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

Communications Laboratories (Comlabs), Inc.
EMnet Originator (software version 4.0)

TR-EMnet-12921

July 2011

FEMA

Table of Contents

List of Tables

1.0 Introduction

This report presents the results from a test of the EMnet Originator, software version number 4.0, 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. The 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. If the Pass/Fail accredited rating is based on IMTEL's opinion, an explanation for the rating is marked with a solid square (■). 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 national emergency communications network designed to provide a standardized platform for emergency and routine (non-emergency) communications between network endpoints.

1.2 Test Objective

The objective of this CA test was to determine conformance to the program requirements. This product is a CAP Message Originator. 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 explained within **Section 2.1 Detailed Test Results.**

[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.

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.

Table 1: Supporting Tools

Tool	Version
XRay2	2.2.6

1.4 Test Schedule

IMTEL staff conducted testing on the system 20 - 22 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

Section 2.1 Detailed Test Results and **Section 2.2 Summarized Test Results** are within IMTEL's ISO/IEC 17025:2005 scope of accreditation. If the Pass/Fail accredited rating is based on IMTEL's opinion, an explanation for the rating is marked with a solid square (■). 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 (*).

The following results are organized according to the test suites for a CAP Message Originator 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 discussions with the vendor as well as the utilization of the product documentation, IMTEL's test engineers configured the product and verified network connectivity required for testing. Test Case IPAWS_CA_0000 – Production Ready Status execution simulates the product as it would be configured in an operational production environment.

2.1.2 Message Producer Test Suites

The objective of these test suites are to verify messages produced by the product under test conform to the OASIS CAP v1.2 Standard and OASIS CAP v. 1.2 USA IPAWS Profile Version 1.0. It is not necessary that the product tested exercise every feature and/or every permutation of Profile messages. It is, however, necessary that the product under test produce conforming messages when requested to do so and that the content of those messages remain consistent with the requests that produced them.

2.1.2.1 Scenarios

1. Generated an EAS Alert message containing remote resources.

2. Generated an EAS Alert message without remote resources.

2.1.2.2 Detailed Results – Test Suite 10 (OASIS CAP v1.2 Standard)

Table 3: Test Suite 10 (OASIS CAP Version 1.2 Standard Results)

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
1	The message is valid against the CAP Version 1.2 schema [OASIS CAP Version 1.2 §4.2(a); IPAWS Profile Version 1.0 §3.2(a)].	▲	▲
2■	The <identifier> element contains an indication of sender-wide uniqueness [OASIS CAP Version 1.2 <identifier> note (1)].[5]	▲	▲
3	The <identifier> element is free of spaces, commas, less than symbols, and ampersands [OASIS CAP Version 1.2 <identifier> note (2)].	▲	▲
4■	The <sender> element contains an indication of global uniqueness [OASIS CAP Version 1.2 <sender> note (1)].[6]	▲	▲
5	The <sender> element is free of spaces, commas, less than symbols, and ampersands [OASIS CAP Version 1.2 <sender> note (2)].	▲	▲
6	The <msgType> is “Alert” or “Update,” as per this scenario [OASIS CAP Version 1.2, <msgType> element].	▲	▲
7	For messages with a <scope> of “Public” or “Private,” the <restriction> element is not present [OASIS CAP Version 1.2, <restriction> note].	▲	▲

[5] For this test and each scenario, the <identifier> element included an incremental six digits identifier. In the test engineer’s opinion, this approach meets the requirements of the CAP v1.2 Standard.

[6] In the test engineer’s opinion, the <sender> element met the requirements of the CAP v1.2 Standard, as it included a unique identifier as the sender’s address.

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
8	For messages with a <scope> of "Restricted," the <restriction> element is present [OASIS CAP Version 1.2 <restriction> note].		
9	The <references> element is a space-delimited collection of triples [OASIS CAP Version 1.2 <references> notes (1) and (2)].		
10a■	The first of each triple identified in step 9 would pass the <sender> element test described in step 4 [OASIS CAP Version 1.2 <references> note (1)]. [7]		
10b	The first of each triple identified in step 9 would pass the <sender> element test described in step 5 [OASIS CAP Version 1.2 <references> note (1)].		
11a■	The second of each triple identified in step 9 would pass the <identifier> element test described in step 2 [OASIS CAP Version 1.2 <references> note (1)]. [8]		
11b	The second of each triple identified in step 9 would pass the <identifier> element tests described in step 3 [OASIS CAP Version 1.2 <references> note (1)].		
12	The third of each triple identified in step 9 meets restrictions imposed by the schema on the <sent> element [OASIS CAP Version 1.2 <references> note (1)].		

[7] In the context of this test, a "triple" is a series of three (3) data items separated by commas. The <reference> element is comprised of the sender, the identifier, and a date time stamp. In the test engineer's opinion, the triple was not applicable.

[8] In the test engineer's opinion this is the same comment as footnote 7.

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
13■	The <category> elements within a given <info> element are unique [OASIS CAP Version 1.2 <category> definition and notes (1) and (2)].[9]	▲	▲
14■	The <responseType> elements within a given <info> element are unique [OASIS CAP Version 1.2 <responseType> definition and notes (1) and (2)].[10]	●	●
15■	For messages with both <expires> and <effective> elements, the time indicated by <expires> is “after” the time indicated by <effective> element [OASIS CAP Version 1.2 <effective> and <expires> definitions].[11]	▲	▲
16■	The <web> elements contain an absolute Uniform Resource Identifier (URI) rather than a relative URI [OASIS CAP Version 1.2 <web> note].[12]	▲	▲
17■	The <mimeType> elements are actual Multipurpose Internet Mail Extensions (MIME) types as per Internet Assigned Number Authority (IANA) [OASIS CAP Version 1.2 <mimeType> note].[13]	▲	●

[9] IMTEL’s understanding of the <category> specification of CAP and IMTEL’s opinion not to tolerate duplicate <category> elements.

[10] IMTEL’s understanding of the <responseType > specification of CAP and IMTEL’s opinion not to tolerate duplicate < responseType> elements.

[11] IMTEL’s understanding of the <expires> and <effective> specifications of CAP and our interpretation of the semantics of the <effective> and <expires> elements.

[12] IMTEL’s understanding of Request for Comments (RFC) 2396.

[13] IMTEL’s understanding of RFC 2046.

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
18■	Each <size> element describes approximately size of its referenced or included resource, where “approximately” means “to within a factor of 3” [OASIS CAP Version 1.2 <size> note (1)].[14]	▲	●
19■	Each <digest> element contains a Secure Hash Algorithm 1 (SHA-1) hash of its referenced or included (and decoded) resource [OASIS CAP Version 1.2 <digest> definition].[15]	●	●
20■	Each <polygon> element contains a white-space delimited list of at least four World Geodetic System 1984 (WGS 84) coordinate pairs, the first and last of which are the same [OASIS CAP Version 1.2 <polygon> notes].[16]	●	●
21■	Each <circle> element contains a WGS 84 coordinate pair followed by a space and a radius value in kilometers [OASIS CAP Version 1.2 <circle> notes].[16]	●	●
22■	Each radius identified in the previous step is less than 10 000 kilometers (the approximate distance from pole to equator) [OASIS CAP Version 1.2 <circle> notes].[16]	●	●

[14] IMTEL’s understanding of the <size> element description of CAP.

[15] IMTEL’s understanding of Federal Information Processing Standard (FIPS) 180-2 and the assumption that SHA-1 digests are rendered as 40 American Standard Code for Information Interchange (ASCII) characters in big-endian hex, as in FIPS 180-2, but without any spaces.

[16] IMTEL’s understanding of WGS 84.

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
23■	The <areaDesc> element matches any Specific Area Message Encoding (SAME), FIPS, and/or Zone Improvement Plan (ZIP) values inside <geocode> elements [OASIS CAP Version 1.2 <geocode> notes].[17]	▲	▲
24■	The value of each <altitude> element is at least -20 000 000 feet (the "depth" of the center of the Earth) and not more than 180 000 feet (the approximate extent of the stratosphere) [OASIS CAP Version 1.2 <altitude> note (2)].[18]	●	●
25a■	For each <ceiling> element, there is a corresponding <altitude> element [OASIS CAP Version 1.2 <ceiling> notes].[18]	●	●
25b■	For each <ceiling> element is not less than the value of the corresponding <altitude> element and not more than 180 000 feet (the approximate extent of the stratosphere) [OASIS CAP Version 1.2 <ceiling> notes].[18]	●	●

[17] IMTEL's understanding of National Institute of Standards and Technology (NIST) FIPS (http://www.itl.nist.gov/fipspubs/fip6-4.htm), SAME (http://www.weather.gov/nwr/nwrsame.htm), and ZIP Code value (http://zip4.usps.com/zip4/citytown_zip.jsp).

[18] IMTEL's understanding of CAP.

2.1.2.3 Detailed Results – Test Suite 11 (OASIS CAP v. 1.2 USA IPAWS Profile Version 1.0)

Table 4: Test Suite 11 (OASIS CAP 1.2 USA IPAWS Profile Version 1.0 Results)

Legend:	Meets requirements (Pass) Does not meet requirements (Fail) No Rating or Not Applicable (NA) to the scenario		
Test Number	**Test Criterion**	**Scenario 1 Result**	**Scenario 2 Result**
1	At least one <info> element exists [IPAWS Profile Version 1.0 <info> specification].	▲	▲
2	The <status> element is “Actual” [IPAWS Profile Version 1.0 <status> specification].	▲	▲
3	At least one <code> element contains the case- and space- sensitive string “IPAWSv1.0” [OASIS CAP Version 1.2 <code> notes; IPAWS Profile Version 1.0 <code> specification].	▲	▲
4	Each <info> element contains at least one <area> element [IPAWS Profile Version 1.0 <area> specification].	▲	▲
5	Each <info> element contains the same <category> and <eventCode> elements [IPAWS Profile Version 1.0 <info> specification (1)].	▲	▲
6■	Each <info> element contains exactly one <eventCode> element whose <valueName> element is “SAME,” and that the corresponding <value> element is a SAME-standard-three-letter value [IPAWS Profile Version 1.0 <info> specification (2), <eventCode> specifications (2) and (3)].[19]	▲	▲
7	Each <info> element contains an <expires> element [IPAWS Profile Version 1.0 <expires> specification].	▲	▲

[19] IMTEL’s understanding of CFR 47 §11.31(e).

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

Test Number	Test Criterion	Scenario 1 Result	Scenario 2 Result
8■	The <description> element contains a meaningful value [IPAWS Profile Version 1.0 <description> specification]. [20]	●	●
9■	The <instruction> element contains a meaningful value [IPAWS Profile Version 1.0 <instruction> specification]. [21]	●	●
10■	Each <info> element contains a <parameter> element whose <valueName> element is “EAS-ORG” and whose <value> element is the originator's SAME organization code [first IPAWS Profile Version 1.0 <parameter> specification].[19]	▲	▲
11	At least one <resourceDesc> element has a case-sensitive value of “EAS Broadcast Content” [IPAWS Profile Version 1.0 <resourceDesc> specification (1) and note (1)].	▲	●
12*	For each <resource> element whose <resourceDesc> is “EAS Broadcast Content,” the <mimeType> element contains one of “audio/x-ipaws-audio,” “audio/x-ipaws-streaming- audio,” “video/x-ipaws-video,” or “video/x-ipaws-streaming-video” [IPAWS Profile Version 1.0 <mimeType> specification].	▲	●
13■	At least one SAME code (5- or 6-digit extended FIPS code) occurs [IPAWS Profile Version 1.0 <geocode> specification].[22]	▲	▲

[20] IMTEL’s understanding of the <description> element description of CAP. For each scenario, the product produced text based on the test engineer’s input.

[21] IMTEL’s understanding of the <instruction> element description of CAP.

[22] IMTEL’s understanding NIST FIPS Publications 6-4, http://www.itl.gov/fipspubs/fip6-4.html.

2.2 Summarized Test Results

Table 5: Test Results – CAP Message Originator

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.	▲	See section 2.1.1.1 for Detailed Results.
Message Producer Test Suite 10	Verify that messages produced by the product conform to OASIS CAP Version 1.2 Standard.	▲	Some components of Test Suite 10 are based on the engineer's opinion and are described in section 2.1.2.2.
Message Producer Test Suite 11	Verify that messages produced by the product conform to the OASIS CAP 1.2 USA IPAWS Profile Version 1.0.	▲	Some components of Test Suite 11 are based on the engineer's opinion and are described in section 2.1.2.3.

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 6: Additional Observations

Test Suite	Test Number	Observation
10	4	The product was assigned a private IP address on the IPAWS CA network environment. Within the bounds of the IPAWS CA test environment, the <sender> element was globally unique. The IP address may not be unique with regards to another similar environment.
10	9, 10a, 10b, 11a, 11b	Test engineer noted no <references> elements.

Test Suite	Test Number	Observation
10	13	Test engineer noted only one <category> element.
10	14	Test engineer noted no <responseType> element.
10	16	Test engineer noted that whatever was input was accepted into the <web> element.
10	17, 18	Test engineer noted no <resource> elements.
10	20, 21, 22, 24, 25a, 25b	Test engineer noted no physical location in message.
11	11	Test engineer noted no <resourceDesc> element.
11	12	Test engineer noted no <resource> element.

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

13. Internet Engineering Task Force (IETF) Request for Comments (RFC), http://www.ietf.org/

14. Zone Improvement Plan (ZIP), http://zip4.usps.com/zip4/citytown_zip.jsp

4.0 Appendix B: List of Acronyms

A2LA	American Association for Laboratory Accreditation
ASCII	American Standard Code for Information Interchange
CA	Conformity Assessment
CAP	Common Alerting Protocol
CFR	Code of Federal Regulations
Comlabs	Communications 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
IANA	Internet Assigned Number Authority
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
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

NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
RFC	Request For Comments
SAIC	Science Applications International Corporation
SAME	Specific Area Message Encoding
SHA-1	Secure Hash Algorithm 1
TR	Test Report
URI	Uniform Resource Identifier
USA	United States of America
WGS 84	World Geodetic System 1984
XML	Extensible Markup Language
ZIP	Zone Improvement Plan