simulate the production environment.

2.0 Test Results

Test results in section **2.1 Detailed Test Results** and section **2.2 Summarized Test Results** are within IMTEL's ISO/IEC 17025:2005 scope of accreditation. Other individual findings, observations, and results that fall outside the scope of accreditation are marked with an asterisk (*).

The following results are organized according to the test suites for a CAP-to-EAS Converter, and provide a summary of key findings.

2.1 Detailed Test Results

2.1.1 Test Case IPAWS_CA_0000 - Production Ready Status

The objective of this test case was to determine whether the product is Production Ready and can be installed, configured, and operated according to vendor-supplied documentation. Following vendor-provided setup instructions, the test engineer installed and configured the product in preparation for the test.

2.1.1.1 Results

Based on product documentation, IMTEL's test engineers configured the product. A ping message was sent from IMTEL's computer to the product's assigned IP address which successfully generated a response.

2.1.2 Test Case IPAWS_CA_2000 EAS Baseline Alert

The test engineer sent conforming Profile messages to the product to establish basic Profile message consumption and EAS alert production.

2.1.2.1 Results

When the product was tested to ensure that it would consume a basic Profile message, the product consumed the conforming messages and generated the expected EAS alerts.

2.1.2.2 References

OASIS CAP Version 1.2 Standard; OASIS CAP v1.2 USA IPAWS Profile Version 1.0; FCC CFR, Title 47, Part 11 §11.31; CAP EAS Implementation Guide §3.4.

2.1.3 Test Case IPAWS_CA_2001 Message Type

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes "non -Alert" messages (i.e., messages whose <msgType> element is not "Alert"). All such messages in this test case contained a <references> element that correctly refers to a previously issued "Alert" message.

2.1.3.1 Results

The product was tested to ensure that it would correctly consume various message types (e.g., “Update”, “Error”, and “Ack”). When the product was tested with <msgType> elements of “Alert” or “Update”, the product generated the expected EAS alert. When the product was tested with <msgType> elements of “Ack” or “Error”, as expected the product did not generate an EAS alert.

2.1.3.2 References

OASIS CAP Version 1.2 Standard, <msgType> element; CAP EAS Implementation Guide §3.8.

2.1.4 Test Case IPAWS_CA_2002 Language*

The test engineer sent conforming Profile messages to the product to observe the product's performance when presented with English and non-English <language> elements.

2.1.4.1 Results

When the product was tested to consume a message with a <language> element that was only English, the product generated an EAS alert. When the product consumed a message with a <language> element that was non-English, the product did not generate an EAS alert. When the product consumed a message containing two <language> elements, one of English and another non-English, the product generated an EAS alert for only the English <language> element.

2.1.4.2 References

OASIS CAP Version 1.2 Standard, <language> element; CAP EAS Implementation Guide §3.7.

2.1.5 Test Case IPAWS_CA_2003 Message Importance

The test engineer sent conforming Profile messages to the product to determine whether the product alerts regardless of the content of the <urgency>, <severity>, and <certainty> elements of a Profile message.

Messages in this test case contain all individual <urgency>, <severity>, and <certainty> values allowed by the Profile, but not all combinations thereof.

2.1.5.1 Results

When the product consumed multiple messages containing different content in the Message Importance elements, the product generated the expected EAS alerts.

2.1.5.2 References

OASIS CAP Version 1.2 Standard, <urgency>, <severity>, and <certainty> elements; FCC CFR Title 47, Part 11 §11.31, and the lack of this information in an EAS alert; CAP EAS Implementation Guide §6.7.

2.1.6 Test Case IPAWS_CA_2004 Queuing*

The test engineer sent conforming Profile messages to the product to observe the product's performance when presented with input more quickly than it can produce output.

2.1.6.1 Results

When the product consumed messages that were sent more quickly than EAS alerts could be generated, the product generated the correct EAS alerts in the proper sequence.

2.1.6.2 References

OASIS CAP Version 1.2 Standard, §4.4 Conformance as a CAP V1.2 Message Consumer.

2.1.7 Test Case IPAWS_CA_2100 Event Code

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes and handles event codes as defined by the <eventCode> specification in the Profile.

Messages in this test case exercise all event codes in FCC Part 11 §11.31, as well as other three-letter event codes. Some messages in this test case contain multiple <eventCode> elements.

2.1.7.1 Results

When the product was tested to ensure that it would correctly consume messages containing event codes defined by the <eventCode> specification in the Profile, all event codes were recognized and handled by the product and the expected EAS alerts were generated.

2.1.7.2 References

OASIS CAP Version 1.2 Standard, <eventCode> element; OASIS CAP v1.2 USA IPAWS Profile Version 1.0, <eventCode> element; CAP EAS Implementation Guide §3.4.1.2.

2.1.8 Test Case IPAWS_CA_2101 Geocode Handling - National Political

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes national alerts in incoming Profile messages.

Messages in this test case contain a variety of national alerts. All messages are intended to produce EAS output.

2.1.8.1 Results

When the product was tested to ensure that it would correctly consume a message that contained an SAME <geocode> value of all zeros (i.e., 000000), the product generated an EAS alert as expected.

2.1.8.2 References

OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <geocode> element; CAP EAS Implementation Guide §3.4.1.3.

2.1.9 Test Case IPAWS_CA_2102 Geocode Handling - Local Political

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes its assigned political location information in incoming Profile messages.

Messages in this test case contain one <area> element containing a specific county's Federal Information Processing Standard (FIPS) code in different places and in combination with other FIPS codes. All messages are intended to produce EAS output.

2.1.9.1 Results

The product was tested to ensure that it would properly consume messages that contain local FIPS codes for a specific county in the <area> element. The product generated the expected EAS alerts when it received messages from the specific county for which the product was configured.

2.1.9.2 References

OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <geocode> element; FCC CFR, Title 47, Part 11 §11.31; CAP EAS Implementation Guide §3.4.1.3.

2.1.10 Test Case IPAWS_CA_2103 EAS Duplicates

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes different Profile messages that resolve to duplicate EAS output. FCC Part 11 §11.33 (10) prohibits duplicate EAS output.

2.1.10.1 Results

For a CAP-to-EAS converter this test case is an observation (not an FCC-compliant device). When the product was tested to ensure that it would identify duplicate messages generating the same EAS output, the product did not produce an EAS alert for duplicate messages.

2.1.10.2 References

FCC Part 11 §11.33(10); CAP EAS Implementation Guide §3.11.

2.1.11 Test Case IPAWS_CA_2104 CAP Duplicates*

The test engineer sent conforming Profile messages to the product to observe the product's performance when presented with CAP messages containing the same identifying information (i.e., <identifier>, <sender>, and <sent> elements) but different alert content information (e.g., event codes, originator codes, expiration times).

2.1.11.1 Results

When the product consumed messages that are considered CAP Duplicates, the product did not generate an EAS alert for duplicate messages.

2.1.11.2 References

OASIS CAP Version 1.2 Standard; <identifier>, <sender>, and <sent> elements; CAP EAS Implementation Guide §3.11.

2.1.12 Test Case IPAWS_CA_2105 Degenerate Messages*

The test engineer sent conforming Profile messages to the product to 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.

Messages 2105-degenerate-a1, 2105-degenerate-a2, and 2105-degenerate-a3 are messages whose <msgType> is “Alert,” “Update,” and “Cancel,” respectively, but do not contain an <info> element.

Messages 2105-degenerate-b1 and 2105-degenerate-b2 are messages whose <msgType> are “Update” and “Cancel,” respectively, but do not contain a <references> element.

Messages 2105-degenerate-c1 through 2105-degenerate-c4 contain <eventCode> elements with a valueName of “SAME” and <value> elements of “nic,” “qqq,” “WXYZ,” and “NICX.” Message 2105-degenerate-c5 contains an eventCode with a <valueName> that isn't SAME and a <value> of “CDW.”

Message 2105-degenerate-d1 contains an EAS originator of “civ”; message 2105-degenerate-d2 contains an EAS originator of “QQQ.”

Message 2105-degenerate-e1 contains an <area> element without any location information; message 2105-degenerate-e2 contains two such <area> elements.

2.1.12.1 Results

When the product was tested to ensure that it would not generate EAS alerts for nonsensical and/or non-EAS-triggering messages, all messages were ignored and no EAS alerts were generated.

2.1.12.2 References

OASIS CAP Version 1.2 Standard; OASIS CAP v1.2 USA IPAWS Profile Version 1.0; FCC CFR, Title 47, Part 11.

2.1.13 Test Case IPAWS_CA_2200 Text-to-Speech

The test engineer sent conforming Profile messages to the product to determine whether the product creates speech from text as described by §3.6 of the CAP EAS Implementation Guide.

In particular, the CAP EAS Implementation Guide provides detail with respect to turning the FCC required text and the <senderName>, <description>, and <instruction> elements of a Profile message into

audio speech. There are inconsistencies between the algorithm and the flowchart in §3.6.4.4 of the CAP EAS Implementation 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.

2.1.13.1 Results

The product consumed messages intended to determine if the product can create speech from text. The product generated multiple EAS alerts with the expected speech output.

2.1.13.2 References

OASIS CAP Version 1.2 Standard and OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <senderName>, <description>, and <instruction> elements; CAP EAS Implementation Guide §3.6.

2.1.14 Test Case IPAWS_CA_2201 <area> Element

The test engineer sent conforming Profile messages to the product to determine whether the product handles <area> elements as described by the <area> entry in §6.7 of the CAP EAS Implementation Guide.

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."

2.1.14.1 Results

When the product was tested to ensure that when a message containing a second <area> block was sent, it would not process more than the first <area> block; the product responded as expected.

2.1.14.2 References

OASIS CAP Version 1.2 Standard <area> element; CAP EAS Implementation Guide <area> entry of §6.7.

2.1.15 Test Case IPAWS_CA_2202 Remote Resources*

The test engineer sent conforming Profile messages to the product to observe whether the product handles remote audio resources as described by §3.5 of the CAP EAS Implementation Guide.

In particular, the CAP EAS Implementation Guide describes what is and is not an acceptable remote audio resource, EAS-related limitations on audio resources, Multipurpose Internet Mail Extensions (MIME) types, sample and bit rates, etc.

2.1.15.1 Results

When the product was tested to ensure that it would correctly handle remote audio resources, the product generated EAS audio as expected.

2.1.15.2 References

OASIS CAP Version 1.2 Standard and OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <resource> element; CAP EAS Implementation Guide §3.5[5].

2.1.16 Test Case IPAWS_CA_2203 Duration

The test engineer sent conforming Profile messages to the product to determine whether the product handles <expires> elements as described by the <expires> entry in §6.7 of the CAP EAS Implementation Guide.

Note that §6.7 of the CAP EAS Implementation Guide contains an error in its description of the <expires> element; it specifically says, "[the <expires> element is] 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.

2.1.16.1 Results

When the product was tested to ensure that it would validate the time period contained within a message, the product correctly determined the appropriate time period and generated the expected EAS alerts.

2.1.16.2 References

OASIS CAP Version 1.2 Standard; OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <sent> and <expires> elements; CAP EAS Implementation Guide <expires> entry of §6.7.

2.1.17 Test Case IPAWS_CA_2204 EAS Must-Carry

The test engineer sent conforming Profile messages to the product to determine whether the product handles Gubernatorial Must Carry alerts as described by §3.4.1.7 and the <parameter> EAS-Must-Carry entry of §6.7 of the CAP EAS Implementation Guide.

In particular, the CAP EAS Implementation Guide requires that Gubernatorial Must Carry messages override any Originator and Event Code filtering in an EAS product.

[5] IPAWS CA recognizes the CAP EAS Implementation Guide as per FEMA's memorandum of concurrence; see http://www.eas-cap.org/.

2.1.17.1 Results

The product was reconfigured to support all Event Codes messages except CEM. When the reconfigured product was tested to ensure that it would correctly consume a message containing the Gubernatorial Must Carry flag, it generated the expected EAS alert.

2.1.17.2 References

OASIS CAP v1.2 USA IPAWS Profile Version 1.0 "EAS-Must-Carry" parameter; CAP EAS Implementation Guide §3.4.1.7 and the <parameter> EAS-Must-Carry entry of §6.7.

2.1.18 Test Case IPAWS_CA_2205 Message Type

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes “Cancel” messages (i.e., messages whose <msgType> element is “Cancel”). The message in this test case contains a <references> element that correctly refers to a previously issued “Alert” message.

2.1.18.1 Results

When the product was tested to ensure that it would correctly recognize messages with <msgType> elements that contain a value of “Cancel”, the product did not generate an EAS alert.

2.1.18.2 References

OASIS CAP Version 1.2 Standard and OASIS CAP v1.2 USA IPAWS Profile Version 1.0 <msgType> element; CAP EAS Implementation Guide §3.8.3.

2.1.19 Test Case IPAWS_CA_2206 EAS Originator

The test engineer sent conforming Profile messages to the product to determine whether the product handles the EAS-ORG <parameter> as described by the EAS-ORG Special EAS parameter entry of §6.7 of the CAP EAS Implementation Guide.

In particular, the CAP EAS Implementation Guide requires that messages without a correct EAS-ORG <parameter> be rejected.

2.1.19.1 Results

When the product was tested to ensure that it would reject messages without a correct EAS-ORG <parameter>, as expected the product did not generate an EAS alert.

2.1.19.2 References

CAP EAS Implementation Guide EAS-ORG special parameter entry of §6.7.

2.1.20 Test Case IPAWS_CA_2207 Target Audience

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes non-public Profile messages (and does not emit EAS alerts for them).

2.1.20.1 Results

The product was tested to ensure that it would not generate an EAS alert for non-public messages that contain the values of "Private" and "Restricted" within their <scope> elements. When messages contained a <scope> value of "Private" or "Restricted", the product did not generate an EAS alert and the product log stated that only public messages are allowed. Furthermore, when the message contained a <scope> value of "Public", the product generated an EAS alert as expected.

2.1.20.2 References

OASIS CAP Version 1.2 Standard, <scope> element notes; CAP EAS Implementation Guide <scope> entry of §6.7.

2.1.21 Test Case IPAWS_CA_2208 Expired Messages

The test engineer sent conforming Profile messages to the product to determine whether the product recognizes expired Profile messages.

2.1.21.1 Results

For a CAP-to-EAS converter this test case is an observation only (not an FCC-compliant device). When the product was tested to ensure that it would not generate an alert for an expired message, the product did not generate an EAS alert and the product log stated that the alert had expired.

2.1.21.2 References

OASIS CAP Version 1.2 Standard and OASIS CAP v1.2 USA IPAWS Profile Version 1.0, <expires> element; CAP EAS Implementation Guide §6.7.

2.2 Summarized Test Results

Table 3: Test Results – CAP-to-EAS Converter

Legend:	▲ Meets requirements (Pass) ▼ Does not meet requirements (Fail) ● No Rating or Not Applicable (NA) to the system

Test Case Identifier and Title	Test Case Objective	Rating	Key Findings
IPAWS_CA_0000 Production Ready Status	Verify that the product under test is production ready. Ensure proper turn-on and communication functionality.	▲	
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.	●	Observations only; see results for complete information.
IPAWS_CA_2003 Message Importance	Determine whether the product 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.	●	Observations only; see results for complete information.

Legend:	 Meets requirements (Pass) Does not meet requirements (Fail) No Rating or Not Applicable (NA) to the system

Test Case Identifier and Title	Test Case Objective	Rating	Key Findings
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 or observe whether the product under test recognizes different Profile messages that resolve to duplicate EAS output.		Observations only; see results for complete information.
IPAWS_CA_2104 CAP Duplicates*	Observe the product's performance when presented with CAP messages containing the same identifying information (i.e., <identifier>, <sender>, and <sent> elements) but different alert content information (e.g., event codes, originator codes, or expiration times).		Observations only; see results for complete information.

Legend:	 Meets requirements (Pass) Does not meet requirements (Fail) No Rating or Not Applicable (NA) to the system

Test Case Identifier and Title	Test Case Objective	Rating	Key Findings
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.	○	Observations only; see results for complete information.
IPAWS_CA_2200 Text-to-Speech	Determine 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.	○	Observations only; see results for complete information.
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.	△	

Legend:	
	▲ Meets requirements (Pass) ▼ Does not meet requirements (Fail) ● No Rating or Not Applicable (NA) to the system

Test Case Identifier and Title	Test Case Objective	Rating	Key Findings
IPAWS_CA_2204 EAS Must-Carry	Determine whether the product under test handles Gubernatorial Must Carry alerts as described by §3.4.1.7 and the <parameter> EAS-Must-Carry entry of §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.	●	Observations only; see results for complete information.

* Observations fall outside the scope of accreditation.

2.3 Additional Observations*

The results in this section are observations made by test engineers during the execution of test cases. Such observations were not used in determination of any test results and/or ratings in this report and are provided for informational purposes only.

Table 4: Additional Observations

Observation	Test Case References
Test Engineers noted that during the execution of this test case, the Text-to-Speech audio rendered “Non-Standard Event” for event code value “QQQ”.	Test Case IPAWS_CA_2200 Event Code

3.0 Appendix A: References

1. A2LA, http://www.a2la.org/

2. Communications Laboratories (Comlabs), Inc., http://www.comlabs.com/

3. EAS CAP Industry Group, EAS-CAP Implementation Guide Subcommittee, CAP EAS Implementation Guide, Version 1.0, 17 May 2010, http://www.eas-cap.org/

4. 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

5. FEMA's memorandum of concurrence with the "ECIG Recommendations For a CAP EAS Implementation Guide" Guidance Revised, 02 December 2010, http://www.eas-cap.org/

6. Federal Information Processing Standards Publication 6-4, 31 August 1990, http://www.itl.nist.gov/fipspubs/fip6-4.htm

7. Homeland Security Presidential Directorate – 20, http://www.dhs.gov/xabout/laws/gc_1219245380392.shtm

8. ISO/IEC 17025: 2005, http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883

9. IPAWS, http://www.fema.gov/emergency/ipaws/

10. 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

11. 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/

12. Specific Area Message Encoding (SAME), http://www.weather.gov/nwr/nwrsame.htm

4.0 Appendix B: List of Acronyms

A2LA	American Association for Laboratory Accreditation
CA	Conformity Assessment
CAP	Common Alerting Protocol
CFR	Code of Federal Regulations
Comlabs	Communication Laboratories
DHS	Department of Homeland Security
EAS	Emergency Alert System
EKU	Eastern Kentucky University
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
IEC	International Electrotechnical Commission
IMTEL	Incident Management Test and Evaluation Laboratory
IPAWS	Integrated Public Alert and Warning System
ISO	International Organization for Standardization
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
NA	Not Applicable
OASIS	Organization for the Advancement of Structured Information Standards
SAIC	Science Applications International Corporation
SAME	Specific Area Message Encoding

TR	Test Report
USA	United States of America
XML	Extensible Markup Language