ATIS-0700022

CMAS Supplemental Information Retrieval Interface Testing Specification

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0700022, *CMAS Supplemental Information Retrieval Interface Testing Specification*

Is an American National Standard developed by the **Wireless Technologies and Systems Committee (WTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700022

CMAS Supplemental Information Retrieval Interface Testing Specification

Alliance for Telecommunications Industry Solutions

Approved September 2015

Abstract

This Standard defines the operational testing procedures for the CMAS Supplemental Information Retrieval between the Commercial Mobile Service Provider (CMSP) Gateway and the Federal Alert Gateway the over the Reference Point “C” Interface.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word SHALL and recommendations by the word SHOULD. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word May denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, WTSC, which was responsible for its development, had the following leadership:

M. Younge, WTSC Chair (T-Mobile)

D. Zelmer, WTSC Vice-Chair (AT&T)

P. Musgrove, WTSC SN Chair (AT&T)

G. Schumacher, WTSC SN Vice-Chair (Sprint)

P. Sanders, Technical Editor (One2Many)

The **Systems and Networks (SN)** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Tables

ATIS Standard on:

CMAS Supplemental Information Retrieval Interface Testing Specification

1 Scope, Purpose, & Application

1.1 Scope

This Standard defines operational testing procedures for the Retrieval of Supplementary Information Retrieval procedure between the Commercial Mobile Service Provider (CMSP) Gateway and the Federal Alert Gateway and over the C-Interface.

The present Standard should be regarded as a supplement to the *Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Test Specification* [Ref 2] and adds a test case for Spanish text message retrieval only.

1.2 Purpose

The purpose of interface testing is to evaluate whether systems or components transmit data and control information correctly to each other.

Specifically, the present *ATIS CMAS Supplemental Information Retrieval Interface Testing Specification* defines a set of tests to verify the following minimal set of functionality during interface and regression testing:

- Ability to perform Spanish text message retrieval.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] J-STD-101, *Joint ATIS/TIA CMAS Alert Gateway to CMSP Gateway Interface Specification*; October, 2009 including J-STD-101.a, *Supplement A to J-STD-101, Joint ATIS/TIA CMAS Alert Gateway to CMSP Gateway Interface Specification*; August 2011 and including J-STD-101.b, *Supplement B to J-STD-101, Joint ATIS/TIA CMAS Alert Gateway to CMSP Gateway Interface Specification*; December 2012.[1]

[Ref 2] J-STD-102, *Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Test Specification*; January, 2011 including J-STD-102.a, *Supplement A to J-STD-102, Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Test Specification*; December, 2012.[2]

[Ref 3] ATIS-0700012.v002, *Implementation Guidelines for CMAS Supplemental Information Retrieval*; *Revision 2*.[3]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) < https://www.atis.org/docstore/product.aspx?id=24919 >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) < https://www.atis.org/docstore/product.aspx?id=25515 >.

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) < https://www.atis.org/docstore/product.aspx?id=26126 >.

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

3.1.1 Commercial Mobile Service Provider: A Commercial Mobile Service Provider (or CMS Provider) is an FCC licensee providing commercial mobile service as defined in section 332 (d)(1) of the Communications Act of 1934 (47 U.S.C. 332(d)(1)). Section 332(d)(1) defines the term commercial mobile service as any mobile service (as defined in 47 U.S.C. 153) that is provided for profit and makes interconnected service available: (a) to the public; or (b) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Federal Communications Commission.

3.1.2 CMSP Gateway: A CMSP administered system, identified by a unique IP address or Fully Qualified Domain Name (FQDN), interfacing to the Federal Alert Gateway and exchanging information per this Standard.

3.1.3 Operational Testing: Operational testing is the field test, under realistic conditions, of any system or component, for determining that system or component's overall effectiveness and suitability for use before field trials or general usage of the system or component. Operational testing provides information for the overall assessment of how well a system will provide the desired capability when operated by typical users in the expected environment.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
CAP	Common Alerting Protocol
CMAC	Commercial Mobile Alert for C Interface
CMAS	Commercial Mobile Alert System
CMSP	Commercial Mobile Service Provider
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
XML	eXtensible Markup Language

4 Testing Methodology & Environment

The execution of the test procedure as described in the present Testing Specification is assumed to be preceded by the testing procedure as described in J-STD-102, *Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Test Specification* [Ref 2], and therefore assumes the environment as described in that Specification to be available.

Before the execution of the Test Cases in this Standard, the following configuration needs to be verfied:

- The Federal Alert Gateway supports generating Spanish text messages.
- The CMSP Gateway supports retrieval of Spanish text messages.

5 Test Case

This clause contains the test case for messages and conditions for inter-gateway tests for Spanish text retrieval. The test case contains the following components:

- General description of the test case.
- Definition of the items to be tested by the test case.
- Notes relative to the test case environment or execution.

- Identification of any test tools required for the execution of the test case.
- Identification of any assumed capabilities required by either the Federal Alert Gateway or the CMSP Gateway for the execution of the test case.
- Identification of the test personnel required for the execution of the test case.
- Identification of the requirements from the *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification* [Ref 1] which are verified by the test case.
- Identification of any required prerequisite conditions which are required by the test case.
- Test case steps including references to the appropriate messages and expected message contents as defined in Annex A, *Input CAP Messages*; Annex B, *Expected CMAC Messages*; and Annex C, *Expected ACK Messages*.

5.1 Inter-Gateway Test Case

This clause defines the test case between the Federal Gateway and the CMSP Gateway across the Reference Point "C" interface. This clause contains the following inter-gateway test case:

- CMAS-TC-S1 test case when the Federal Gateway notifies the CMSP Gateway that Spanish text is available.

5.1.1 CMAS-TC-S1 – Spanish Text Message Retrieval Test

The purpose of the Spanish Text Message Retrieval Test procedure (CMAS-TC-S1) is to test sending the Spanish Text Message Retrieval request and response messages. The procedure will test transmission of the Spanish Text Message Retrieval request message from the CMSP Gateway and the delivery of the requested Spanish Text Message by the Federal Alert Gateway.

5.1.1.1 Items to Be Tested

The following CMAS entities are to be tested with this test procedure:

- Federal Alert Gateway.
- CMSP Gateway.

5.1.1.2 Notes

The following test procedure tests the interface between a Federal Alert Gateway and a CMSP Gateway. Each test step is labeled to indicate which test personnel takes the required actions for that step.

5.1.1.3 Test Tools

The following test tools will be used to complete this test procedure:

- Alert Origination Simulator.

5.1.1.4 Test Capabilities

The following capabilities will be necessary to complete this test procedure. Test capabilities are specified for both the Federal Alert Gateway and CMSP Gateway.

- Federal Alert Gateway Test Capabilities:
    - Ability to display message logs.

  - Ability to display messages in “raw” XML format.

- CMSP Gateway Test Capabilities:
  - Ability to accept Spanish Text Message Retrieval request command from user.
  - Ability to display message logs.
  - Ability to display messages in “raw” XML format.

5.1.1.5 Test Personnel

Test personnel in the following roles will conduct various test steps as part of this test procedure:

- Federal Test Support.
- CMSP Test Support.

5.1.1.6 Requirements Addressed

There is no requirement number associated with the Supplemental Information Retrieval message and call flow in the *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification* [Ref 1].

5.1.1.7 Prerequisites Conditions

- The Federal Alert Gateway and CMSP Gateway have an established IPsec tunnel and TCP connection.
- The Federal Alert Gateway is not in a Transmission Control Cease status with respect to the CMSP Gateway being tested (e.g., receiving Transmission Control-Cease messages from the CMSP Gateway).
- The Federal Alert Gateway and CMSP Gateway have passed testing for General Connectivity (CMAS-TC-008 or CMAS-TC-009, see J-STD-102 [Ref 2]).
- The CMSP Gateway has been provisioned to retrieve the Spanish Text Message either automatically following a reception of a CMAC message from the Federal Alert Gateway (alert, update, or cancel) or manually by the CMSP Test Support.

5.1.1.8 Test Steps

The following table defines the individual test steps that are performed sequentially to complete the test procedure.

> NOTE: Element values in the Expected Results column that are dependent on the actual test execution are specified with variables, such as [CMAC Sent Date-Time] and are indicated with brackets. Further discussion is provided in Annex B, *Input CAP Messages*; Annex C, *Expected CMAC Messages*; and Annex D, *Expected ACK Messages*.

Table 5.1 – Steps for Test Case CMAS-TC-S1 – Spanish Text Message Retrieval Test

STEP #	ACTION PERFORMED:	EXPECTED RESULTS	RQMT ID (JCMAS-C-RQMT #)	STEP COMPLETION (PASS, FAIL, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send A.1 CAP Message "Imminent Threat Alert" #1 (Annex A, *Input CAP Messages*) to the Federal Alert Gateway, which includes both English and Spanish text.	NOTE: The Federal Alert Gateway transmits the B.1 CMAC message #1 "Imminent Threat Alert" (Annex B, *Expected CMAC message*) with English text and includes the CMAC_note element with the indication that Spanish text is available to the CMSP Gateway and the CMSP Gateway responds with a C.1 Ack Message #1 (Annex C, *Expected Ack message)*. The Federal Alert Gateway stores the Spanish text for retrieval by the CMSP Gateway.	N/A	N/A
2	**CMSP Test Support:** The CMSP Gateway sends an HTTP GET with the URI provided in the CMAC_note element.	NOTE: The Federal Alert Gateway responds with an HTTP response.	N/A	N/A
3	**CMSP Test Support:** View CMSP Gateway message log.	The log file shows the sending of HTTP GET with the URI provided in the CMAC_note element identifying the location of the Spanish Text Message.	N/A	
4	**CMSP Test Support:** View CMSP Gateway message log.	Verify that the message body of the received message conforms to the XML schema as shown in Annex D.	N/A	

Annex A Input CAP Message

(normative)

The following CAP message is to be used in the test procedures. The included elements are required in CAP, but are not necessarily used in this test case. Some of the element values are default or sample values. The elements and element values that are relevant to the test procedures are indicated with blue text. Some of the element values, such as <sent> time, are dependent on the actual test execution. These element values are specified with variables, such as [CAP Sent Date-Time] and are indicated with brackets and red text.

A.1 CAP Message #1 – Imminent Threat Alert

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:emergency:cap:1.2">
    <identifier>[CAP Message ID 1]</identifier>
    <sender>[Message Sender 1]</sender>
    <sent>[CAP Sent Date-Time 1]</sent>
    <status>Actual</status>
    <msgType>Alert</msgType>
    <source/>
    <scope>Public</scope>
    <restriction/>
    <addresses> 200004</addresses>
    <code>IPAWSv1.0</code>
    <addresses> 200004</addresses>
    <references/>
    <incidents/>
    <info>
      <language>en-US</language>
      <category>Safety</category>
      <event>Immediate Evacuation Warning</event>
      <responseType>Evacuate</responseType>
      <urgency>Immediate</urgency>
      <severity>Extreme</severity>
      <certainty>Observed</certainty>
      <audience/>
      <eventCode>
         <valueName>SAME</valueName>
         <value>EVI</value>
      </eventCode>
      <expires>[Expires Date-Time 1]</expires>
      <senderName>NYC_OEM</senderName>
      <headline>TEST Mandatory Evacuation Zone A</headline>
      <description>TEST Mandatory Evacuation Zone A</description>
      <instruction/>
      <contact>Phone:123-456-7890 Cell:123-456-7890 E-mail:jdoe@oem.nyc.gov</contact>
      <parameter>
         <valueName>CMAMtext</valueName>
         <value>[English Text Message 1]</value>
       </parameter>
       <area>
          <areaDesc>Citywide</areaDesc>
          <geocode>
            <valueName>SAME</valueName>
            <value>036005</value>
          </geocode>
          <geocode>
            <valueName>SAME</valueName>
            <value>036047</value>
```

```
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036061</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036081</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036085</value>
        </geocode>
      </area>
   </info>
   <info>
       <language>es-US</language>
       <category>Safety</category>
      <event>Immediate Evacuation Warning</event>
      <responseType>Evacuate</responseType>
      <urgency>Immediate</urgency>
      <severity>Extreme</severity>
      <certainty>Observed</certainty>
      <audience/>
      <eventCode>
         <valueName>SAME</valueName>
         <value>EVI</value>
      </eventCode>
      <expires>[Expires Date-Time 1]</expires>
      <senderName>NYC_OEM</senderName>
      <headline>TEST EVACUACION OBLIGATORIA Zone A</headline>
      <description>TEST EVACUACION OBLIGATORIA Zone A</description>
      <instruction/>
      <contact>Phone:123-456-7890 Cell:123-456-7890 E-mail:jdoe@oem.nyc.gov</contact>
      <parameter>
        <valueName>CMAMtext</valueName>
        <value>[Spanish Text Message 1]</value>
      </parameter>
      <area>
        <areaDesc>Citywide</areaDesc>
        <geocode>
          <valueName>SAME</valueName>
          <value>036005</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036047</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036061</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036081</value>
        </geocode>
        <geocode>
          <valueName>SAME</valueName>
          <value>036085</value>
        </geocode>
      </area>
   </info>
</alert>
```

Annex B Expected CMAC Message

(normative)

The following message is the expected CMAC message that results from executing test cases in clause 5. Some of the element values are based on default or sample values from the CAP message in Annex A, *Input CAP Message*. The elements and element values that are relevant to the expected results in the test procedures are indicated with blue text. Some of the element values, such as the <CMAC_sent_date_time> value, are dependent on the actual test execution. These element values are specified with variables, such as [CMAC Sent Date-Time] and are indicated with brackets and red text.

B.1 CMAC Message #1 – Imminent Threat Alert (Expected Result of CAP Message #1)

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns="cmac:1.0">
  <CMAC_protocol_version>1.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 1]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 1]</CMAC_message_number>
  <CMAC_referenced_message_cap_identifier/>
  <CMAC_sender>[Message Sender 1]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 1]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_response_code>Evacuate</CMAC_response_code>
  <CMAC_note>SPANISH [URI]</CMAC_note>
  <CMAC_cap_alert_uri>[Message URI 1]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 1]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 1]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
      <CMAC_category>Safety</CMAC_category>
      <CMAC_event_code>EVI</CMAC_event_code>
       <CMAC_response_type>Evacuate</CMAC_response_type>
      <CMAC_severity>Extreme</CMAC_severity>
      <CMAC_urgency>Immediate</CMAC_urgency>
      <CMAC_certainty>Observed</CMAC_certainty>
      <CMAC_expires_date_time>[Expires Date-Time 1]</CMAC_expires_date_time>
       <CMAC_sender_name>NYC_OEM</CMAC_sender_name>
      <CMAC_text_language>English</CMAC_text_language>
      <CMAC_text_alert_message_length>[English Text Message Length 1]
         </CMAC_text_alert_message_length>
      <CMAC_text_alert_message>[English Text Message 1]</CMAC_text_alert_message>
      <CMAC_Alert_Area>
         <CMAC_area_description>FAIRFAX COUNTY IN VIRGINIA</CMAC_area_description>
         <CMAC_cmas_geocode>36005</CMAC_cmas_geocode>
         <CMAC_cmas_geocode>36047</CMAC_cmas_geocode>
         <CMAC_cmas_geocode>36061</CMAC_cmas_geocode>
         <CMAC_cmas_geocode>36081</CMAC_cmas_geocode>
         <CMAC_cmas_geocode>36085</CMAC_cmas_geocode>
         <CMAC_cap_geocode>
            <valueName>SAME</valueName>
            <value>036005</value>
         </CMAC_cap_geocode>
         <CMAC_cap_geocode>
            <valueName>SAME</valueName>
            <value>036047</value>
         </CMAC_cap_geocode>
         <CMAC_cap_geocode>
            <valueName>SAME</valueName>
            <value>036061</value>
         </CMAC_cap_geocode>
```

```
            <CMAC_cap_geocode>
               <valueName>SAME</valueName>
               <value>036081</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
               <valueName>SAME</valueName>
               <value>036085</value>
            </CMAC_cap_geocode>
         </CMAC_Alert_Area>
      </CMAC_alert_info>
      <CMAC_Digital_Signature>[Digital Signature 1]</CMAC_Digital_Signature>
   </CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #1 of the logged CMAC message:

Table B.1 – CMAC Message #1 Expected Messages & Values

CMAC ELEMENT	VALUE
<CMAC_protocol_version>	“1.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 1]
<CMAC_message_number>	[CMAC Message Number 1]
<CMAC_sender>	[Message Sender 1] from CAP Message #1
<CMAC_sent_date_time>	[CMAC Sent Date-Time 1] in UTC in XML dateTime format
<CMAC_status>	“Actual”
<CMAC_message_type>	“Alert”
<CMAC_cap_alert_uri>	[Message URI 1]
<CMAC_cap_identifier>	[CAP Message ID 1] from CAP Message #1
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 1] from CAP Message #1
<CMAC_category>	“Met”
<CMAC_event_code>	“SVR”
<CMAC_severity>	“Severe”
<CMAC_urgency>	“Immediate”
<CMAC_certainty>	“Observed”
<CMAC_expires_date_time>	[Expires Date-Time 1] from CAP Message #1 in UTC in XML dateTime format
<CMAC_text_language>	“English”
<CMAC_text_alert_message_length>	[Text Message Length 1] equal to the number of characters in <CMAC_text_alert_message> value
<CMAC_text_alert_message>	[Text Message 1] not exceeding 90 English characters
<CMAC_area_description>	FAIRFAX COUNTY IN VIRGINIA
<CMAC_cmas_geocode>	51059

Annex C Expected ACK Message

(normative)

The following message is the expected CMAC Ack message sent by the CMSP Gateway in response to the CMAC Alert message in Annex B, *Expected CMAC Message*. Some of the element values are based on default or sample values from the CMAC messages. The elements and element values that are relevant to the expected results in the test procedures are indicated with blue text. Some of the element values, such as the <CMAC_sent_date_time> value, are dependent on the actual test execution. These element values are specified with variables, such as [CMAC Sent Date-Time] and are indicated with brackets and red text.

C.1 Ack Message #1 (Expected Result of CMAC Message #1)

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="cmac:1.0">
   <CMAC_protocol_version>1.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>[CMSP Gateway ID 1]</CMAC_sending_gateway_id>
   <CMAC_message_number>[CMAC Ack Message Number 1]</CMAC_message_number>
   <CMAC_referenced_message_number>[CMAC Message Number 1]
      </CMAC_referenced_message_number>
   <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 1]</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Ack</CMAC_message_type>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of Ack Message #1 of the logged CMAC message:

Table C.1 – Ack Message #1 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	"1.0"
<CMAC_sending_gateway_id>	[CMSP Gateway ID 1]
<CMAC_message_number>	[CMAC Ack Message Number 1]
<CMAC_referenced_message_number>	[CMAC Message Number 1] from CMAC Message #1
<CMAC_sent_date_time>	[CMAC Ack Sent Date-Time 1] in UTC in XML dateTime format
<CMAC_status>	"System"
<CMAC_message_type>	"Ack"

Annex D Expected CMAC Supplemental Information Message

(normative)

The following message is the expected CMAC Supplemental Information message that results from executing test cases in clause 5. Some of the element values are based on default or sample values from the CAP message in Annex A, *Input CAP Message*. The elements and element values that are relevant to the expected results in the test procedures are indicated with blue text. Some of the element values, such as the <CMAC_sent_date_time> value, are dependent on the actual test execution. These element values are specified with variables, such as [CMAC Sent Date-Time] and are indicated with brackets and red text.

D.1 CMAC Supplemental Information Message #1 – Spanish Text (Expected Result of HTTP Get message after CMAC Message #1)

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAS_Supplemental_Information xmlns = "cmas:1.0">
   <CMAC_message_number>[CMAC Supplemental Information Message Number 1]
         </CMAC_message_number>
   <CMAC_supplemental_text_language>Spanish</CMAC_supplemental_text_language>
   <CMAC_supplemental_text_alert_message_length>[Spanish Text Message Length
1]</CMAC_supplemental_text_alert_message_length>
   <CMAC_supplemental_text_alert_message>[Spanish Text Message
1]</CMAC_supplemental_text_alert_message>
</CMAS_Supplemental_Information>
```

The following table contains the expected message elements and values of the CMAC Supplemental Information Message #1 of the logged CMAC Supplemental Information message:

Table D.1 – CMAC Supplemental Information Message #1 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	"1.0"
<CMAC_message_number>	[CMAC Message Number 1]
CMAC_supplemental_text_language	"Spanish"
<CMAC_supplemental_text_alert_message_length>	[Text Message Length 1] equal to the number of characters in <CMAC_supplemental_text_alert_message> value
<CMAC_supplemental_text_alert_message>	[Text Message 1] not exceeding 150 Spanish characters