ATIS STANDARD

ATIS-0700038.v003

ATIS Standard on -

Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test Specification

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, 5G, 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 the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

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 NOR 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 https://www.atis.org/policy/patent-assurances/ 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.

Published by

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

Copyright © 2022 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

ATIS-0700038.v003

ATIS Standard on

Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test Specification

Alliance for Telecommunications Industry Solutions

Approved March 2, 2022

Abstract

This Standard defines the testing of the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for WEA alerts based upon the requirements in ATIS-0700037, *Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification*.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, 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 USA)

T. Brooks, WTSC SN Chair (T-Mobile USA)

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

P. Sanders, Technical Editor (one2many)

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

Table of Contents

Table of Figures

Table of Tables

ATIS STANDARD **ATIS-0700038.v003**

ATIS Standard on –

Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test Specification

Preface

The authority-to-individual emergency alerting capability to mobile devices was originally called Commercial Mobile Alert System (CMAS) in the first three Reports and Orders from the Federal Communications Commission (FCC). This standard was originally developed based upon the CMAS terminology and CMAS was operational in April 2012. However, in February 2013, the FCC renamed Commercial Mobile Alert System (CMAS) to Wireless Emergency Alerts (WEA) with associated updates to the appropriate sections of Part 11 of the 47 CFR. Subsequently, the FCC has issued additional enhancements and rules for this government-to-individual emergency alerting capability to mobile devices, and these are identified as modifications to WEA.

Consequently, this specification may use both the term CMAS and the term WEA. These terms should be considered as equivalent terms, with WEA being the preferred term.

This specification contains references to the uniquely numbered requirements in ATIS-0700037 [Ref 1]. Any requirements which have been added, modified, or deleted from the eWEA version of the C-Interface specification will have suffixes applied to their requirement numbers. Any new requirements will have a suffix of R3A in the format of [WEA-C-RQMT-nnnn$_{\text{R3A}}$]. Any modified requirements will have a suffix of R3M in the format of [WEA-C-RQMT-nnnn$_{\text{R3M}}$]. Any deleted requirements will have a suffix of R3D in the format of [WEA-C-RQMT-nnnn$_{\text{R3D}}$].

This ATIS specification is the Wireless Emergency Alert (WEA) 3.0 standard for the testing of the WEA Federal Alert Gateway to CMSP Gateway interface, and it is based upon the requirements in ATIS-0700037 [Ref 1]. This ATIS specification supersedes ATIS-0700038, *Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test Specification*. Any assumptions, requirements, and test cases from the previous version of ATIS-0700038 applicable in WEA 3.0 are included in this test specification.

The regulatory background is described in detail in the Service Description in ATIS-0700035 [Ref 100].

1 Scope, Purpose, & Application

1.1 Scope

This Standard defines operational testing procedures for the communications between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway over the C-Interface. This includes operational testing of all processing functionality within the Federal Emergency Management Agency (FEMA)-administered WEA entities and the CMSP-administered WEA entities that directly impacts communications over the C-Interface. Operational testing of all other processing within the FEMA and CMSP entities including the CMSP infrastructure is beyond the scope of this Standard.

1.2 Purpose

The purpose of interface testing is to evaluate whether systems or components transmit data and control information correctly to each other. In addition, the tests defined in this Standard may be used during regression testing when updates are made to either the Federal Alert Gateway or the CMSP Gateway.

Specifically, ATIS-0700038 [Ref 1] defines a set of tests to verify the following minimal set of functionalities during interface and regression testing:

- Ability to complete the C-Interface startup procedures.
- Ability to bring up the IP Security (IPSec) tunnel.

- Ability to bring up the Transmission Control Protocol (TCP)/Internet Protocol (IP) connection.
- Ability to receive, process, and acknowledge valid CMAS Alert, Update, Cancel, Required Monthly Test (RMT), State/Local WEA Test, and Public Safety messages.
- Ability to handle transmission control cease and resume messages.
- Ability to handle link test messages.
- Ability to perform Common Alerting Protocol (CAP) message retrieval.

This Standard is not intended to define test cases for the complete development lifecycle, nor is it intended to provide complete requirements verification or complete compliance testing. Requirements verification testing is typically performed during the unit, integration, and system testing phases and is beyond the scope of this Standard.

1.3 Application

Although FCC Part 10 rules for CMAS [Ref 2] require RMTs and periodic link testing, these rules do not require interface compliance testing. This Standard addresses interface compliance testing and may be used as part of the interconnect agreement between the FEMA-administered WEA entities and the CMSP-administered WEA entities. Such interconnect agreements are beyond the scope of this Standard.

FCC Report and Order and Further Notice of Proposed Rulemaking (FCC 21-77) [Ref 26], re-designates WEA Presidential Alerts to include alerts from both the President and from the FEMA Administrator and renames the Presidential Alert to National Alert. Protocol encoding on the C-interface however still uses the value "Presidential".

2 References

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

2.1 Normative References

[Ref 1] ATIS-0700037, *Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification*.[1]

[Ref 2] FCC 08-184, *Federal Communications Commission Third Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System*; August 7th, 2008.[2]

[Ref 3] INCITS 38-2009, *Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas*; International Committee for Information Technology Standards (INCITS).[3]

[Ref 4] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[4]

[Ref 5] IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.[4]

[Ref 6] IETF RFC 4301, *Security Architecture for the Internet Protocol*.[4]

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS). < http://www.atis.org >

[2] This document is available from the Federal Communications Commission (FCC). < http://www.fcc.gov/ >

[3] This document is available from the International Committee for Information Technology Standards (INCITS) at < https://standards.incits.org/apps/group_public/project/details.php?project_id=204 >

[4] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[Ref 7] IETF RFC 4303, *IP Encapsulating Security Payload (ESP)*.[4]

[Ref 8] IETF RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2) Protocol*.[4]

[Ref 9] FCC 08-99, *First Report and Order in the Matter of The Commercial Mobile Alert System*.[2]

[Ref 10] IETF RFC 8221, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.[4]

[Ref 11] IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPSec*.[4]

[Ref 12] IETF RFC 8017, *PKCS #1: RSA Cryptography Specifications Version 2.2*.[4]

[Ref 13] IETF RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*.[4]

[Ref 14] IETF RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*.[4]

[Ref 15] IETF RFC 7230, *Hypertext Transfer Protocol -- HTTP/1.1: Message Syntax and Routing*.[4]

[Ref 16] IETF RFC 1122, *Requirements for Internet Hosts – Communication Layers*.[4]

[Ref 17] IETF RFC 793, *Transmission Control Protocol*.[4]

[Ref 18] IETF STD 5 (RFC 791), *Internet Protocol*.[4]

[Ref 19] IETF STD 5 (RFC 792), *Internet Control Message Protocol*.[4]

[Ref 20] IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*.[4]

[Ref 21] IETF RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*.[4]

[Ref 22] IETF RFC 4291, *IP Version 6 Addressing Architecture*.[4]

[Ref 23] Void

[Ref 24] Federal Information Processing Standards Publication 180-3, *Secure Hash Standard; National Institute of Standards and Technology (NIST)*.[5]

[Ref 25] National Weather Service Instruction 10-1712, *Operations and Services Dissemination Policy NWSPD 10-17 NOAA Weather Radio (NWR) All Hazards Specific Area Message Encoding (SAME)*.[6]

[Ref 26] FCC 21-77, *Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking in the Matter of Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System;* June 17, 2021.[2]

2.2 Informative References

[Ref 100] ATIS-0700035, *Wireless Emergency Alert (WEA) 3.0 Service Description*.[1]

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

Analysis Verification Method: This is a method in which hardware or software designs are compared with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements.

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;

[5] This document is available from the National Institute of Technology and Standards (NIST). < http://www.nist.gov/aes >

[6] This document is available from the National Weather Service. < http://www.weather.gov/ >

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.

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.

CMSP Gateway Group: A CMSP Gateway Group is the set of CMSP Gateways whose IP addresses or Fully Qualified Domain Name (FQDN) are visible to the Federal Alert Gateway across the Reference Point "C" interface. A CMSP Gateway Group will consist of one or two CMSP Gateways.

Demonstration Verification Method: This is a method in which qualitative determination of properties is made for a configuration item, including software and/or the use of technical data and documentation. The items being verified are observed, but not quantitatively measured, in a dynamic state.

Inspection Verification Method: This method is used to determine compliance without using special laboratory equipment, procedures, or services and consists of a nondestructive static-state examination of hardware, software, and/or technical data and documentation.

Operational Testing: Operational testing is the field test, under realistic conditions, of any system or component, for determining that system or components' 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.

Test Verification Method: This is a method in which performance is measured before, during, or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance. The process uses standardized laboratory equipment, procedures, and/or services.

3.2 Acronyms & Abbreviations

AMBER	America's Missing: Broadcast Emergency Response
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
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIFO	First In-First Out
FIPS[7]	Federal Information Processing Series - or - Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
HTTP	HyperText Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
RMT	Required Monthly Test
SA	Security Association
SAME	Specific Area Message Encoding
TCP	Transmission Control Protocol

[7] In the context of identifiers of states, counties, and county equivalents, FIPS means "Federal Information Processing Series". In the context of NIST standards, FIPS means "Federal Information Processing Standard".

UTC	Coordinated Universal Time
WEA	Wireless Emergency Alert
WTSC	Wireless Technologies and Systems Committee
XML	eXtensible Markup Language

4 Testing Methodology & Environment

This clause defines the methodology and environment that will be used for the C-Interface testing. The following topics are described in this clause:

- Test environment architecture
- Test tools
- Test support personnel

NOTE: It is important that all test personnel (Federal and CMSP) take all necessary steps to ensure that any test CAP and Commercial Mobile Alert for C Interface (CMAC) messages generated as part of this specification are only sent to CMSP Alert Gateways being tested and are not generated or sent in any manner that could allow them to inadvertently be directly or indirectly transmitted to operating CMSP Alert Gateways or distributed to the public.

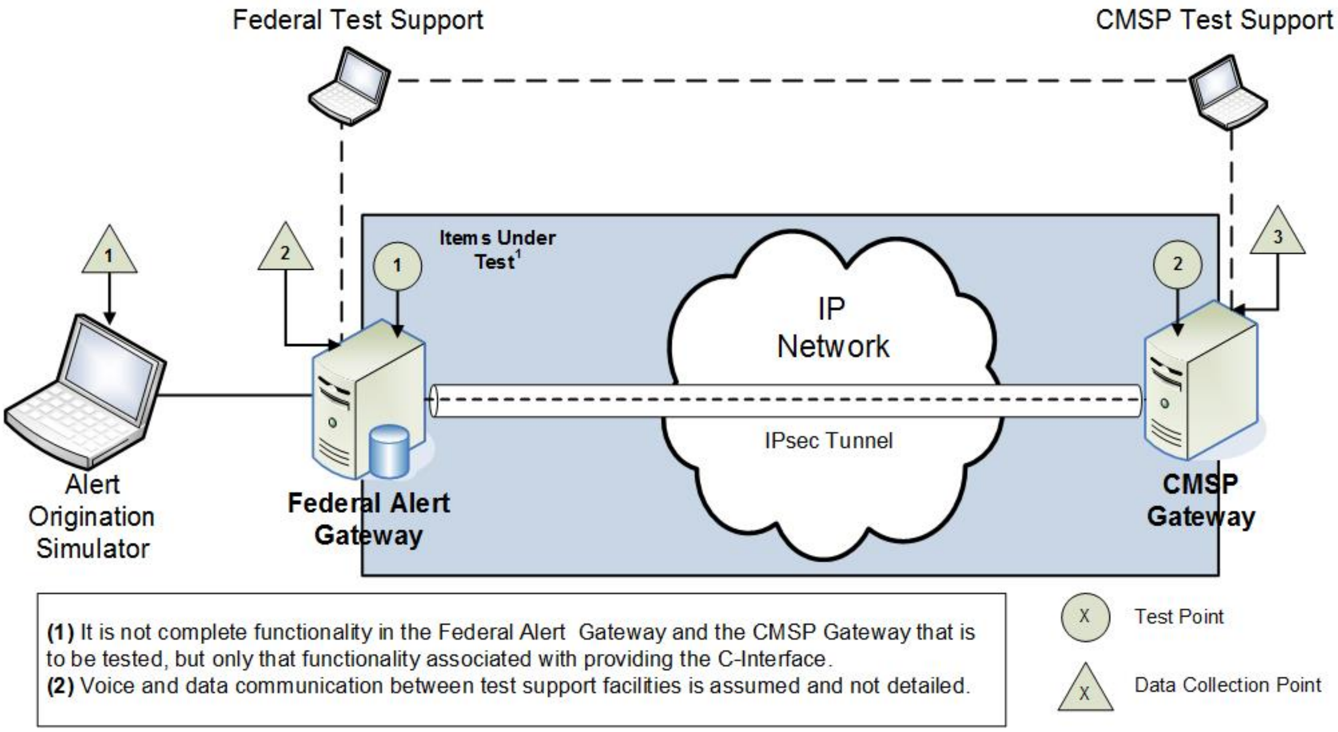
4.1 Test Environment Architecture

The following figures depict the architecture for CMAS C-Interface testing for both a single CMSP Gateway configuration and a dual CMSP Gateway configuration. The Federal Alert Gateway and the CMSP Gateways are connected via the C-Interface over an IP network. CAP input to the Federal Alert Gateway is provided by an Alert Origination Simulator (see 4.2, *Test Tools*). Test Support personnel are required at both Federal Alert Gateway and CMSP Gateway facilities. The roles and functions of the Test Support personnel are defined in Clause 4.3, *Test Personnel*.

The following figures identify *Data Collection Points* and *Test Points* which are defined as follows:

- *Test Point:* Points of interest that are used to support testing and belong to the system under test.
- *Data Collection Point:* Points of interest that are used to support testing but outside of the system under test.

The following figure depicts the test architecture for a CMSP Gateway configuration:



(1) It is not complete functionality in the Federal Alert Gateway and the CMSP Gateway that is to be tested, but only that functionality associated with providing the C-Interface.
(2) Voice and data communication between test support facilities is assumed and not detailed.

Figure 4.1: C-Interface Test Architecture for Single CMSP Gateway

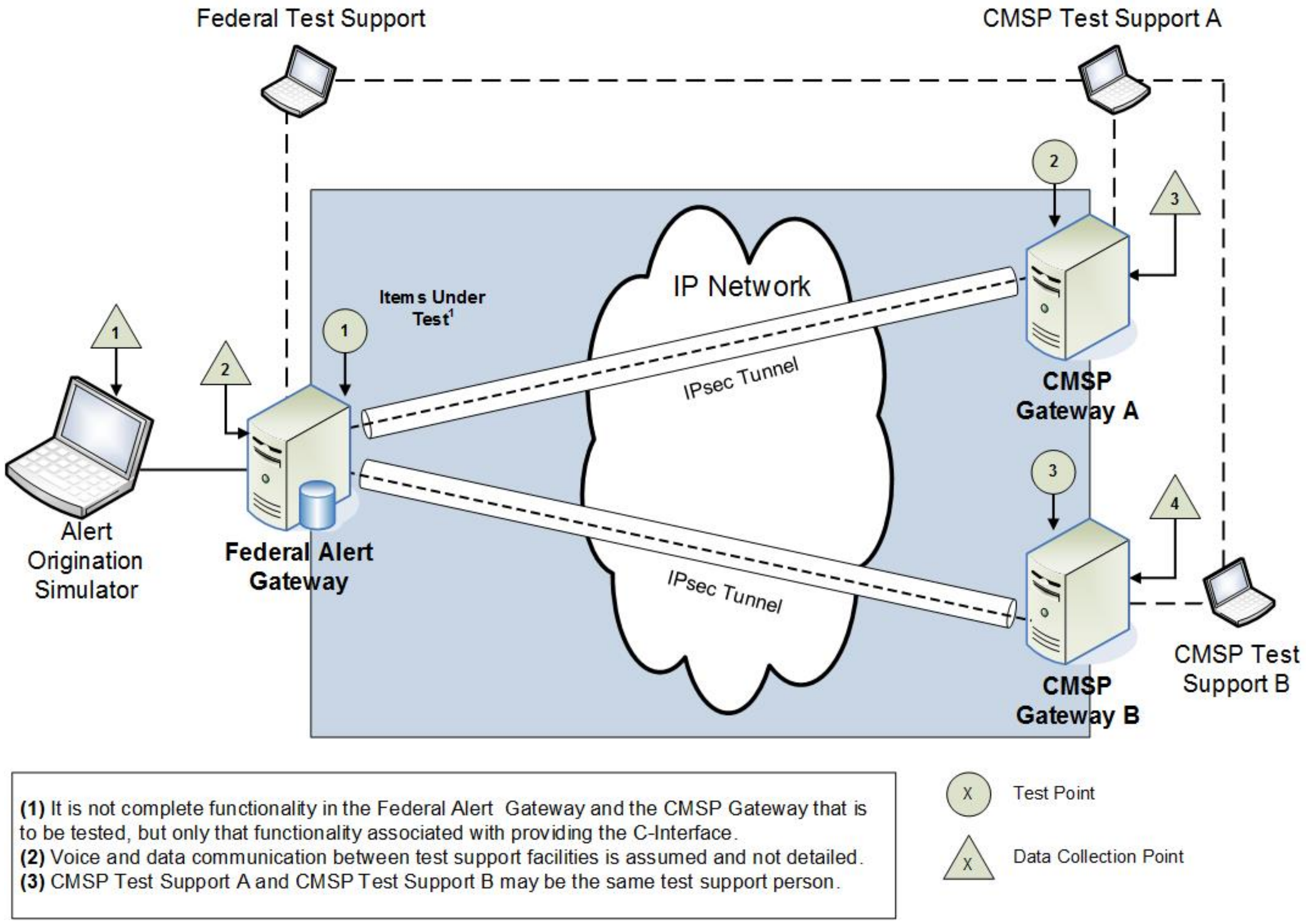
The above figure shows the following two Test Points:

1. Federal Alert Gateway
2. CMSP Gateway.

The above figure shows the following three Data Collection Points:

1. Alert Origination Simulator
2. Federal Alert Gateway
3. CMSP Gateway.

The following figure depicts the test architecture for dual CMSP Gateways configuration:



(1) It is not complete functionality in the Federal Alert Gateway and the CMSP Gateway that is to be tested, but only that functionality associated with providing the C-Interface.
(2) Voice and data communication between test support facilities is assumed and not detailed.
(3) CMSP Test Support A and CMSP Test Support B may be the same test support person.

Figure 4.2: C-Interface Test Architecture for Dual CMSP Gateways

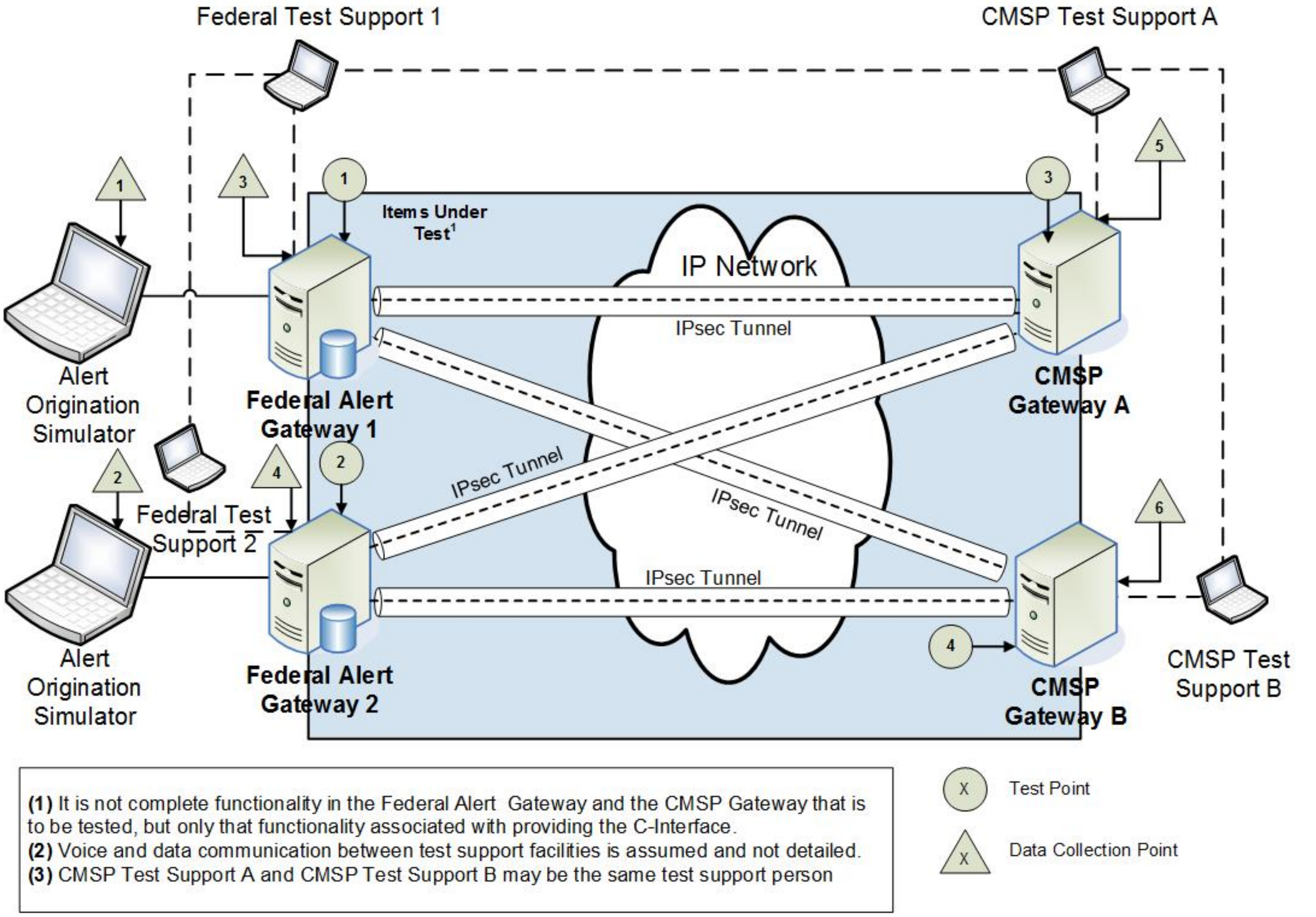
The above figure shows the following three Test Points:

1. Federal Alert Gateway
2. CMSP Gateway A
3. CMSP Gateway B.

The above figure shows the following four Data Collection Points:

1. Alert Origination Simulator
2. Federal Alert Gateway
3. CMSP Gateway A
4. CMSP Gateway B.

The following figure depicts the test architecture for dual Federal Alert Gateways and dual CMSP Gateways configuration:



(1) It is not complete functionality in the Federal Alert Gateway and the CMSP Gateway that is to be tested, but only that functionality associated with providing the C-Interface.
(2) Voice and data communication between test support facilities is assumed and not detailed.
(3) CMSP Test Support A and CMSP Test Support B may be the same test support person

Figure 4.3: C-Interface Test Architecture for Dual Federal Alert Gateways and Dual CMSP Gateways

The above figure shows the following four Test Points:

1. Federal Alert Gateway 1
2. Federal Alert Gateway 2
3. CMSP Gateway A
4. CMSP Gateway B.

The above figure shows the following six Data Collection Points:

1. Alert Origination Simulator
2. Alert Origination Simulator
3. Federal Alert Gateway 1
4. Federal Alert Gateway 2
5. CMSP Gateway A
6. CMSP Gateway B.

Additional Data Collection Points and Test Points may be added to the architecture in the future.

4.2 Test Tools

This clause defines the test tools that may be used for the C-Interface testing. Each individual test case in Clause 5, *Test Cases*, identifies which test tools are required.

4.2.1 Alert Origination Simulator

The Alert Origination Simulator is a test tool used to inject specified CAP test messages into the Federal Alert Gateway. The Alert Origination Simulator will be capable of storing and displaying a copy of each generated CAP message.

4.3 Test Personnel

This clause defines the test personnel that may be required for the C-Interface testing. Each individual test case in Clause 5, *Test Cases*, identifies which test personnel are required.

4.3.1 Federal Test Support

The Federal Test Support personnel will be located in the Federal facilities and will perform the following functions:

- Provide control inputs to the Alert Origination Simulator and Federal Alert Gateway.
- Collect test data such as system logs.
- Display Federal Alert Gateway message logs.
- Review messages in “raw” eXtensible Markup Language (XML) format.
- Verify conformance to the CMAC XML schema.
- Obtain the current date and time to a granularity of seconds.

4.3.2 CMSP Test Support

The CMSP Test Support personnel will be located in the CMSP facilities and will perform the following functions:

- Provide control inputs to the CMSP Gateway.
- Collect test data such as system logs.
- Review CMSP message logs.
- Review messages in “raw” XML format.
- Verify conformance to the CMAC XML schema.
- Obtain the current date and time to a granularity of seconds.

In the dual CMSP Gateway test configuration, the CMSP may elect to have the same CMSP Test Support personnel handle both CMSP Gateways or may elect to have separate CMSP Test Support personnel at each CMSP Gateway.

4.4 Pre-Test Requirements

The purpose of this clause is to verify through inspection that both the CMSP Gateway and the Federal Alert Gateway interfaces have been developed using the appropriate interface standards. Completion of this verification is entrance criteria for the subsequent test cases.

4.4.1 Pre-Test Notes

A number of standards are used in the development of the Federal Alert Gateway and the CMSP Gateway for the purposes of exchanging messages. The following steps verify that both the CMSP Gateway and Federal Alert Gateway interfaces have been developed using the appropriate standards.

4.4.2 Pre-Test Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*:

- WEA-C-RQMT-1700
- WEA-C-RQMT-1810
- WEA-C-RQMT-1820
- WEA-C-RQMT-1900
- WEA-C-RQMT-1920
- WEA-C-RQMT-1950
- WEA-C-RQMT-2700
- WEA-C-RQMT-3000
- WEA-C-RQMT-3100
- WEA-C-RQMT-3200
- WEA-C-RQMT-3210
- WEA-C-RQMT-3220
- WEA-C-RQMT-3300
- WEA-C-RQMT-3310.

NOTE: Requirements WEA –C-RQMT-3300 and WEA –C-RQMT-3310 are implicitly verified when IETF RFC 793 [Ref 17], *Transmission Control Protocol*, is validated as they are inherent to this RFC.

4.4.3 Pre-Test Verification Items

Compliance to the following standards is verified through applicable documentation provided by the relevant developer of both the CMSP Gateway and the Federal Alert Gateway:

1. IETF RFC 5280 [Ref 4], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
2. IETF RFC 6960 [Ref 5], *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.*
3. IETF RFC 4301 [Ref 6], *Security Architecture for the Internet Protocol*.
4. IETF RFC 4303 [Ref 7], *IP Encapsulating Security Payload (ESP)*.
5. IETF RFC 7296 [Ref 8], *Internet Key Exchange (IKEv2) Protocol*.
6. IETF RFC 8221 [Ref 10], *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.
7. IETF RFC 3602 [Ref 11], *The AES-CBC Cipher Algorithm and Its Use with IPSec*.
8. IETF RFC 8017 [Ref 12], *PKCS #1: RSA Cryptography Specifications Version 2.2*.
9. IETF RFC 4868 [Ref 13], *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*.
10. IETF RFC 2404 [Ref 14], *The Use of HMAC-SHA-1-96 within ESP and AH*.
11. IETF RFC 7230 [Ref 15], *Hypertext Transfer Protocol -- HTTP/1.1: Message Syntax and Routing*.

12. IETF RFC 1122 [Ref 16], *Requirements for Internet Hosts – Communication Layers*.
13. IETF RFC 793 [Ref 17], *Transmission Control Protocol*.
14. IETF STD 5 (RFC 791) [Ref 18], *Internet Protocol*.
15. IETF STD 5 (RFC 792) [Ref 19], *Internet Control Message Protocol*.
16. IETF RFC 8200, [Ref 20], *Internet Protocol, Version 6 (IPv6) Specification*.
17. IETF RFC 7231 [Ref 21], *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*.
18. IETF RFC 4291 [Ref 22], *IP Version 6 Addressing Architecture*.
19. Federal Information Processing Standards Publication 180-3 [Ref 24], *Secure Hash Standard*.

4.5 Pre-Test Configuration Information

Before the execution of the Test Cases in this Standard, the following preparations need to be completed:

- Configuration Worksheet for Federal Alert Gateway
- Configuration Worksheet for CMSP Gateway.

4.5.1 Configuration Worksheet for Federal Alert Gateway

In order to configure the Federal Alert Gateway, the Federal Test Support shall obtain the entire CMSP Gateway Group configuration data needed from the CMSP Test Support. This configuration data includes, for example, the CMSP Gateway IP address, Geo-Location Filtering areas, and timers. The following template is recommended to be used to obtain the information from the CMSP Test Support:

Table 4.1: Configuration Worksheet for Federal Alert Gateway

Parameter	Description	Range of Values	Test Value	Notes
CMSP Name	Unique identification of CMSP.	Text string		
CMSP Gateway A Address	IP address or Fully Qualified Domain Name. Uniquely identifies the CMSP Gateway. Provides a verifiable identity for Internet Key Exchange (IKE) authentication.	IP address / Text string		
CMSP Gateway B Address alternate	IP address or Fully Qualified Domain Name. Uniquely identifies the CMSP Gateway. Provides a verifiable identity for IKE authentication.	IP address / Text string (optional)		
Geo-Location Filtering	Should alerts be forwarded to the CMSP only when the alert area falls within a predefined list of states?	“Yes” (filter based on list of states) “No” (forward all alerts regardless of alert area)		
List of Geo-Location Filtering States	List of all states, separated by comma, in which the CMSP would like to receive alerts if value of Geo-Location Filtering parameter is “Yes”.	Two-digit Federal Information Processing Standards (FIPS) State Numeric Codes, per INCITS 38-2009 [Ref 3]		

Parameter	Description	Range of Values	Test Value	Notes
Reconnect Number	The number of times that the CMSP Gateway will attempt to establish an IPsec tunnel and a TCP connection. NOTE: This parameter is for informative purpose only and may not impact the Federal Alert Gateway configuration.	Numerical value 1 to 10		
IPsec Security Association (SA) Maximum Lifetime	IPsec SA Maximum Lifetime is the maximum time duration in minutes before the IPsec security association expires. This parameter should be ~10 minutes for testing and a few hours for operations.	Numerical value Range 10-480 minutes, in minute increments. Default Value of 480 minutes (8 hours)		
IKE SA Maximum Lifetime	IKE SA Maximum Lifetime is the maximum time duration in minutes before the IKE security association expires. This parameter should be ~10 minutes for testing. The IKE SA Maximum Lifetime should be set higher than the IPsec SA Maximum Lifetime.	Numerical value Range 10- 1440 minutes, in 10-minute increments. Default Value of 1440 minutes (24 hours)		
SA Renewal	Maximum time in minutes elapsed after SA expiration before a new SA is initiated. NOTE: A “Null” value for SA renewal indicates that SAs are not automatically renewed after expiration.	Numerical value in the range from 0 to 60 minutes.		Applicable for both IKE SAs and IPsec SAs.
Rekey	Minimum time before SA expiration when a new SA is initiated. NOTE: A “Null” value for Rekey time period indicates that SAs are not automatically replaced before expiration. Any other value for Rekey time period will cause SAs to be rekeyed before expiration, thus making the SA renewal parameter moot.	Numerical value in the range from 0 to 60 minutes.		Applicable for both IKE SAs and IPsec SAs.
CMSP Gateway Initiated Link Test Message	Indicates if the CMSP Gateway supports the optional CMSP Gateway initiated Link Test Message.	“Yes” (CMSP Gateway supports optional CMSP Gateway initiated Link Test Message) “No” (CMSP Gateway does not support optional CMSP Gateway initiated Link Test Message)		
CMSP Gateway CAP Retrieval	Indicates if the CMSP Gateway supports the optional CAP Retrieval functionality.	“Yes” (CMSP Gateway supports optional CAP Retrieval functionality) “No” (CMSP Gateway does not support optional CAP Retrieval functionality)		
Other application-specific parameters				

4.5.2 Configuration Worksheet for CMSP Gateway

In order to configure the CMSP Gateway, the CMSP Test Support shall obtain the Federal Alert Gateway configuration data needed from Federal Test Support. The following template is recommended to be used to obtain the information from the Federal Test Support:

Table 4.2: Configuration Worksheet for CMSP Gateway

Parameter	Description	Range of Values	Test Value	Notes
Federal Alert Gateway #1 Address	IP address or Fully Qualified Domain Name[8]. Uniquely identifies the Federal Alert Gateway 1 for the test cases. Provides a verifiable identity for IKE authentication.	IP address / Text string		
Federal Alert Gateway #2 Address	IP address or Fully Qualified Domain Name[8]. Uniquely identifies the Federal Alert Gateway 2 for the test cases. Provides a verifiable identity for IKE authentication.	IP address / Text string		
Reconnect Number	The number of times that the Federal Alert Gateway will attempt to establish an IPsec tunnel and a TCP connection. NOTE: This parameter is for informative purpose only and may not impact the CMSP Gateway configuration.	Numerical value 1 to 10		
Retransmit Number	The number of times that the Federal Alert Gateway will attempt to send a CMAC message to the CMSP Gateway when the expected response is not received. NOTE: This parameter is for informative purpose only and may not impact the CMSP Gateway configuration.	Numerical value 1 to 10		
Link Test Period	The time interval in minutes between Link Test Message transmitted by the Federal Alert Gateway. NOTE: This parameter is for informative purpose only and may not impact the CMSP Gateway configuration.	Numerical value 1 to 120 minutes, in 1-minute increments		

[8] When a Fully Qualified Domain Name uniquely identifies the Federal Alert Gateway, the IP address of the Federal Alert Gateway may be provisioned in the CMSP's network (i.e., at the option of the CMSP) for Domain Name Service implemented in the CMSP's network.

Parameter	Description	Range of Values	Test Value	Notes
IPsec SA Maximum Lifetime	IPsec SA Maximum Lifetime is the maximum time duration before the IPsec security association expires. This parameter should be ~10 minutes for testing and a few hours for operations.	Numerical value Range 10-480 minutes, in minute increments. Default Value of 480 minutes (8 hours)		
IKE SA Maximum Lifetime	IKE SA Maximum Lifetime is the maximum time duration before the IKE security association expires. This parameter should be ~10 minutes for testing. The IKE SA Maximum Lifetime should be set higher than the IPsec SA Maximum Lifetime.	Numerical value Range 10- 1440 minutes, in 10-minute increments. Default Value of 1440 minutes (24 hours)		
SA Renewal	Maximum time elapsed after SA expiration before a new SA is initiated. NOTE: A “Null” value for SA renewal indicates that SAs are not automatically renewed after expiration.	“Null” or a numerical value in the range from 0 to 60 minutes.		Applicable for both IKE SAs and IPsec SAs.
Rekey	Minimum time before SA expiration when a new SA is initiated. NOTE: A “Null” value for Rekey time period indicates that SAs are not automatically replaced before expiration. Any other value for Rekey time period will cause SAs to be rekeyed before expiration, thus making the SA renewal parameter moot.	“Null” or a numerical value in the range from 0 to 60 minutes.		Applicable for both IKE SAs and IPsec SAs.
Other application-specific parameters				

NOTE: CMAC message transactions use TCP port 8080 and CAP retrieval message transaction uses TCP port 80.

4.6 Configurations for Test Cases

Pre-Test Requirements and Test Cases specified in this Standard should be applied using the configurations described below:

1. Apply the pre-test verification of 4.4, *Pre-Test Requirements*, individually to Federal Alert Gateway 1, Federal Alert Gateway 2, CMSP Gateway A, and CMSP Gateway B (if CMSP Gateway B is present). This verifies that all gateways support applicable standards.
2. Apply CMAS-TC-101 individually to Federal Alert Gateway 1 and Federal Alert Gateway 2, and CMAS-TC-201 individually to CMSP Gateway A and CMSP Gateway B (if CMSP Gateway B is present). This verifies that all gateways are configured properly.
3. Apply CMAS-TC-008 or CMAS-TC-009 in Dual Federal Alert Gateways and Dual CMSP Gateways configuration to Federal Alert Gateways 1 and 2 and CMSP Gateways A and B (or only CMSP Gateway A, if CMSP Gateway B is not present). This verifies connection establishment operation of each device.
4. Apply CMAS-TC-001, CMAS-TC-002, CMAS-TC-003, CMAS-TC-004, CMAS-TC-005, and CMAS-TC-006 in Single Federal Alert Gateway and Single CMSP Gateway configuration to Federal Alert Gateway 1 or 2 and CMSP Gateway A. This verifies proper handling of Alert, Update, Cancel, RMT, and Link Test messages and Digital Signatures by the application.

5. Apply CMAS-TC-007 and CMAS-TC-011 either in Single Federal Alert Gateway and Dual CMSP Gateways configuration to Federal Alert Gateway 1 or 2 and CMSP Gateways A and B, or in Single Federal Alert Gateway and Single CMSP Gateway configuration to Federal Alert Gateway 1 or 2 and CMSP Gateway A (if CMSP Gateway B is not present). This tests for proper operation of Transmission Control messages and message queuing.
6. Apply CMAS-TC-010 in Single Federal Alert Gateway and Single CMSP Gateway configuration to Federal Alert Gateway 1 or 2 and CMSP Gateway A. This tests for proper geo-location filtering operation.
7. Apply CMAS-TC-012 in Single Federal Alert Gateway and Single CMSP Gateway configuration to Federal Alert Gateway 1 or 2 and CMSP Gateway A. This tests for proper CAP retrieval operation.

5 Test Cases

This clause contains the various test cases for various messages and conditions for both stand-alone gateway tests and inter-gateway tests. Each 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 ATIS-0700037 [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 B, *Input CAP Messages*; Annex C, *Expected CMAC Messages*; and Annex D, *Expected ACK Messages*.

This clause is divided into the following test case categories:

- Federal Alert Gateway Stand-Alone Test Cases
- CMSP Gateway Stand-Alone Test Cases
- Inter-Gateway Test Cases.

5.1 Federal Alert Gateway Stand-Alone Test Cases

This clause defines the test cases for the stand-alone Federal Alert Gateway testing. The test cases in this clause must be successfully completed before executing the inter-gateway test cases in Clause 5.3, *Inter-Gateway Test Cases*.

This clause contains the following stand-alone Federal Alert Gateway test case:

- CMAS-TC-101 test case for Federal Alert Gateway Profile Data.

5.1.1 CMAS-TC-101 – Federal Alert Gateway Profile Data Test

The purpose of the Profile Data test procedure (CMAS-TC-101) is to verify that the required parameters and verifiable identities for the CMSP gateways are stored in CMSP Profile of the Federal Alert Gateway. Later inter-gateway tests in Clause 5.3, *Inter-Gateway Test Cases*, verify that the connections are established in accordance with these profiles, identities verified, and secure tunnels established.

5.1.1.1 Items to Be Tested

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

- Federal Alert Gateway.

5.1.1.2 Notes

Connections are established between the Federal Alert Gateway and the CMSP Gateway, according to gateway profiles stored at each end. This test examines and verifies the contents of the stored gateway profiles. This is largely a test conducted by the method of inspection.

5.1.1.3 Test Tools

No test tools are necessary to complete this test procedure.

5.1.1.4 Test Capabilities

The following capabilities will be necessary to complete this test procedure:

- Federal Alert Gateway Test Capabilities:
  - Ability to display contents of CMSP Profiles.

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.

5.1.1.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-0100
- WEA-C-RQMT-0110
- WEA-C-RQMT-0120
- WEA-C-RQMT-0200.

5.1.1.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- All required data for the CMSP Gateways must be previously stored in the CMSP Gateway profile of the Federal Alert Gateway under test.
- Before this test case can be executed, all entry criteria under Clause 4.5, *Pre-Test Configuration Information*, must be completed. This is necessary to ensure that all parties involved in testing activities are ready, and that interface testing can start without delay.

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-101 – Federal Alert Gateway Profile Data Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Display the contents of the CMSP Profile for the CMSP Gateway Group under test, as stored in the Federal Alert Gateway.	Contents of the CMSP Profile are displayed.	• RQMT-0100	
2	**Federal Test Support:** Verify CMSP Name in the CMSP Profile.	Text string containing the unique identification of the CMSP.	• RQMT-0110 • RQMT-0120 • RQMT-0200	
3	**Federal Test Support**: Verify CMSP Gateway A Address in the CMSP Profile.	Valid IP address or Fully Qualified Domain Name for CMSP Gateway A.	• RQMT-0110 • RQMT-0120 • RQMT-0200	
4	**Federal Test Support:** Verify CMSP Gateway B Address alternate in the CMSP Profile.	Blank if CMSP has only one gateway. Otherwise, valid IP address or Fully Qualified Domain Name for CMSP Gateway B.	• RQMT-0110 • RQMT-0120 • RQMT-0200	
5	**Federal Test Support:** Verify Geo-Location Filtering in the CMSP Profile.	"Yes" if this CMSP wants messages to be filtered based on a list of states. "No" otherwise.	• RQMT-0110 • RQMT-0120 • RQMT-0200	
6	**Federal Test Support (conditional):** Verify List of Geo-Location Filtering States in the CMSP Profile if Geo-Location Filtering is set to "Yes".	List of two-digit FIPS State Numeric Codes, per INCITS 38-2009 [Ref 3], corresponding to the states in which the CMSP would like to receive alerts. If value of the Geo-Location Filtering attribute in the CMSP Profile in step 5 above is "Yes", then this list should contain at least one valid FIP State Numeric Code. If value of the Geo-Location Filtering attribute in the CMSP Profile in step 5 above is "No", then this list should contain no entries.	• RQMT-0110 • RQMT-0120 • RQMT-0200	
7	**Federal Test Support:** Verify C-Interface Message Version.	"2.0".	• RQMT-0200	

5.2 CMSP Gateway Stand-Alone Test Cases

This clause defines the test cases for the stand-alone CMSP Gateway testing. The test cases in this clause must be successfully completed before executing the inter-gateway test cases in Clause 5.3, *Inter-Gateway Test Cases*.

This clause contains the following stand-alone CMSP Gateway test cases:

- CMAS-TC-201 test case for CMSP Gateway Profile Data.

5.2.1 CMAS-TC-201 – CMSP Gateway Profile Data Test

The purpose of the Profile Data test procedure (CMAS-TC-201) is to verify that the required parameters and verifiable identities for the Federal Alert Gateways are stored in the Federal Alert Gateway Profile of the CMSP Gateway. Later inter-gateway tests in Clause 5.3, *Inter-Gateway Test Cases*, verify that the connections are established in accordance with these profiles, identities verified, and secure tunnels established.

5.2.1.1 Items to Be Tested

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

CMSP Gateway.

5.2.1.2 Notes

Connections are established between the Federal Alert Gateway and the CMSP Gateway according to gateway profiles stored at each end. This test examines and verifies the contents of the stored gateway profiles. This is largely a test conducted by the method of inspection.

5.2.1.3 Test Tools

No test tools are necessary to complete this test procedure.

5.2.1.4 Test Capabilities

The following capabilities will be necessary to complete this test procedure.

- CMSP Gateway Test Capabilities:
  - Ability to display contents of the Federal Alert Gateway Profile.

5.2.1.5 Test Personnel

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

- CMSP Test Support.

5.2.1.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0600
- WEA-C-RQMT-0700
- WEA-C-RQMT-0720.

5.2.1.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- All required data for the Federal Alert Gateways must be previously stored in the Federal Alert Gateway Profile of the CMSP Gateway under test.
- Before this test case can be executed, all entry criteria under Clause 4.5, *Pre-Test Configuration Information*, must be completed. This is necessary to ensure that all parties involved in testing activities

are ready and interface testing can start without delay.

5.2.1.8 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 5.2: Steps for Test Case CMAS-TC-201 – CMSP Gateway Profile Data Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**CMSP Test Support:** Display the contents of the Federal Alert Gateway Profile stored in the CMSP Gateway.	Contents of the Federal Alert Gateway Profile are displayed.	• RQMT-0700	
2	**CMSP Test Support:** Verify the number of entries in the Federal Alert Gateway Profile.	The Federal Alert Gateway Profile has one entry for each Federal Alert Gateway available for this CMSP.	• RQMT-0600	
3	**CMSP Test Support:** Verify Federal Alert Gateway Address for each entry in the Federal Alert Gateway Profile.	Valid IP address or Fully Qualified Domain Name for the Federal Alert Gateway.	• RQMT-0600 • RQMT-0720	

5.3 Inter-Gateway Test Cases

This clause defines the test cases between the Federal Gateway and the CMSP Gateway across the Reference Point “C” interface. The test cases in Clause 5.1, *Federal Alert Gateway Stand-Alone Test Cases,* and Clause 5.2, *CMSP Gateway Stand-Alone Test Cases,* must be successfully completed before executing the inter-gateway test cases defined in this clause.

This clause contains the following inter-gateway test cases:

- CMAS-TC-001 test case for Alert Message
- CMAS-TC-002 test case for Digital Signature
- CMAS-TC-003 test case for Update Message
- CMAS-TC-004 test case for Cancel Message
- CMAS-TC-005 test case for Required Monthly Test (RMT)
- CMAS-TC-006 test case for Link Test Message
- CMAS-TC-007 test case for Transmission Control
- CMAS-TC-008 test case for General Connectivity via Link Test Message
- CMAS-TC-009 test case for General Connectivity via Transmission Control Resume Message
- CMAS-TC-010 test case for Geo-Location Filtering
- CMAS-TC-011 test case for Message Queuing
- CMAS-TC-012 test case for CAP Retrieval.

The proper handling of the digital signatures by the CMSP Gateways that do not support non-repudiation is implicitly tested by test cases CMAS-TC-001, CMAS-TC-003, CMAS-TC-004, and CMAC-TC-005.

5.3.1 CMAS-TC-001 – Alert Message Test

The purpose of the Alert Message test procedure (CMAS-TC-001) is to test the requirements associated with sending CMAC alert messages. The procedure will test transmission of the alert message from the Federal Alert Gateway, reception of the message at a CMSP Gateway, logging of the message, proper message format, and message responses. This test case does not test non-repudiation. See test case CMAS-TC-002 Digital Signature Test for the testing of the optional support of non-repudiation.

5.3.1.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway

5.3.1.2 Notes

The Alert message is a type of CMAC message sent from the Federal Alert Gateway to the CMSP Gateway. There are five types of Alert messages used in this test: Imminent Threat, National, America's Missing: Broadcast Emergency Response (AMBER) alerts, Public Safety, and State/Local WEA Test alerts.

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.

5.3.1.3 Test Tools

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

- Alert Origination Simulator.

5.3.1.4 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
  - Ability to verify conformance to the CMAC XML schema.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in “raw” XML format
  - Ability to verify conformance to the CMAC XML schema.

5.3.1.5 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.

5.3.1.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0130
- WEA-C-RQMT-0400
- WEA-C-RQMT-0410
- WEA-C-RQMT-0414
- WEA-C-RQMT-0416
- WEA-C-RQMT-0480
- WEA-C-RQMT-0496
- WEA-C-RQMT-0500
- WEA-C-RQMT-0540
- WEA-C-RQMT-0900
- WEA-C-RQMT-0950
- WEA-C-RQMT-1000
- WEA-C-RQMT-1010
- WEA-C-RQMT-1150
- WEA-C-RQMT-2500
- WEA-C-RQMT-2510
- WEA-C-RQMT-2530
- WEA-C-RQMT-2540
- WEA-C-RQMT-2553
- WEA-C-RQMT-2557
- WEA-C-RQMT-2590
- WEA-C-RQMT-2630
- WEA-C-RQMT-2640
- WEA-C-RQMT-2650
- WEA-C-RQMT-2670
- WEA-C-RQMT-2810
- WEA-C-RQMT-2850
- WEA-C-RQMT-2920.

5.3.1.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).

- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

  NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.
- If non-repudiation functionality can be disabled in the CMSP Gateway, the disabling of the non-repudiation functionality should be a prerequisite for this test.

5.3.1.8 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 5.3: Steps for Test Case CMAS-TC-001 - Alert Message Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 “Imminent Threat Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #2 “National Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #3 “AMBER Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3.1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #12 “Public Safety Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3.2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #13 “State/Local WEA Test Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
4	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains five CMAC messages (Annex C, *Expected CMAC Messages*) resulting from CAP Message #1, CAP Message #2, CAP Message #3, CAP Message #12, and CAP Message #13.	• RQMT-0130 • RQMT-0400 • RQMT-0410 • RQMT-0414 • RQMT-0416 • RQMT-0480 • RQMT-1000 • RQMT-1010 RQMT-1150 • RQMT-2553 • RQMT-2557 • RQMT-2650 • RQMT-2670 • RQMT-2850	
5	**CMSP Test Support:** Verify that the first received CMAC message (CMAC Message #1 resulting from CAP Message #1) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2553 • RQMT-2557 • RQMT-2630 • RQMT-2850	
6	**CMSP Test Support:** Verify that the second received CMAC message (CMAC Message #2 resulting from CAP Message #2) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2553 • RQMT-2557 • RQMT-2630 • RQMT-2850	
7	**CMSP Test Support:** Verify that the third received CMAC message (CMAC Message #3 resulting from CAP Message #3) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2553 • RQMT-2557 • RQMT-2630 • RQMT-2850	
7.1	**CMSP Test Support:** Verify that the fourth received CMAC message (CMAC Message #14 resulting from CAP Message #12) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2553 • RQMT-2557 • RQMT-2630 • RQMT-2670 • RQMT-2850	
7.2	**CMSP Test Support:** Verify that the fifth received CMAC message (CMAC Message #15 resulting from CAP Message #13) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2553 • RQMT-2557 • RQMT-2630 • RQMT-2650 • RQMT-2850	
8	**CMSP Test Support:** Verify the <CMAC_protocol_version> element value in the first CMAC message received (resulting from CAP Message #1).	The <CMAC_protocol_version> element value is “2.0”.	• RQMT-0496 • RQMT-2500	
8.1	**CMSP Test Support:** Verify occurrence of the <CMAC_Alert_Text> segment for English.	One occurrence of the <CMAC_text_language> element has a value of “English”.	• RQMT-2553	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
8.2	**CMSP Test Support:** Verify all occurrences of the <CMAC_Alert_Text> segment have different languages.	All occurrences of the <CMAC_text_language> element have unique values (e.g., no value for any language occurs more than once).	• RQMT-2557	
8.3	**CMSP Test Support:** Verify all occurrences of the <CMAC_Alert_Text> segment contain both 90-character maximum alert message and 360-character maximum alert message.	All occurrences of the <CMAC_Alert_Text> segment have both 90-character maximum alert and 360-character maximum alert messages.	• RQMT-2850	
9	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the first logged CMAC message (resulting from CAP Message #1) from the CMSP Gateway message log contains the mandatory message elements and associated values transmitted by the Federal Alert Gateway.	The logged CMAC message contains the message elements and values as defined in Table C.1: *CMAC Message #1 Expected Messages & Values*.	• RQMT-2510 • RQMT-1150	
10	**CMSP Test Support:** Verify that only the CMAC messages resulting from CAP Message #2, CAP Message #3, CAP Message #12, and CAP Message #13 from the CMSP Gateway message log contain the <CMAC_special_handling> element.	The first logged CMAC message (resulting from CAP Message #1) does not contain the <CMAC_special_handling> element, and the second, third, fourth, and fifth logged CMAC messages (resulting from CAP Messages #2, #3, #12, and #13) do contain the <CMAC_special_handling> element.	• RQMT-2530 • RQMT-1150 • RQMT-2650 • RQMT-2670	
11	**CMSP Test Support:** Verify the <CMAC_Alert_Area> in the first received CMAC message from the CMSP Gateway message log contains one instance of <CMAC_cmas_geocode> element.	The <CMAC_Alert_Area> segment of the first received CMAC message (resulting from CAP Message #1) contains one instance of a <CMAC_cmas_geocode> element.	• RQMT-2540	
12	**CMSP Test Support:** Verify the <CMAC_message_number> values for the logged CMAC messages from the CMSP Gateway message log have increased monotonically with each message.	The <CMAC_message_number> value in the fifth logged CMAC message (resulting from CAP Message #13) is one greater than the <CMAC_message_number> value in the fourth CMAC message (resulting from CAP Message #12) which is one greater than the <CMAC_message_number> value in the third logged CMAC message (resulting from CAP Message #3) is one greater than the <CMAC_message_number> value in the second logged CMAC message (resulting from CAP Message #2), which is one greater than the <CMAC_message_number> value in the first logged CMAC message (resulting from CAP Message #1).	• RQMT-2640	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
13	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains five Ack responses from the CMSP Gateway (Appendix D), sent in response to CMAC Message #1, CMAC Message #2, CMAC Message #3 CMAC Message #14, and CMAC Message #15.	• RQMT-0900 • RQMT-0950 • RQMT-0500 • RQMT-0540 • RQMT-2810	
14	**Federal Test Support & CMSP Test Support:** Federal Test Support verifies with the CMSP Test Support that the first logged Ack message (resulting from CMAC Message #1) from the Federal Alert Gateway message log contains the mandatory message elements and associated values transmitted by the CMSP Gateway.	The first logged Ack message contains the message elements and values as defined in Table D.1: *Ack Message #1 Expected Messages & Values*.	• RQMT-2590	
15	**Federal Test Support:** Verify the <CMAC_message_number> values for the logged Ack messages from the Federal Alert Gateway message log have increased monotonically with each message.	The <CMAC_message_number> value in the fifth logged Ack message (Ack Message #6 resulting from CMAC Message #15) is one greater than the <CMAC_message_number> value in the fourth logged Ack message (Ack message #5 resulting from CMAC Message #14), which is one greater than the <CMAC_message_number> value in the third logged Ack message (Ack Message #3 resulting from CMAC Message #3) is one greater than the <CMAC_message_number> value in the second logged Ack message (Ack message #2 resulting from CMAC Message #2), which is one greater than the <CMAC_message_number> value in the first logged Ack message (Ack message #1 resulting from CMAC Message #1).	• RQMT-2640	
16	**Federal Test Support:** Verify that the first received Ack message (Ack message #1 resulting from CMAC Message #1) conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	
17	**Federal Test Support:** Verify that the second received Ack message (Ack message #2 resulting from CMAC Message #2) conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	
18	**Federal Test Support:** Verify that the third received Ack message (Ack Message #3 resulting from CMAC Message #3) conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
18.1	**Federal Test Support:** Verify that the fourth received Ack message (Ack Message #5 resulting from CMAC Message #14) conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	
18.2	**Federal Test Support:** Verify that the fifth received Ack message (Ack Message #6 resulting from CMAC Message #15) conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	
19	**CMSP Test Support:** View the CMSP Gateway message log.	The CMSP Gateway message log does not contain any messages from the Federal Alert Gateway following the fifth CMAC Alert message (CMAC Message #15 of Annex C, *Expected CMAC Messages*).	• RQMT-2920	

5.3.2 CMAS-TC-002 – Digital Signature Test

The purpose of the digital signature test procedure (CMAS-TC-002) is to test the requirements associated with sending a CMAC message containing a digital signature segment. This test case is optional for any CMSP Gateway that does not support non-repudiation.

5.3.2.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway

5.3.2.2 Notes

The digital signature segment enclosed in CMAC messages can optionally be used by a CMSP Gateway for non-repudiation. The digital signature segment is included in Alert, Update, Cancel, and RMT messages, which are transmitted from the Federal Alert Gateway to the CMSP Gateway. The digital signature segment is a child segment of <CMAC_Alert_Attributes>.

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.

5.3.2.3 Test Tools

The following test tools will be used to complete this test procedure. The specific test tools used are to be specified on the Test Log and Signature Page.

- Alert Origination Simulator.

5.3.2.4 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
  - Ability to verify conformance to the CMAC XML schema.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in “raw” XML format
  - Ability to verify conformance to the CMAC XML schema.

5.3.2.5 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.

5.3.2.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-2400
- WEA-C-RQMT-2410
- WEA-C-RQMT-2420
- WEA-C-RQMT-2430
- WEA-C-RQMT-2440
- WEA-C-RQMT-2450
- WEA-C-RQMT-2630.

5.3.2.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).
- The Federal Alert Gateway and CMSP Gateway have passed testing for the Alert Message (CMAS-TC-001).
- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

  NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.
- Non-repudiation functionality should be supported in the CMSP Gateway.

5.3.2.8 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 5.4: Steps for Test Case CMAS-TC-002 – Digital Signature Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 "Imminent Threat Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
2	**CMSP Test Support:** Verify that the received CMAC message (resulting from CAP Message #1) conforms to the CMAC XML schema.	The CMAC Message has no errors.	• RQMT-2440 • RQMT-2630	
3	**CMSP Test Support:** Verify that XML Digital Signature of the received CMAC message (resulting from CAP Message #1) includes a valid XML Digital Signature.	The XML Digital Signature is successfully validated.	• RQMT-2400 • RQMT-2410 • RQMT-2420 • RQMT-2430 • RQMT-2440	
4	**CMSP Test Support:** Verify the Signature Method value in the <CMAC_Digital_Signature> segment of the received CMAC message (resulting from CAP Message #1).	<SignatureMethod> element contains an attribute with value of: Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256".	• RQMT-2400	
5	**CMSP Test Support:** Verify the Digest Method value in the <CMAC_Digital_Signature> segment of the received CMAC message (resulting from CAP Message #1).	<DigestMethod> element contains an attribute with a value of: Algorithm="http://www.w3.org/2001/04/xmlenc#sha256".	• RQMT-2410	
6	**CMSP Test Support:** Verify the Canonicalization Method value in the <CMAC_Digital_Signature> segment of the received CMAC message (resulting from CAP Message #1).	<CanonicalizationMethod> element contains an attribute with a value of: Algorithm= "http://www.w3.org/TR/xml-exc-c14n/".	• RQMT-2420	
7	**CMSP Test Support:** Verify the Transform value within the <CMAC_Digital_Signature> segment of the received CMAC message (resulting from CAP Message #1).	<Transform> element contains an attribute with a value of: Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature".	• RQMT-2430	
8	**Federal Test Support:** View Federal Alert Gateway Message log.	The Federal Alert Gateway message log contains an Ack response from the CMSP Gateway.	• RQMT-2450	

5.3.3 CMAS-TC-003 – Update Message Test

The purpose of the Update message test procedure (CMAS-TC-003) is to test the requirements associated with sending CMAC Update messages. The procedure will test transmission of the Update message from the Federal Alert Gateway, reception of the message at a CMSP Gateway, logging of the message, proper message format, and message responses.

5.3.3.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway

5.3.3.2 Notes

The Update message is a type of CMAC message sent from the Federal Alert Gateway to the CMSP Gateway. The Update message updates a previously issued alert message and is sent to warn the CMSP subscribers about changes associated with the event that caused the issuance of the previous alert. There are five types of Update messages used in this test: Imminent Threat, National, AMBER alerts, Public Safety, and State/Local WEA Test alerts.

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.

5.3.3.3 Test Tools

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

- Alert Origination Simulator.

5.3.3.4 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.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in “raw” XML format
  - Ability to verify conformance to the CMAC XML schema.

5.3.3.5 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.

5.3.3.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0130
- WEA-C-RQMT-0400
- WEA-C-RQMT-0420
- WEA-C-RQMT-0425
- WEA-C-RQMT-0427
- WEA-C-RQMT-0428
- WEA-C-RQMT-0480
- WEA-C-RQMT-0950
- WEA-C-RQMT-1000
- WEA-C-RQMT-1020
- WEA-C-RQMT-1150
- WEA-C-RQMT-2520
- WEA-C-RQMT-2530
- WEA-C-RQMT-2630
- WEA-C-RQMT-2810.

5.3.3.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).
- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

  NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.3.8 Test Steps

The following table defines the individual test steps that are to be 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 5.5: Steps for Test Case CMAS-TC-003 – Update Message Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 "Imminent Threat Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway. Record the [Expires Date-Time 1] entered into CAP Message #1 for use later in this test.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #2 "National Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #3 "AMBER Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3.1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #12 "Public Safety Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
3.2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #13 "State/Local WEA Test Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
4	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains CMAC messages #1, #2, #3, #14, and #15 (Annex B, *Input CAP Messages*) resulting from CAP Message #1, CAP Message #2, CAP Message #3, CAP Message #12, and CAP Message #13.	N/A	N/A
5	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains five Ack responses from the CMSP Gateway (Ack Message #1, Ack Message #2, Ack Message #3, Ack Message #5, and Ack Message #6 in Annex D, *Expected ACK Messages*), sent in response to CMAC Message #1, CMAC Message #2, CMAC Message #3 CMAC Message #14, and CMAC Message #15.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
6	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #4 "Imminent Threat Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway with an [Expires Date-Time 4] different from [Expires Date-Time 1] entered and noted in Step 1 of this test.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
7	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #5 "National Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
8	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #6 "AMBER Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
8.1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #14 "Public Safety Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
8.2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #15 "State/Local WEA Test Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
9	**CMSP Test Support:** View CMSP Gateway message log**.**	The CMSP Gateway message log contains CMAC messages #4, #5, #6, #16, and #17 (Annex C, *Expected CMAC Messages*).	• RQMT-0400 • RQMT-0420 • RQMT-0427 • RQMT-0428 • RQMT-1000 • RQMT-1020 • RQMT-1150	
10	**CMSP Test Support:** Verify that the sixth received CMAC message (CMAC Message #4 resulting from CAP Message #4) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-0130 • RQMT-0480 • RQMT-2630	
11	**CMSP Test Support:** Verify that the seventh received CMAC message (CMAC Message #5 resulting from CAP Message #5) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
12	**CMSP Test Support:** Verify that the eighth received CMAC message (CMAC Message #6 resulting from CAP Message #6) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
12.1	**CMSP Test Support:** Verify that the ninth received CMAC message (CMAC Message #16 resulting from CAP Message #14) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2670 • RQMT-2850	
12.2	**CMSP Test Support:** Verify that the tenth received CMAC message (CMAC Message #17 resulting from CAP Message #15) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2650 • RQMT-2850	
13	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the sixth received CMAC message (resulting from CAP Message #4) contains the mandatory and conditional message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the message elements and values as defined in Table C.2: *CMAC Message #4 Expected Messages & Values*.	• RQMT-2520	
14	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the seventh received CMAC message (resulting from CAP Message #5) contains the mandatory and conditional message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the message elements and values as defined in Table C.3: *CMAC Message #5 Expected Messages & Values*.	• RQMT-2520	
15	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the eighth received CMAC message (resulting from CAP Message #6) contains the mandatory and conditional message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the message elements and values as defined in Table C.4: *CMAC Message #6 Expected Messages & Values*.	• RQMT-2520	
15.1	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the ninth received CMAC message (resulting from CAP Message #14) contains the mandatory and conditional message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the message elements and values as defined in Table C.11: *CMAC Message #16 Expected Messages & Values*.	• RQMT-2670	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
15.2	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the tenth received CMAC message (resulting from CAP Message #15) contains the mandatory and conditional message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the message elements and values as defined in Table C.12: *CMAC Message #17 Expected Messages & Values*.	• RQMT-2650	
15.3	**CMSP Test Support:** Verify all occurrences of the <CMAC_Alert_Text> segment contain both 90-character maximum alert message and 360-character maximum alert message.	All occurrences of the <CMAC_Alert_Text> segment have both 90-character maximum alert and 360-character maximum alert messages.	• RQMT-2850	
16	**CMSP Test Support:** Verify that only the CMAC Update messages resulting from CAP Messages #5, #6, #14, and #15 from the CMSP Gateway message log contain the <CMAC_special_handling> element.	The sixth received CMAC message (resulting from CAP Message #4) does not contain the <CMAC_special_handling> element and the seventh, eighth, ninth, and tenth received CMAC messages (resulting from CAP Messages #5, #6, #14, and #15) do contain the <CMAC_special_handling> element.	• RQMT-2530 • RQMT-1150 • RQMT-2650 • RQMT-2670	
17	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains five Ack responses from the CMSP Gateway sent in response to CMAC Message #4, CMAC Message #5, CMAC Message #6, CMAC Message #16, and CMAC Message #17.	• RQMT-0950 • RQMT-2810	
18	**Federal Test Support:** Use Alert Origination Simulator to send CAP Message #7 “Invalid CMAS Criteria Update” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits a Cancel message (CMAC Message #7) to the CMSP Gateway and the CMSP Gateway responds with an Ack. Receipt of this Ack at the Federal Alert Gateway should be verified prior to moving to the next step.	N/A	N/A
19	**CMSP Test Support:** View CMSP Gateway message log	The CMSP Gateway message log contains CMAC message #7 (Annex C, *Expected CMAC Messages*).	• RQMT-0425	

NOTE: CAP Message #7 (step 18) is a valid CAP message but contains values for the urgency and severity elements that are invalid for WEA distribution. Therefore, the Federal Alert Gateway will stop the ongoing broadcast by sending a Cancel Message (CMAC Message #7) to the CMSP Gateway and will not update the alert.

5.3.4 CMAS-TC-004 – Cancel Message Test

The purpose of the Cancel message test procedure (CMAS-TC-004) is to test the requirements associated with sending CMAC Cancel messages. The procedure tests transmission of the Cancel message from the Federal Alert Gateway, reception of the message at a CMSP Gateway, logging of the message, proper message format, and message responses.

5.3.4.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway.

5.3.4.2 Notes

The Cancel message is a type of CMAC message sent from the Federal Alert Gateway to the CMSP Gateway. The Cancel message cancels a previously issued alert message and is sent when the event that caused the issuance of the previous alert has changed and the appropriate government entities have decided that the event is no longer an imminent threat to life or property. There are three types of Cancel messages used in this test: Imminent Threat, National, and AMBER alerts.

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.

5.3.4.3 Test Tools

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

- Alert Origination Simulator.

5.3.4.4 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.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in “raw” XML format
  - Ability to verify conformance to the CMAC XML schema.

5.3.4.5 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.

5.3.4.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-0130
- WEA-C-RQMT-0400
- WEA-C-RQMT-0430
- WEA-C-RQMT-0480

- WEA-C-RQMT-0950
- WEA-C-RQMT-1000
- WEA-C-RQMT-1030
- WEA-C-RQMT-1150
- WEA-C-RQMT-2560
- WEA-C-RQMT-2630
- WEA-C-RQMT-2810.

5.3.4.7 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).
- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.4.8 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 5.6: Steps for Test Case CMAS-TC-004 – Cancel Message Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 “Imminent Threat Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
2	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains CMAC message #1 (Annex C, *Expected CMAC Messages*) resulting from CAP Message #1.	N/A	N/A
3	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains an Ack response from the CMSP Gateway (Ack Message #1 in Annex D, *Expected ACK Messages*), sent in response to CMAC Message #1.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
4	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #8 "Imminent Threat Cancel" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	• RQMT-0130 • RQMT-0480 • RQMT-1150	
5	**CMSP Test Support:** View CMSP Gateway message log**.**	The CMSP Gateway message log contains CMAC message #8 (Annex C, *Expected CMAC Messages*).	• RQMT-0400 • RQMT-0430 • RQMT-1000 • RQMT-1030	
6	**CMSP Test Support:** Verify that the second received CMAC message (CMAC Message #8 resulting from CAP Message #8) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
7	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the second received CMAC message (resulting from CAP Message #8) contains the mandatory message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the following message elements and values as defined in Table C.5: *CMAC Message #8 Expected Messages & Values*.	• RQMT-2560	
8	**Federal Test Support:** View Federal Alert Gateway message log**.**	The Federal Alert Gateway message log contains an Ack response from the CMSP Gateway, sent in response to CMAC Message #8.	• RQMT-0950 • RQMT-2810	

5.3.5 CMAS-TC-005 – Required Monthly Test (RMT) Test

The purpose of the RMT message test procedure (CMAS-TC-005) is to test the requirements associated with sending CMAC RMT messages. The procedure will test transmission of the RMT message from the Federal Alert Gateway, reception of the message at a CMSP Gateway, logging of the message, proper message format, and message responses.

5.3.5.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway.

5.3.5.2 Notes

The RMT message is a type of CMAC test message sent from the Federal Alert Gateway to the CMSP Gateway. This message is to be sent only once per calendar month.

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.

5.3.5.3 Test Tools

There are no test tools that are necessary to complete this test procedure.

5.3.5.4 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.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in "raw" XML format
  - Ability to verify conformance to the CMAC XML schema.

5.3.5.5 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.

5.3.5.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0400
- WEA-C-RQMT-0440
- WEA-C-RQMT-0480
- WEA-C-RQMT-0950
- WEA-C-RQMT-1000
- WEA-C-RQMT-1050
- WEA-C-RQMT-2570
- WEA-C-RQMT-2630
- WEA-C-RQMT-2810
- WEA-C-RQMT-2850

5.3.5.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).

- The CMSP Gateway has not logged any previous RMT messages sent by the Federal Alert Gateway within the calendar month.
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.5.8 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 5.7: Steps for Test Case CMAS-TC-005 – Required Monthly Test (RMT) Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Send CMAC Message #9 "RMT" (Annex C, *Expected CMAC Messages*) to the CMSP Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
2	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains CMAC message #9 (Annex C, *Expected CMAC Messages*).	• RQMT-0400 • RQMT-0440 • RQMT-0480 • RQMT-1000 • RQMT-1050	
3	**CMSP Test Support:** Verify that the received CMAC message (CMAC Message #9) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
4	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the CMAC message (CMAC Message #9) contains the mandatory message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the following message elements and values as defined in Table C.6: *CMAC Message #9 Expected Messages & Values*.	• RQMT-2570	
4.1	**CMSP Test Support:** Verify all occurrences of the <CMAC_Alert_Text> segment contain both 90-character maximum alert message and 360-character maximum alert message.	All occurrences of the <CMAC_Alert_Text> segment have both 90-character maximum alert and 360-character maximum alert messages.	• RQMT-2850	
5	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains an Ack response from the CMSP Gateway, sent in response to CMAC Message #9.	• RQMT-0950 • RQMT-2810	

5.3.6 CMAS-TC-006 – Link Test Messages Test

The purpose of the Link Test messages test procedure (CMAS-TC-006) is to test the requirements associated with sending CMAC Link Test messages. The procedure will test transmission of the Link Test message, reception of the message, logging of the message, proper message format, and message responses for both Federal Alert Gateway initiated Link Test messages and CMSP Gateway initiated Link Test messages.

5.3.6.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway.

5.3.6.2 Notes

The Link Test message is a type of CMAC message that is generated periodically by the Federal Alert Gateway and occasionally by the CMSP Gateway to verify that the interface is available.

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.

5.3.6.3 Test Tools

There are no test tools that are necessary to complete this test procedure.

5.3.6.4 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
  - Ability to verify conformance to the CMAC XML schema.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs
  - Ability to display messages in “raw” XML format
  - Ability to verify conformance to the CMAC XML schema
  - Ability to send Link Test messages triggered by Test Support personnel.

5.3.6.5 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.

5.3.6.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-0400

- WEA-C-RQMT-0450
- WEA-C-RQMT-0460
- WEA-C-RQMT-0500
- WEA-C-RQMT-0530
- WEA-C-RQMT-0900
- WEA-C-RQMT-0940
- WEA-C-RQMT-0950
- WEA-C-RQMT-1000
- WEA-C-RQMT-1060
- WEA-C-RQMT-1070
- WEA-C-RQMT-2580
- WEA-C-RQMT-2590
- WEA-C-RQMT-2630
- WEA-C-RQMT-2810
- WEA-C-RQMT-2820
- WEA-C-RQMT-2910.

5.3.6.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).
- Link Test Period at the Federal Alert Gateway is set to 1 minute.

5.3.6.8 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 5.8: Steps for Test Case CMAS-TC-006 – Link Test Messages Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Wait for 2 minutes.	NOTE: The Federal Alert Gateway transmits at least two instances of the Link Test Message (CMAC Message #10 in Annex C*, Expected CMAC Messages*) to the CMSP Gateway and the CMSP Gateway responds to each instance with an Ack.	N/A	N/A
2	**CMSP Test Support:** Use CMSP Gateway to send CMAC Message #11 "CMSP Gateway Initiated Link Test" (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
3	**Federal Test Support:** View Federal Alert Gateway message log**.**	The Federal Alert Gateway message log contains at least two Ack responses from the CMSP Gateway sent in response to two instances of CMAC Message #10. The Federal Alert Gateway message log contains CMAC Message #11(Annex C, *Expected CMAC Messages*), and does not contain any messages from the CMSP Gateway following CMAC Message #11.	• RMQT-0500 • RQMT-0530 • RQMT-0900 • RQMT-0940 • RQMT-0950 • RQMT-2810 • RQMT-2820	
4	**Federal Test Support:** Verify that the received CMAC Link Test message conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
5	**Federal Test Support & CMSP Test Support:** Federal Test Support verifies with the CMSP Test Support that the received CMAC Link Test message contains the mandatory message elements and associated values transmitted by the CMSP Gateway.	The CMAC message contains the following message elements and values as defined in Table C.8: *CMAC Message #11 Expected Messages & Values*.	• RQMT-2580	
6	**CMSP Test Support:** View CMSP Gateway message log**.**	The CMSP Gateway message log contains at least two instances of CMAC Message #10 (Annex C, *Expected CMAC Messages*) and an Ack response from the Federal Alert Gateway sent in response to CMAC Message #11 (Ack Message #4 in Annex D, *Expected ACK Messages*).	• RQMT-0400 • RQMT-0450 • RQMT-0460 • RQMT-1000 • RQMT-1060 • RQMT-1070 • RQMT-2910	
7	**CMSP Test Support:** Verify that the first received CMAC Link Test message conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
8	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the first received CMAC Link Test message contains the mandatory message elements and associated values transmitted by the Federal Alert Gateway.	The CMAC message contains the following message elements and values as defined in Table C.7: *CMAC Message #10 Expected Messages & Values*.	• RQMT-2580	
9	**CMSP Test Support:** Verify that the received Ack message (step 6) from the Federal Alert Gateway conforms to the CMAC XML schema.	The Ack message has no errors.	• RQMT-2630	
10	**CMSP Test Support & Federal Test Support:** CMSP Test Support verifies with the Federal Test Support that the received Ack message contains the mandatory message elements and associated values transmitted by the Federal Alert Gateway.	The Ack message contains the following message elements and values defined in Table D.2: *Ack Message #4 Expected Messages & Values*.	• RQMT-2590	

5.3.7 CMAS-TC-007 – Transmission Control Test

The purpose of the Transmission Control test procedure (CMAS-TC-007) is to test the requirements associated with controlling the transmission of messages across the interface between the Federal Alert Gateway and the CMSP Gateway. The procedure will test transmission of the Transmission Control – Cease and Transmission Control – Resume messages from a CMSP Gateway, reception of the messages at the Federal Alert Gateway, logging of the messages, proper message format, and message responses. This test case also verifies the Federal Alert Gateway that has received a Transmission Control Cease from a CMSP Gateway would still acknowledge the Link Test message if sent by that CMSP Gateway.

5.3.7.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway A
- CMSP Gateway B (optional).

5.3.7.2 Notes

The message transmission is controlled by transmission control CMAC messages sent from the CMSP Gateway to the Federal Alert Gateway. There are two types of transmission control messages: Transmission Control – Cease and Transmission Control – Resume.

The following test procedure tests the interface between a Federal Alert Gateway and CMSP Gateways. The test procedure can be conducted using a single CMSP Gateway (CMSP Gateway A) or two CMSP Gateways (CMSP Gateways A and B). When conducting the test with only one CMSP Gateway, complete test steps 1 through 10. When conducting the test with two CMSP Gateways, complete test steps 1 through 11. If only one CMSP Gateway is used, requirement WEA-C-RQMT-0490 is not tested.

Step #3 and the verification thereof in step #5 may be skipped if the CMSP Gateway does not support the optional CMSP Gateway initiated Link Test message.

Each test step is labeled to indicate which test personnel takes the required actions for that step.

5.3.7.3 Test Tools

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

- Alert Origination Simulator.

5.3.7.4 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
  - Ability to verify conformance to the CMAC XML schema.
- CMSP Gateway A Test Capabilities:
  - Ability to display message logs
  - Ability to send Link Test, Transmission Control – Cease and Transmission Control - Resume messages triggered by Test Support personnel.
- CMSP Gateway B Test Capabilities:
  - Ability to display message logs.

5.3.7.5 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 A
- CMSP Test Support B (optional).

NOTE: The CMSP Test Support A and CMSP Test Support B roles may be conducted by the same personnel.

5.3.7.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-0460
- WEA-C-RQMT-0490 (addressed only when using CMSP Gateways A and B)
- WEA-C-RQMT-0500
- WEA-C-RQMT-0510
- WEA-C-RQMT-0520
- WEA-C-RQMT-0560
- WEA-C-RQMT-0900
- WEA-C-RQMT-0920
- WEA-C-RQMT-0930

- WEA-C-RQMT-2610
- WEA-C-RQMT-2620
- WEA-C-RQMT-2630
- WEA-C-RQMT-2910.

5.3.7.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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).
- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

  NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.7.8 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 5.9: Steps for Test Case CMAS-TC-007 – Transmission Control Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**CMSP Test Support A:** Use CMSP Gateway A to send CMAC Message #12 “Transmission Control – Cease” (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. Receipt of this Ack at CMSP Gateway A should be verified prior to moving to the next step.	N/A	N/A
2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 “Imminent Alert” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway does not send a message to CMSP Gateway A.	N/A	N/A
3	**CMSP Test Support A:** Use CMSP Gateway A to send CMAC Message #11 “CMSP Gateway Initiated Link Test” (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. Receipt of this Ack at CMSP Gateway A should be verified prior to moving to the next step.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
4	**CMSP Test Support A:** Use CMSP Gateway A to send CMAC Message #13 “Transmission Control – Resume” (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. Receipt of this Ack at CMSP Gateway A should be verified prior to moving to the next step.	N/A	N/A
5	**Federal Test Support:** View Federal Alert Gateway message log.	The Federal Alert Gateway message log contains CMAC Message #12, CMAC Message #11, and CMAC Message #13 (Annex C, *Expected CMAC Messages*).	• RQMT-0500 • RQMT-0510 • RQMT-0520 • RQMT-0900 • RQMT-0920 • RQMT-0930	
6	**Federal Test Support:** Verify that the first received CMAC message (CMAC Message #12) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
7	**Federal Test Support:** Verify that the third received CMAC message (CMAC Message #13) conforms to the CMAC XML schema.	The CMAC message has no errors.	• RQMT-2630	
8	**Federal Test Support & CMSP Test Support:** Federal Test Support verifies with the CMSP Test Support that the first received CMAC message (CMAC Message #12) contains the mandatory message elements and associated values transmitted by the CMSP Gateway.	The CMAC message contains the following message elements and values as defined in Table C.9: *CMAC Message #12 Expected Messages & Values*.	• RQMT-2610	
9	**Federal Test Support & CMSP Test Support:** Federal Test Support verifies with the CMSP Test Support that the third received CMAC message (CMAC Message #13) contains the mandatory message elements and associated values transmitted by the CMSP Gateway.	The CMAC message contains the following message elements and values as defined in Table C.10: *CMAC Message #13 Expected Messages & Values*.	• RQMT-2620	
10	**CMSP Test Support A:** View CMSP Gateway A message log.	The CMSP Gateway A message log contains three Ack responses from the Federal Alert Gateway, sent in response to CMAC Message #12, CMAC Message #11, and CMAC Message #13.	• RQMT-0460 • RQMT-0560 • RQMT-2910	

NOTE: Only complete the following test step if two CMSP Gateways (CMSP Gateways A and B) are being tested. If only one CMSP Gateway is being tested, the test procedure ends here.

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
11	**CMSP Test Support B:** View CMSP Gateway B message log.	The CMSP Gateway B message log contains CMAC message #1 (Annex C, *Expected CMAC Messages*).	• RQMT-0490	

NOTE: CMSP Gateway B receives CMAC message #1 after Step #2.

5.3.8 CMAS-TC-008 – General Connectivity Test via Link Test Message

The purpose of the General Connectivity test procedure (CMAS-TC-008) is to test the requirements associated with establishing connections between the Federal Alert Gateway and the CMSP Gateway. The procedure will test connection establishment at startup and after a network failure. The test case is based upon the optional CMSP Gateway initiated Link Test message. Any CMSP Gateway that does not support the CMSP Gateway initiated Link Test message functionality should use CMAS-TC-009 instead of this test case.

5.3.8.1 Items to Be Tested

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

- Federal Alert Gateway 1
- Federal Alert Gateway 2
- CMSP Gateway A
- CMSP Gateway B (optional).

5.3.8.2 Notes

Establishment and verification of a connection between the Federal Alert Gateway and the CMSP Gateway is a precursor to transmitting CMAC messages. This test verifies actions initiated by both the Federal Alert Gateway and the CMSP Gateway. System operation when an entity or the connectivity to an entity is not available is also tested.

The following test procedure tests the connection between two Federal Alert Gateways (1 and 2) and two CMSP Gateways (A and B). When conducting the test with only one CMSP Gateway, actions and expected results relevant to CMSP Gateway B should not be used. Each test step is labeled to indicate which test personnel takes the required actions for that step.

This test is only required for CMSPs with CMSP Gateways supporting the optional CMSP initiated Link Test message. For other CMSPs the test is optional.

5.3.8.3 Test Tools

No test tools are necessary to complete this test procedure.

5.3.8.4 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 enable and disable the connection to network
  - Ability to take offline and to restart the Federal Alert Gateway application

  - Ability to display message logs
  - Ability to display error logs.
- CMSP Gateway Test Capabilities:
  - Ability to send Link Test messages triggered by Test Support personnel
  - Ability to take offline and to restart the CMSP Gateway application
  - Ability to display message logs
  - Ability to display error logs.

  NOTE: An error log is any kind of viewable log or other indication that IPsec or TCP connections have failed to establish.

5.3.8.5 Test Personnel

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

- Federal Test Support 1
- Federal Test Support 2
- CMSP Test Support A
- CMSP Test Support B.

5.3.8.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0300
- WEA-C-RQMT-0310
- WEA-C-RQMT-0330
- WEA-C-RQMT-0710
- WEA-C-RQMT-0800
- WEA-C-RQMT-0840
- WEA-C-RQMT-0850
- WEA-C-RQMT-3320
- WEA-C-RQMT-3330.

5.3.8.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- The Federal Alert Gateways have passed testing for Federal Alert Gateway Profile Data (Test Case CMAS-TC-101) and the CMSP Gateway(s) have passed testing for CMSP Gateway Profile Data (Test Case CMAS-TC-201).
- 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 CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateways are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateways is set to 1 minute.

- The Federal Alert Gateways and the CMSP Gateway(s) are offline (i.e., not capable of establishing a network connection).
- Before this test case can be executed, all entry criteria under Clause 4.5, *Pre-Test Configuration Information,* must be completed. This ensures that all parties involved in testing activities are ready and interface testing can start without delay.

5.3.8.8 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 5.10: Steps for Test Case CMAS-TC-008 – General Connectivity Test via Link Test Message

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**CMSP Test Support A:** Initiate startup procedures for CMSP Gateway A.	NOTE: CMSP Gateway A attempts to establish connection with both Federal Alert Gateways but fails after a timeout period, because the Federal Alert Gateways are offline.	N/A	N/A
2	**CMSP Test Support A:** View the error log on CMSP Gateway A.	CMSP Gateway A error log contains entries for failure to establish IPsec connections with both Federal Alert Gateways.	• RQMT-3330	
3	**CMSP Test Support B:** Initiate startup procedures for CMSP Gateway B.	NOTE: CMSP Gateway B attempts to establish connection with both Federal Alert Gateways but fails after a timeout period, because the Federal Alert Gateways are offline.	N/A	N/A
4	**CMSP Test Support B:** View the error log on CMSP Gateway B.	CMSP Gateway B error log contains entries for failure to establish IPsec connections with both Federal Alert Gateways.	• RQMT-3330	
5	**CMSP Test Support A:** Bring CMSP Gateway A to offline state.	NOTE: CMSP Gateway A will be offline, not accepting any connections from Federal Alert Gateways.	N/A	N/A
6	**CMSP Test Support B:** Bring CMSP Gateway B to offline state.	NOTE: CMSP Gateway B will be offline, not accepting any connections from Federal Alert Gateways.	N/A	N/A
7	**Federal Test Support 1:** Initiate startup procedures for Federal Alert Gateway 1.	NOTE: Federal Alert Gateway 1 attempts to establish connection with both CMSP Gateways but fails after a timeout period, because the CMSP Gateways are offline.	N/A	N/A
8	**Federal Test Support 1:** View the error log on Federal Alert Gateway 1.	Federal Alert Gateway 1 error log contains entries for failure to establish IPsec connections with both CMSP Gateways.	• RQMT-3330	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
9	**Federal Test Support 2:** Initiate startup procedures for Federal Alert Gateway 2.	NOTE: Federal Alert Gateway 2 attempts to establish connection with both CMSP Gateways but fails after a timeout period, because the CMSP Gateways are offline.	N/A	N/A
10	**Federal Test Support 2:** View the error log on Federal Alert Gateway 2.	Federal Alert Gateway 2 error log contains entries for failure to establish IPsec connections with both CMSP Gateways.	• RQMT-3330	
11	**CMSP Test Support A:** Initiate startup procedures for CMSP Gateway A.	NOTE: Connections to both Federal Alert Gateways are established.	N/A	N/A
12	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
13	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack response from Federal Alert Gateway 1 in response to the Link Test message.	• RQMT-0330 • RQMT-0800	
14	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
15	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack response from Federal Alert Gateway 2 in response to the Link Test message.	• RQMT-0330 • RQMT-0800	
16	**CMSP Test Support B:** Initiate startup procedures for CMSP Gateway B.	NOTE: Connections to both Federal Alert Gateways are established.	N/A	N/A
17	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
18	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack response from Federal Alert Gateway 1 in response to the Link Test message.	• RQMT-0330 • RQMT-0800	
19	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
20	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack response from Federal Alert Gateway 2 in response to the Link Test message.	• RQMT-0330 • RQMT-0800	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
21	**Federal Test Support 1:** Bring Federal Alert Gateway 1 to offline state.	NOTE: Connections to both CMSP Gateways are terminated.	N/A	N/A
22	**Federal Test Support 2:** Bring Federal Alert Gateway 2 to offline state.	NOTE: Connections to both CMSP Gateways are terminated.	N/A	N/A
23	**Federal Test Support 1:** Initiate startup procedures for Federal Alert Gateway 1.	NOTE: Connections to both CMSP Gateways are reestablished.	N/A	N/A
24	**Federal Test Support 1:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks.	N/A	N/A
25	**Federal Test Support 1:** View Federal Alert Gateway 1 message log.	Federal Alert Gateway 1 message log contains an Ack response from CMSP Gateway A and an Ack response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0300 • RQMT-0710 • RQMT-0850	
26	**Federal Test Support 2:** Initiate startup procedures for Federal Alert Gateway 2.	NOTE: Connections to both CMSP Gateways are reestablished.	N/A	N/A
27	**Federal Test Support 2:** Wait for 1 minute.	NOTE: Federal Alert Gateway 2 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks.	N/A	N/A
28	**Federal Test Support 2:** View Federal Alert Gateway 2 message log.	Federal Alert Gateway 2 message log contains an Ack response from CMSP Gateway A and an Ack response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0300 • RQMT-0710 • RQMT-0850	
29	**Federal Test Support 1:** Disable Federal Alert Gateway 1 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 1 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
30	**Federal Test Support 2:** Disable Federal Alert Gateway 2 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 2 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
31	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
32	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
33	**CMSP Test Support A:** View the error log on CMSP Gateway A.	CMSP Gateway A error log contains entries for failure to establish TCP or IPsec connections with both Federal Alert Gateways.	• RQMT-3320	
34	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
35	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
36	**CMSP Test Support B:** View the error log on CMSP Gateway B.	CMSP Gateway B error log contains entries for failure to establish TCP connections with both Federal Alert Gateways.	• RQMT-3320	
37	**Federal Test Support 1:** Reconnect Federal Alert Gateway 1 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
38	**Federal Test Support 2:** Reconnect Federal Alert Gateway 2 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
39	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
40	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack response from Federal Alert Gateway 1 in response to the Link Test message.	• RQMT-0840	
41	**CMSP Test Support A:** Use CMSP Gateway A to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
42	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack response from Federal Alert Gateway 2 in response to the Link Test message.	• RQMT-0840	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
43	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
44	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack response from Federal Alert Gateway 1 in response to the Link Test message.	• RQMT-0840	
45	**CMSP Test Support B:** Use CMSP Gateway B to send a Link Test message (CMAC Message #11 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack.	N/A	N/A
46	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack response from Federal Alert Gateway 2 in response to the Link Test message.	• RQMT-0840	
47	**Federal Test Support 1:** Disable Federal Alert Gateway 1 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 1 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
48	**Federal Test Support 2:** Disable Federal Alert Gateway 2 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 2 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
49	**Federal Test Support 1 and Federal Test Support 2:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 and Federal Alert Gateway 2 attempt to transmit Link Test messages but fail after a timeout period.	N/A	N/A
50	**Federal Test Support 1:** View the error log on Federal Alert Gateway 1.	Federal Alert Gateway 1 error log contains entries for failure to establish TCP connections with both CMSP Gateways.	• RQMT-3320	
51	**Federal Test Support 2:** View the error log on Federal Alert Gateway 2.	Federal Alert Gateway 2 error log contains entries for failure to establish TCP connections with both CMSP Gateways.	• RQMT-3320	
52	**Federal Test Support 1:** Reconnect Federal Alert Gateway 1 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
53	**Federal Test Support 2:** Reconnect Federal Alert Gateway 2 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
54	**Federal Test Support 1:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
55	**Federal Test Support 1:** View Federal Alert Gateway 1 message log.	Federal Alert Gateway 1 message log contains an Ack response from CMSP Gateway A and an Ack response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0310	
56	**Federal Test Support 2:** View Federal Alert Gateway 2 message log.	Federal Alert Gateway 2 message log contains an Ack response from CMSP Gateway A and an Ack response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0310	

5.3.9 CMAS-TC-009 – General Connectivity Test via Transmission Control Resume Message

The purpose of the General Connectivity test procedure (CMAS-TC-009) is to test the requirements associated with establishing connections between the Federal Alert Gateway and the CMSP Gateway. The procedure will test connection establishment at startup and after a network failure. The test case is based upon the Transmission Control Resume message. This test case verifies the same requirements as CMAS-TC-008, so this test case should not be used if CMAS-TC-008 has already been completed.

5.3.9.1 Items to Be Tested

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

- Federal Alert Gateway 1
- Federal Alert Gateway 2
- CMSP Gateway A
- CMSP Gateway B (optional).

5.3.9.2 Notes

Establishment and verification of a connection between the Federal Alert Gateway and the CMSP Gateway is a precursor to transmitting CMAC messages. This test verifies actions initiated by both the Federal Alert Gateway and the CMSP Gateway. System operation when an entity or the connectivity to an entity is not available is also tested.

The following test procedure tests the connection between two Federal Alert Gateways (1 and 2) and two CMSP Gateways (A and B). When conducting the test with only one CMSP Gateway, actions and expected results relevant to CMSP Gateway B should not be used. Each test step is labeled to indicate which test personnel takes the required actions for that step.

5.3.9.3 Test Tools

No test tools are necessary to complete this test procedure.

5.3.9.4 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 enable and disable the connection to network
  - Ability to take offline and to restart the Federal Alert Gateway application
  - Ability to display message logs
  - Ability to display error logs.
- CMSP Gateway Test Capabilities:
  - Ability to send Transmission Control - Resume messages triggered by Test Support personnel
  - Ability to take offline and to restart CMSP Gateway application
  - Ability to display message logs
  - Ability to display error logs.

    NOTE: An error log is any kind of viewable log or other indication that IPsec or TCP connections have failed to establish.

5.3.9.5 Test Personnel

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

- Federal Test Support 1
- Federal Test Support 2
- CMSP Test Support A
- CMSP Test Support B.

5.3.9.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point “C” Interface Requirements*.

- WEA-C-RQMT-0300
- WEA-C-RQMT-0310
- WEA-C-RQMT-0330
- WEA-C-RQMT-0710
- WEA-C-RQMT-0800
- WEA-C-RQMT-0840
- WEA-C-RQMT-0850
- WEA-C-RQMT-3320
- WEA-C-RQMT-3330.

5.3.9.7 Prerequisites Conditions

The following prerequisite conditions must be established prior to performing this test procedure:

- 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 Gateways have passed testing for Federal Alert Gateway Profile Data (Test Case CMAS-TC-101) and the CMSP Gateway(s) have passed testing for CMSP Gateway Profile Data (Test

Case CMAS-TC-201).

- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateways are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateways is set to 1 minute.
- The Federal Alert Gateways and the CMSP Gateway(s) are offline (i.e., not capable of establishing a network connection).
- Before this test case can be executed, all entry criteria under Clause 4.5, *Pre-Test Configuration Information,* must be completed. This ensures that all parties involved in testing activities are ready and that interface testing can start without delay.

5.3.9.8 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 5.11: Steps for Test Case CMAS-TC-009 – General Connectivity Test via Transmission Control Resume Message

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**CMSP Test Support A:** Initiate startup procedures for CMSP Gateway A.	NOTE: CMSP Gateway A attempts to establish connection with both Federal Alert Gateways but fails after a timeout period, because the Federal Alert Gateways are offline.	N/A	N/A
2	**CMSP Test Support A:** View the error log on CMSP Gateway A.	CMSP Gateway A error log contains entries for failure to establish IPsec connections with both Federal Alert Gateways.	• RQMT-3330	
3	**CMSP Test Support B:** Initiate startup procedures for CMSP Gateway B.	NOTE: CMSP Gateway B attempts to establish connection with both Federal Alert Gateways but fails after a timeout period, because the Federal Alert Gateways are offline.	N/A	N/A
4	**CMSP Test Support B:** View the error log on CMSP Gateway B.	CMSP Gateway B error log contains entries for failure to establish IPsec connections with both Federal Alert Gateways.	• RQMT-3330	
5	**CMSP Test Support A:** Bring CMSP Gateway A to offline state.	NOTE: CMSP Gateway A will be offline, not accepting any connections from Federal Alert Gateways.	N/A	N/A
6	**CMSP Test Support B:** Bring CMSP Gateway B to offline state.	NOTE: CMSP Gateway B will be offline, not accepting any connections from Federal Alert Gateways.	N/A	N/A
7	**Federal Test Support 1:** Initiate startup procedures for Federal Alert Gateway 1.	NOTE: Federal Alert Gateway 1 attempts to establish connection with both CMSP Gateways but fails after a timeout period, because the CMSP Gateways are offline.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
8	**Federal Test Support 1:** View the error log on Federal Alert Gateway 1.	Federal Alert Gateway 1 error log contains entries for failure to establish IPsec connections with both CMSP Gateways.	• RQMT-3330	
9	**Federal Test Support 2:** Initiate startup procedures for Federal Alert Gateway 2.	NOTE: Federal Alert Gateway 2 attempts to establish connection with both CMSP Gateways but fails after a timeout period, because the CMSP Gateways are offline.	N/A	N/A
10	**Federal Test Support 2:** View the error log on Federal Alert Gateway 2.	Federal Alert Gateway 2 error log contains entries for failure to establish IPsec connections with both CMSP Gateways.	• RQMT-3330	
11	**CMSP Test Support A:** Initiate startup procedures for CMSP Gateway A.	NOTE: Connections to both Federal Alert Gateways are established.	N/A	N/A
12	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
13	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack or Error response from Federal Alert Gateway 1 in response to the Transmission Control - Resume message.	• RQMT-0330 • RQMT-0800	
14	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
15	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack or Error response from Federal Alert Gateway 2 in response to the Transmission Control - Resume message.	• RQMT-0330 • RQMT-0800	
16	**CMSP Test Support B:** Initiate startup procedures for CMSP Gateway B.	NOTE: Connections to both Federal Alert Gateways are established.	N/A	N/A
17	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control – Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
18	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack or Error response from Federal Alert Gateway 1 in response to the Transmission Control - Resume message.	• RQMT-0330 • RQMT-0800	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
19	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
20	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack or Error response from Federal Alert Gateway 2 in response to the Transmission Control - Resume message.	• RQMT-0330 • RQMT-0800	
21	**Federal Test Support 1:** Bring Federal Alert Gateway 1 to offline state.	NOTE: Connections to both CMSP Gateways are terminated.	N/A	N/A
22	**Federal Test Support 2:** Bring Federal Alert Gateway 2 to offline state.	NOTE: Connections to both CMSP Gateways are terminated.	N/A	N/A
23	**Federal Test Support 1:** Initiate startup procedures for Federal Alert Gateway 1.	NOTE: Connections to both CMSP Gateways are reestablished.	N/A	N/A
24	**Federal Test Support 1:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks or Errors.	N/A	N/A
25	**Federal Test Support 1:** View Federal Alert Gateway 1 message log.	Federal Alert Gateway 1 message log contains an Ack or Error response from CMSP Gateway A and an Ack or Error response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0300 • RQMT-0710 • RQMT-0850	
26	**Federal Test Support 2:** Initiate startup procedures for Federal Alert Gateway 2.	NOTE: Connections to both CMSP Gateways are reestablished.	N/A	N/A
27	**Federal Test Support 2:** Wait for 1 minute.	NOTE: Federal Alert Gateway 2 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks or Errors.	N/A	N/A
28	**Federal Test Support 2:** View Federal Alert Gateway 2 message log.	Federal Alert Gateway 2 message log contains an Ack or Error response from CMSP Gateway A and an Ack or Error response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0300 • RQMT-0710 • RQMT-0850	
29	**Federal Test Support 1:** Disable Federal Alert Gateway 1 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 1 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
30	**Federal Test Support 2:** Disable Federal Alert Gateway 2 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 2 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
31	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
32	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control – Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
33	**CMSP Test Support A:** View the error log on CMSP Gateway A.	CMSP Gateway A error log contains entries for failure to establish TCP connections with both Federal Alert Gateways.	• RQMT-3320	
34	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
35	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway attempts to transmit the message to the Federal Alert Gateway but fails after a timeout period.	N/A	N/A
36	**CMSP Test Support B:** View the error log on CMSP Gateway B.	CMSP Gateway B error log contains entries for failure to establish TCP connections with both Federal Alert Gateways.	• RQMT-3320	
37	**Federal Test Support 1:** Reconnect Federal Alert Gateway 1 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
38	**Federal Test Support 2:** Reconnect Federal Alert Gateway 2 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
39	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control – Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
40	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack or Error response from Federal Alert Gateway 1 in response to the Transmission Control - Resume message.	• RQMT-0840	
41	**CMSP Test Support A:** Use CMSP Gateway A to send a Transmission Control – Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
42	**CMSP Test Support A:** View CMSP Gateway A message log.	CMSP Gateway A message log contains an Ack or Error response from Federal Alert Gateway 2 in response to the Transmission Control - Resume message.	• RQMT-0840	
43	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 1.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
44	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack or Error response from Federal Alert Gateway 1 in response to the Transmission Control - Resume message.	• RQMT-0840	
45	**CMSP Test Support B:** Use CMSP Gateway B to send a Transmission Control - Resume message (CMAC Message #13 in Annex C, *Expected CMAC Messages*) to Federal Alert Gateway 2.	NOTE: The CMSP Gateway transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack or Error.	N/A	N/A
46	**CMSP Test Support B:** View CMSP Gateway B message log.	CMSP Gateway B message log contains an Ack or Error response from Federal Alert Gateway 2 in response to the Transmission Control - Resume message.	• RQMT-0840	
47	**Federal Test Support 1:** Disable Federal Alert Gateway 1 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 1 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
48	**Federal Test Support 2:** Disable Federal Alert Gateway 2 such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway 2 remains operational but without a network connection to either CMSP Gateway.	N/A	N/A
49	**Federal Test Support 1 and Federal Test Support 2:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 and Federal Alert Gateway 2 attempt to transmit Link Test messages but fail after a timeout period.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
50	**Federal Test Support 1:** View the error log on Federal Alert Gateway 1.	Federal Alert Gateway 1 error log contains entries for failure to establish TCP connections with both CMSP Gateways.	• RQMT-3320	
51	**Federal Test Support 2:** View the error log on Federal Alert Gateway 2.	Federal Alert Gateway 2 error log contains entries for failure to establish TCP connections with both CMSP Gateways.	• RQMT-3320	
52	**Federal Test Support 1:** Reconnect Federal Alert Gateway 1 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
53	**Federal Test Support 2:** Reconnect Federal Alert Gateway 2 to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
54	**Federal Test Support 1:** Wait for 1 minute.	NOTE: Federal Alert Gateway 1 transmits Link Test messages (CMAC Message #10 in Annex C, *Expected CMAC Messages*) to both CMSP Gateways and CMSP Gateways respond with Acks or Errors.	N/A	N/A
55	**Federal Test Support 1:** View Federal Alert Gateway 1 message log.	Federal Alert Gateway 1 message log contains an Ack or Error response from CMSP Gateway A and an Ack or Error response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0310	
56	**Federal Test Support 2:** View Federal Alert Gateway 2 message log.	Federal Alert Gateway 2 message log contains an Ack or Error response from CMSP Gateway A and an Ack or Error response from CMSP Gateway B in response to the Link Test messages.	• RQMT-0310	

5.3.10 CMAS-TC-010 – Geo-Location Filtering Test

The purpose of the Geo-Location Filtering test procedure (CMAS-TC-010) is to test the requirements associated with using geographic location codes to filter the areas to which alerts are sent.

5.3.10.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway.

5.3.10.2 Notes

The following test procedure verifies that alerts are only transmitted to selected areas when Geo Location filtering is turned on. The requirement that messages be transmitted to all areas when Geo Location filtering is turned off is verified in other test procedures.

This test is only required for CMSPs choosing to utilize geo-Location filtering. For other CMSPs, the test is optional.

5.3.10.3 Test Tools

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

- Alert Origination Simulator.

5.3.10.4 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 view Geo Location codes in the CMSP profile.
- CMSP Gateway Test Capabilities:
  - Ability to display message logs.

5.3.10.5 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.

5.3.10.6 Requirements Addressed

The following requirement from ATIS-0700037 [Ref 1] is verified by this procedure. The full requirement text is included in Annex A *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-0140.

5.3.10.7 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).
- The CMSP Profile at the Federal Alert Gateway is configured with the correct list of states for the CMSP under test and Geo Location filter option is set to "Yes".
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

  NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.10.8 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 5.12: Steps for Test Case CMAS-TC-010 – Geo-Location Filtering Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Examine CMSP profile for CMSP under test to determine which state Geo-codes are included in list of states to receive transmissions.	NOTE: Federal Alert Gateway will only send alerts to states whose geo codes are listed in the CMSP Profile.	N/A	N/A
2	**Federal Test Support:** Use *Alert Origination Simulator* to insert a 6 digit SAME code [Ref 25] corresponding to a county from one of the states listed in step 1 and to insert a 6 digit SAME code [Ref 25] corresponding to a county not from any of the states listed in step 1 into CAP Message #9 “Imminent Threat Alert for Geo-Location Filtering” (Annex B, *Input CAP Messages*) as the geocode labeled as [County Code #1].		N/A	N/A
3	**Federal Test Support:** Use *Alert Origination Simulator* to send the edited CAP Message #9 “Imminent Threat Alert for Geo-Location Filtering” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
4	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains a CMAC message corresponding to CAP Message #9 transmitted in Step 3.	• RQMT-0140	
5	**Federal Test Support:** Use *Alert Origination Simulator* to insert a 6 digit SAME code [Ref 25] corresponding to a county from one of the states listed in step 1 and to insert a 6 digit SAME code [Ref 25] corresponding to a county not from any of the states listed in step 1 into CAP Message #10 “Imminent Threat Update for Geo-Location Filtering” (Annex B, *Input CAP Messages*) as the geocode labeled as [County Code #1].		N/A	N/A
6	**Federal Test Support:** Use *Alert Origination Simulator* to send the edited CAP Message #10 “Imminent Threat Update for Geo-Location Filtering” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
7	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains a CMAC message corresponding to CAP Message #10 transmitted in Step 6.	• RQMT-0140	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
8	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #11 “Imminent Threat Cancel for Geo-Location Filtering” (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
9	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log contains a CMAC message corresponding to CAP Message #11 transmitted in Step 8.	• RQMT-0140	
10	**Federal Test Support:** Use *Alert Origination Simulator* to insert two 6 digit SAME codes [Ref 25] corresponding to two counties not from any of the states listed in step 1 into CAP Message #9 “Imminent Threat Alert for Geo-Location Filtering” (Annex B, *Input CAP Messages*) as the geocodes labeled as [County Code #1] and [County Code #2].		N/A	N/A
11	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #9 “Imminent Threat Alert for Geo-Location Filtering” (Annex B, *Input CAP Messages*) edited in step 10 to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway does not transmit the message to the CMSP Gateway, because the geocodes don’t belong to counties in the list of allowed states.	N/A	N/A
12	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log does not contain a CMAC message corresponding to CAP Message #9 as it was not transmitted to CMSP Gateway in Step 11.	• RQMT-0140	
13	**Federal Test Support:** Use *Alert Origination Simulator* to insert two 6 digit SAME codes [Ref 25] corresponding to two counties not from any of the states listed in step 1 into CAP Message #10 “Imminent Threat Update for Geo-Location Filtering” (Annex B, *Input CAP Messages*) as the geocodes labeled as [County Code #1] and [County Code #2].		N/A	N/A
14	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #10 “Imminent Threat Update for Geo-Location Filtering” (Annex B, *Input CAP Messages*) edited in step 13 to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway does not transmit the message to the CMSP Gateway, because the geocodes don’t belong to counties in the list of allowed states.	N/A	N/A
15	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log does not contain a CMAC message corresponding to CAP Message #10 as it was not transmitted to CMSP Gateway in Step 14.	• RQMT-0140	

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
16	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #11 "Imminent Threat Cancel for Geo-Location Filtering" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, referencing to CAP Message #10 transmitted in Step 14.	NOTE: The Federal Alert Gateway does not transmit the message to the CMSP Gateway, since the referenced update message was not sent to this CMSP.	N/A	N/A
17	**CMSP Test Support:** View CMSP Gateway message log.	The CMSP Gateway message log does not contain a CMAC message corresponding to CAP Message #11 as it was not transmitted to CMSP Gateway in Step 16.	• RQMT-0140	

5.3.11 CMAS-TC-011 – Messaging Queuing Test

The purpose of the Message Queuing test procedure (CMAS-TC-011) is to test the requirements associated with the order in which messages queued up to be sent are transmitted, precedence given to National messages, and removal of outdated messages in the message queue.

5.3.11.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway A
- CMSP Gateway B (optional).

5.3.11.2 Notes

The following test procedure tests the connection between a Federal Alert Gateway and a CMSP Gateway and verifies that National messages are moved to the head of the message queue and other messages are transmitted on a First In-First Out (FIFO) basis. Each test step is labeled to indicate which test personnel takes the required actions for that step.

5.3.11.3 Test Tools

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

- Alert Origination Simulator.

5.3.11.4 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.
- CMSP Gateway Test Capabilities:
    - Ability to display message logs
    - Ability to send Transmission Control – Cease and Transmission Control - Resume messages

triggered by Test Support personnel.

5.3.11.5 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 A
- CMSP Test Support B (optional).

5.3.11.6 Requirements Addressed

The following requirements from ATIS-0700037 [Ref 1] are verified by this procedure. The full requirement text is included in Annex A, *Summary of Reference Point "C" Interface Requirements*.

- WEA-C-RQMT-1200
- WEA-C-RQMT-1210
- WEA-C-RQMT-1300
- WEA-C-RQMT-1310
- WEA-C-RQMT-1320.

5.3.11.7 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).
- The Federal Alert Gateway and CMSP Gateway have passed testing for basic transmission of messages (CMAS-TC-001, CMAS-TC-003, CMAS-TC-004, and CMAS-TC-007).
- The CMSP Gateway and the CMSP Gateway profile in the Federal Alert Gateway are both configured such that Geo-Location Filtering is turned off (i.e., accepting messages for all regions).
- Link Test Period at the Federal Alert Gateway is set to 120 minutes.

NOTE: This is to prevent periodic Link Test messages from interfering with the test procedure.

5.3.11.8 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 5.13: Steps for Test Case CMAS-TC-011 – Message Queuing Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Disable Federal Alert Gateway such that it cannot exchange CMAC messages with the CMSP Gateways.	NOTE: Federal Alert Gateway remains operational but without a network connection to a CMSP Gateway.	N/A	N/A
2	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 "Imminent Threat Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time-1] set to at least 1 hour later than current time.	NOTE: Federal Alert Gateway attempts to transmit the message but fails after a timeout period and queues the message.	N/A	N/A
3	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #2 "National Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time 2] set to at least 1 hour later than current time.	NOTE: Federal Alert Gateway attempts to transmit the message but fails after a timeout period and queues the message.	N/A	N/A
4	**Federal Test Support:** Wait for 4 minutes.	NOTE: This will ensure all retransmit attempts are completed and the messages are queued.	N/A	N/A
5	**Federal Test Support:** Reconnect Federal Alert Gateway to the network.	NOTE: Network connection to the CMSP Gateways is restored.	N/A	N/A
6	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #3 "AMBER Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A responds with an Ack for each message.	N/A	N/A
7	**CMSP Test Support A:** View CMSP Gateway A message log.	The CMSP Gateway A message log contains CMAC Message #2 National Alert, CMAC Message #1 Imminent Threat Alert, and CMAC Message #3 AMBER Alert, received in this order.	• RQMT-1200 • RQMT 1210 • RQMT 1300 • RQMT 1320	
8	**CMSP Test Support A:** Use CMSP Gateway A to send CMAC Message #12 "Transmission Control – Cease" (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. This step is used to build a queue of unsent messages.	N/A	N/A
9	**(Skip this step if conducting this test with only one CMSP Gateway)** **CMSP Test Support B:** Use CMSP Gateway B to send CMAC Message #12 "Transmission Control – Cease" (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway B transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. This step is used to build a queue of unsent messages.	N/A	N/A

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
10	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 "Imminent Threat Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time 1] set to at least 1 hour later than current time.	NOTE: Since message transmission is temporarily suspended, this message is stored in the Federal Alert Gateway message queue.	N/A	N/A
11	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #3 "AMBER Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time 3] set to at least 1 hour later than current time.	NOTE: Since message transmission is temporarily suspended, this message is stored in the Federal Alert Gateway message queue.	N/A	N/A
12	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #8 "Imminent Threat Cancel" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: This message will remove Imminent Threat Alert message in Step 10 from message queue.	N/A	N/A
13	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #6 "Amber Update" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time 6] set to at least 1 hour later than current time.	NOTE: Since message transmission is temporarily suspended, this message is stored in the Federal Alert Gateway message queue. This message will remove Amber Alert message in Step 11 from message queue.	N/A	N/A
14	**Federal Test Support:** Use *Alert Origination Simulator* to send CAP Message #1 "Imminent Threat Alert" (Annex B, *Input CAP Messages*) to the Federal Alert Gateway, with [Expires Date-Time 1] set to ***1 minute*** later than current time.	NOTE: Since message transmission is suspended, this message is stored in the Federal Alert Gateway message queue.	N/A	N/A
15	**Federal Test Support:** Wait for 2 minutes.	NOTE: Imminent Threat Alert message in Step 14 will expire and will be removed from message queue.	N/A	N/A
16	**CMSP Test Support A:** Use CMSP Gateway A to send CMAC Message #13 "Transmission Control – Resume" (Annex C, *Expected CMAC Messages*) to the Federal Alert Gateway.	NOTE: CMSP Gateway A transmits the message to the Federal Alert Gateway and the Federal Alert Gateway responds with an Ack. Federal Alert Gateway transmits messages stored in queue to CMSP Gateway A and CMSP Gateway A responds with an Ack for each message.	N/A	N/A
17	**CMSP Test Support A:** View CMSP Gateway A message log.	The CMSP Gateway A message log contains only CMAC Message #6 Amber Update, corresponding to CAP Message #6 in step 13.	• RQMT-1310	

5.3.12 CMAS-TC-012 – CAP Retrieval Test

The purpose of the CAP Retrieval Test procedure (CMAS-TC-012) is to test the requirements associated with sending the CAP Retrieval and response messages. The procedure will test transmission of the CAP Retrieval request message from the CMSP Gateway and the delivery of the requested CAP message by the Federal Alert Gateway. This test case is optional for any CMSP Gateway that does not support the CAP retrieval functionality.

5.3.12.1 Items to Be Tested

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

- Federal Alert Gateway
- CMSP Gateway.

5.3.12.2 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.

5.3.12.3 Test Tools

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

- Alert Origination Simulator.

5.3.12.4 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 CAP Retrieval request command from user
    - Ability to display message logs
    - Ability to display messages in “raw” XML format.

5.3.12.5 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.

5.3.12.6 Requirements Addressed

There is no requirement number associated with the CAP Retrieval message and call flow in ATIS-0700037 [Ref 1].

5.3.12.7 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).
- The CMSP Gateway has been provisioned to retrieve the CAP 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.

5.3.12.8 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 5.14: Steps for Test Case CMAS-TC-012 – CAP Retrieval Test

Step #	Action Performed:	Expected Results	Rqmt ID (WEA-C-RQMT #)	Step Completion (Pass, Fail, N/A)
1	**Federal Test Support:** Use *Alert Origination Simulator* to send B.1 CAP Message “Imminent Threat Alert” #1 (Annex B, *Input CAP Messages*) to the Federal Alert Gateway.	NOTE: The Federal Alert Gateway transmits the message to the CMSP Gateway and the CMSP Gateway responds with an Ack.	N/A	N/A
2	**CMSP Test Support:** The CMSP Gateway sends a HyperText Transfer Protocol (HTTP) GET with the CMAC_cap_alert_uri provided in the CMAC Alert message.	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 CMAC_cap_alert_uri identifying the location of the original CAP message.	• RQMT-2720	
4	**CMSP Test Support:** View CMSP Gateway message log.	Verify that the message body contains the actual original CAP Message “Imminent Threat Alert” conforming to CAP Message #1 – Imminent Threat Alert (Annex B, *Input CAP Messages*).	• RQMT-2720	

6 Cross Reference of Requirements to Test Cases

The following table provides a cross reference between ATIS-0700037 [Ref 1] Reference Point “C” requirements, the applicable gateway, the verification method, and the associated test cases.

A summary of ATIS-0700037 [Ref 1] Reference Point “C” requirements is provided in Annex A, *Summary of Reference Point “C” Interface Requirements*.

Under the Applicability heading, an “X” in the column labeled “F” indicates that the requirement is applicable to the Federal Alert Gateway, and an “X” in the column labeled “C” indicates that the requirement is applicable to the CMSP Gateway. For requirements that are applicable to both Gateways, an “X” is entered in both columns.

The columns under the Verification Method heading indicate the various verification methods that are applicable to ATIS-0700037 [Ref 1] Reference Point “C” requirements. The definition of the verification methods is contained in Clause 3, *Definitions*. Any requirement may have more than one associated verification method. The definitions of the columns under the Verification Method heading are as follows:

- An “X” in the column labeled “I” indicates that the Inspection Verification Method will be utilized.
- An “X” in the column labeled “A” indicates that the Analysis Verification Method will be utilized.
- An “X” in the column labeled “D” indicates that the Demonstration Verification Method will be utilized.
- An “X” in the column labeled “R” indicates that the Test Verification Method will be utilized.

Table 6.1: Cross Reference Matrix of Requirements to Test Cases

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-0100	X		X				CMAS-TC-101
WEA-C-RQMT-0110	X		X				CMAS-TC-101
WEA-C-RQMT-0120	X		X				CMAS-TC-101
WEA-C-RQMT-0130	X				X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004
WEA-C-RQMT-0140	X				X		CMAS-TC-010
WEA-C-RQMT-0200	X		X				CMAS-TC-101
WEA-C-RQMT-0300	X				X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0310	X				X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0320	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0330	X				X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0400	X				X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005 CMAS-TC-006
WEA-C-RQMT-0410	X				X		CMAS-TC-001
WEA-C-RQMT-0414	X				X		CMAS-TC-001
WEA-C-RQMT-0416	X				X		CMAS-TC-001
WEA-C-RQMT-0420	X				X		CMAS-TC-003
WEA-C-RQMT-0425	X				X		CMAS-TC-003
WEA-C-RQMT-0427	X				X		CMAS-TC-003
WEA-C-RQMT-0428	X				X		CMAS-TC-003
WEA-C-RQMT-0430	X				X		CMAS-TC-004
WEA-C-RQMT-0440	X				X		CMAS-TC-005

ATIS-0700037 Reference Point "C" Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-0450	X				X		CMAS-TC-006
WEA-C-RQMT-0460	X				X		CMAS-TC-006 CMAS-TC-007
WEA-C-RQMT-0470	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0480	X				X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005
WEA-C-RQMT-0490	X				X		CMAS-TC-007
WEA-C-RQMT-0493	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0496	X				X		CMAS-TC-001
WEA-C-RQMT-0500	X				X		CMAS-TC-001 CMAS-TC-006 CMAS-TC-007
WEA-C-RQMT-0510	X				X		CMAS-TC-007
WEA-C-RQMT-0520	X				X		CMAS-TC-007
WEA-C-RQMT-0530	X				X		CMAS-TC-006
WEA-C-RQMT-0540	X				X		CMAS-TC-001
WEA-C-RQMT-0550	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0560	X				X		CMAS-TC-007
WEA-C-RQMT-0600		X	X				CMAS-TC-201
WEA-C-RQMT-0700		X	X				CMAS-TC-201
WEA-C-RQMT-0710		X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0720		X	X				CMAS-TC-201
WEA-C-RQMT-0800		X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0820		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0830		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0840		X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0850		X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-0900		X			X		CMAS-TC-001 CMAS-TC-006 CMAS-TC-007

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-0910		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-0920		X			X		CMAS-TC-007
WEA-C-RQMT-0930		X			X		CMAS-TC-007
WEA-C-RQMT-0940		X			X		CMAS-TC-006
WEA-C-RQMT-0950		X			X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005 CMAS-TC-006
WEA-C-RQMT-1000		X			X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005 CMAS-TC-006
WEA-C-RQMT-1010		X			X		CMAS-TC-001
WEA-C-RQMT-1020		X			X		CMAS-TC-003
WEA-C-RQMT-1030		X			X		CMAS-TC-004
WEA-C-RQMT-1040		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1050		X			X		CMAS-TC-005
WEA-C-RQMT-1060		X			X		CMAS-TC-006
WEA-C-RQMT-1070		X			X		CMAS-TC-006
WEA-C-RQMT-1080		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1090		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1100		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1110		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1120		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1150		X			X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004
WEA-C-RQMT-1200	X				X		CMAS-TC-011
WEA-C-RQMT-1210	X				X		CMAS-TC-011
WEA-C-RQMT-1300	X				X		CMAS-TC-011
WEA-C-RQMT-1310	X				X		CMAS-TC-011
WEA-C-RQMT-1320	X				X		CMAS-TC-011

ATIS-0700037 Reference Point "C" Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-1400	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1410		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1500	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1510	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1520	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1600	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1610	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1620	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1630		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1700	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-1710	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1720	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1800	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1810	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-1820	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-1900	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-1910	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1920	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-1930	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1940	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-1950	X	X	X				Clause 4.4, *Pre-Test Requirements*

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-1960	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2000	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2010	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2100	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2110	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2120	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2200	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2210	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2220	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2300	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2310	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2320	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2330	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2340	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2400	X				X		CMAS-TC-002
WEA-C-RQMT-2410	X				X		CMAS-TC-002
WEA-C-RQMT-2420	X				X		CMAS-TC-002
WEA-C-RQMT-2430	X				X		CMAS-TC-002
WEA-C-RQMT-2440	X				X		CMAS-TC-002
WEA-C-RQMT-2450		X			X		CMAS-TC-002
WEA-C-RQMT-2500	X	X			X		CMAS-TC-001
WEA-C-RQMT-2510	X				X		CMAS-TC-001
WEA-C-RQMT-2520	X				X		CMAS-TC-003

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-2530	X				X		CMAS-TC-001 CMAS-TC-003
WEA-C-RQMT-2540	X				X		CMAS-TC-001
WEA-C-RQMT-2545$_{\text{R3A}}$	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2546$_{\text{R3A}}$	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2550$_{\text{R3M}}$		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2551$_{\text{R3A}}$		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2553	X				X		CMAS-TC-001
WEA-C-RQMT-2557	X				X		CMAS-TC-001
WEA-C-RQMT-2560	X				X		CMAS-TC-004
WEA-C-RQMT-2565							Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2570	X				X		CMAS-TC-005
WEA-C-RQMT-2580	X	X			X		CMAS-TC-006
WEA-C-RQMT-2590	X	X			X		CMAS-TC-001 CMAS-TC-006
WEA-C-RQMT-2600	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2610		X			X		CMAS-TC-007
WEA-C-RQMT-2620		X			X		CMAS-TC-007
WEA-C-RQMT-2630	X	X			X		CMAS-TC-001 CMAS-TC-002 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005 CMAS-TC-006 CMAS-TC-007
WEA-C-RQMT-2640	X	X			X		CMAS-TC-001
WEA-C-RQMT-2650	X	X			X		CMAS-TC-001
WEA-C-RQMT-2670	X	X			X		CMAS-TC-001
WEA-C-RQMT-2700	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-2710	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2720		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2730	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-2740		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2750	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2760		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2770	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2780	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2800	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2810		X			X		CMAS-TC-001 CMAS-TC-003 CMAS-TC-004 CMAS-TC-005 CMAS-TC-006
WEA-C-RQMT-2820		X			X		CMAS-TC-006
WEA-C-RQMT-2830	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2840	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2850	X				X		CMAS-TC-001
WEA-C-RQMT-2900		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2910	X				X		CMAS-TC-006 CMAS-TC-007
WEA-C-RQMT-2920	X				X		CMAS-TC-001
WEA-C-RQMT-2930		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2940$_{R3A}$	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2950$_{R3A}$		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2960$_{R3A}$		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2964$_{R3A}$	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)

ATIS-0700037 Reference Point “C” Requirement [Ref 1]	Applicability		Verification Method				Associated Test Cases
	F	C	I	A	D	T	
WEA-C-RQMT-2965$_{R3A}$	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-2970$_{R3A}$		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3000	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3100	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3110	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3200	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3210	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3220	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3300	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3310	X	X	X				Clause 4.4, *Pre-Test Requirements*
WEA-C-RQMT-3320	X	X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-3330	X	X			X		CMAS-TC-008 CMAS-TC-009
WEA-C-RQMT-3400	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3410		X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3420	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3430	X						Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3500	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3510	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3600	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)
WEA-C-RQMT-3610	X	X					Untested requirement (See Annex E, *Requirements Not Verified by Tests in This Specification*)

Annex A
(informative)

Annex A Summary of Reference Point "C" Interface Requirements

This annex contains a summary of the Reference Point "C" Interface Requirements that are documented and numbered in ATIS-0700037 [Ref 1].

Table A.1: Reference Point "C" Requirement Summary

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-0100	[WEA-C-RQMT-0100] The Federal Alert Gateway message exchange with the CMSP Gateway shall be per the CMSP profile.
WEA-C-RQMT-0110	[WEA-C-RQMT-0110] The Federal Alert Gateway shall maintain verifiable identities for approved CMSP Gateways.
WEA-C-RQMT-0120	[WEA-C-RQMT-0120] The Federal Alert Gateway shall maintain a CMSP profile that includes the parameters identified in Table 5.3 – *CMSP Profile Definition* in Clause 5.2.1.1, *Federal Alert Gateway Definition of CMSP Profile*.
WEA-C-RQMT-0130	[WEA-C-RQMT-0130] The Federal Alert Gateway shall send all Alert, Update, and Cancel CMAC messages to the CMSP Gateway, unless Geo-Location Filtering is selected in the CMSP profile.
WEA-C-RQMT-0140	[WEA-C-RQMT-0140] The Federal Alert Gateway shall send to the CMSP Gateway only Alert, Update, and Cancel CMAC messages having alert areas with some overlap with the listed states if Geo-Location Filtering is selected in the CMSP profile.
WEA-C-RQMT-0200	[WEA-C-RQMT-0200] The CMSP Profile in the Federal Alert Gateway shall contain the parameters defined in the following table: NOTE: The modification to requirement WEA-C-RQMT-0200 occurs in the C-Interface Message Version entry of Table 5.3 – CMSP Profile Definition.
WEA-C-RQMT-0300	[WEA-C-RQMT-0300] At startup, the Federal Alert Gateway shall attempt to establish an IPsec tunnel and a TCP connection with all CMSP Gateways in the CMSP Gateway Profile.
WEA-C-RQMT-0310	[WEA-C-RQMT-0310] The Federal Alert Gateway shall attempt to establish an IPsec tunnel and a TCP connection every time it has a new message to send to a CMSP Gateway with which no IPsec tunnel or TCP connection exists, unless the Federal Alert Gateway had received a Transmission Control – Cease from the CMSP Gateway.
WEA-C-RQMT-0320	[WEA-C-RQMT-0320] The Federal Alert Gateway shall try establishing an IPsec tunnel and a TCP connection at least per Reconnect Number times.
WEA-C-RQMT-0330	[WEA-C-RQMT-0330] The Federal Alert Gateway shall accept new IPsec tunnel and TCP connection requests from any CMSP Gateway in its CMSP Gateway Profile and establish an IPsec tunnel and a TCP connection with that CMSP Gateway, unless the connection would result in a CMSP Gateway Group being connected with more than two Federal Alert Gateways.
WEA-C-RQMT-0400	[WEA-C-RQMT-0400] The Federal Alert Gateway shall send the following message types to the CMSP Gateway per the CMAC protocol: • Alert (Clause 7.5.1, *Alert Message*) • Update (Clause 7.5.2, *Update Message*) • Cancel (Clause 7.5.3, *Cancel Message*) • RMT (Clause 7.5.7, *RMT Message*) • Link Test (Clause 7.5.6, *Link Test Message*) • Ack (Clause 7.5.4, *Ack Message*) • Error (Clause 7.5.5, *Error Message*).

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-0410	[WEA-C-RQMT-0410] The Federal Alert Gateway shall send an Alert message to the CMSP Gateway Group when triggered by the reception of a CAP Alert message that meets the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41].
WEA-C-RQMT-0414	[WEA-C-RQMT-0414] The Federal Alert Gateway shall send a single Alert message to the CMSP Gateway Group with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, based upon the received CAP Alert message.
WEA-C-RQMT-0416	[WEA-C-RQMT-0416] If Spanish alert text was provided by the alert originators in the received CAP Alert message, the Federal Alert Gateway shall send a single Alert message to the CMSP Gateway Group with Spanish alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, along with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element.
WEA-C-RQMT-0420	[WEA-C-RQMT-0420] The Federal Alert Gateway shall send an Update message to the CMSP Gateway Group when triggered by the reception of a CAP Update message that meets the criteria for a CMAS alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41].
WEA-C-RQMT-0425	[WEA-C-RQMT-0425] If the Federal Alert Gateway receives a single CAP Update message that does not meet the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9]] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41 and the Federal Alert Gateway cannot resolve the discrepancy with the alert originator, the Federal Alert Gateway shall send a Cancel message to the CMSP Gateway Group to cancel the original WEA alert which is referenced in the Update message.
WEA-C-RQMT-0427	[WEA-C-RQMT-0427] The Federal Alert Gateway shall send a single Update message to the CMSP Gateway Group with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, based upon the received CAP Update message.
WEA-C-RQMT-0428	[WEA-C-RQMT-0428] If Spanish alert text was provided by the alert originators in the received CAP Update message, the Federal Alert Gateway shall send a single Update message to the CMSP Gateway Group with Spanish alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, along with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element.
WEA-C-RQMT-0430	[WEA-C-RQMT-0430] The Federal Alert Gateway shall send a Cancel message to the CMSP Gateway Group when triggered by the reception of a CAP Cancel message that meets the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41].
WEA-C-RQMT-0440	[WEA-C-RQMT-0440] The Federal Alert Gateway shall send an RMT message to the CMSP Gateway Group once per month.
WEA-C-RQMT-0450	[WEA-C-RQMT-0450] The Federal Alert Gateway shall send a Link Test message every Link Test Period minute to each CMSP Gateway that did not send a Transmission Control – Cease message.
WEA-C-RQMT-0460	[WEA-C-RQMT-0460] The Federal Alert Gateway shall send an Ack message to the CMSP Gateway when a CMSP Gateway message has been received without error, except when the CMSP Gateway has sent an Ack or an Error message to the Federal Alert Gateway.
WEA-C-RQMT-0470	[WEA-C-RQMT-0470] The Federal Alert Gateway shall send an Error message to the CMSP Gateway when a CMSP Gateway message has been received with any error.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-0480	[WEA-C-RQMT-0480] The Federal Alert Gateway shall send all Alert, Update, Cancel, and RMT messages to CMSP Gateway A, unless it received a Transmission Control – Cease message from CMSP Gateway A to discontinue transmission.
WEA-C-RQMT-0490	[WEA-C-RQMT-0490] The Federal Alert Gateway shall send an Alert, Update, Cancel, or RMT message to CMSP Gateway B under any of the following conditions, unless it received a Transmission Control – Cease message from CMSP Gateway B to discontinue transmission: a. The Federal Alert Gateway received a Transmission Control – Cease message from CMSP Gateway A and discontinued transmission. b. The Federal Alert Gateway cannot establish a connection to CMSP Gateway A after trying Reconnect Number times. c. The Federal Alert Gateway does not receive an Ack/Error response from CMSP Gateway A after transmitting the message Retransmit Number times.
WEA-C-RQMT-0493	[WEA-C-RQMT-0493] The Federal Alert Gateway shall support versions 1.0 and 2.0 CMAC messages (defined in Clause 7.4).
WEA-C-RQMT-0496	[WEA-C-RQMT-0496] The Federal Alert Gateway shall use the version of CMAC messages provisioned in the CMSP's profile when transmitting messages to the associated CMSP. See WEA-C-RQMT-0200.
WEA-C-RQMT-0500	[WEA-C-RQMT-0500] The Federal Alert Gateway shall receive and process the following message types from the CMSP Gateway per the CMAC protocol: • Transmission Control – Cease (Clause 7.5.8, *Transmission Control – Cease Message*) • Transmission Control – Resume (Clause 7.5.9, *Transmission Control – Resume Message*) • Link Test (Clause 7.5.6, *Link Test Message*) • Ack (Clause 7.5.4, *Ack Message*) • Error (Clause 7.5.5, *Error Message*).
WEA-C-RQMT-0510	[WEA-C-RQMT-0510] The Federal Alert Gateway shall receive and log each Transmission Control – Cease message from the CMSP Gateway.
WEA-C-RQMT-0520	[WEA-C-RQMT-0520] The Federal Alert Gateway shall receive and log each Transmission Control – Resume message from the CMSP Gateway.
WEA-C-RQMT-0530	[WEA-C-RQMT-0530] The Federal Alert Gateway shall receive and log Link Test Messages from the CMSP Gateway.
WEA-C-RQMT-0540	[WEA-C-RQMT-0540] The Federal Alert Gateway shall receive and log Ack messages from the CMSP Gateway.
WEA-C-RQMT-0550	[WEA-C-RQMT-0550] The Federal Alert Gateway shall receive and log Error messages from the CMSP Gateway.
WEA-C-RQMT-0560	[WEA-C-RQMT-0560] The Federal Alert Gateway shall respond to all messages from a CMSP Gateway even if that CMSP Gateway has sent a Transmission Control – Cease message.
WEA-C-RQMT-0600	[WEA-C-RQMT-0600] The CMSP Gateway shall maintain a Federal Alert Gateway profile that includes the parameters identified in the following table: Table 4: *Federal Alert Gateway Profile Definition*.
WEA-C-RQMT-0700	[WEA-C-RQMT-0700] CMSP Gateway message exchange with the Federal Alert Gateway shall be per the Federal Alert Gateway profile.
WEA-C-RQMT-0710	[WEA-C-RQMT-0710] The CMSP Gateway shall accept and process messages received from any of the Federal Alert Gateways identified in the Federal Alert Gateway profile.
WEA-C-RQMT-0720	[WEA-C-RQMT-0720] The CMSP Gateway shall maintain verifiable identities for approved Federal Alert Gateways.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-0800	[WEA-C-RQMT-0800] At startup, the CMSP Gateway shall attempt to establish an IPsec tunnel and a TCP connection with the first two Federal Alert Gateways in the Federal Alert Gateway Profile, if an IPsec tunnel and a TCP connection does not already exist with two Federal Alert Gateways.
WEA-C-RQMT-0820	[WEA-C-RQMT-0820] If the CMSP Gateway is unable to establish an IPsec tunnel and a TCP connection with the Federal Alert Gateways, the CMSP Gateway shall go down the list of Federal Alert Gateways in the Federal Alert Gateway Profile until it establishes an IPsec tunnel and a TCP connection or completes the list without establishing the connections.
WEA-C-RQMT-0830	[WEA-C-RQMT-0830] The CMSP Gateway shall try establishing an IPsec tunnel and a TCP connection with each Federal Alert Gateway at least per Reconnect Number times before moving to the next Gateway in the list.
WEA-C-RQMT-0840	[WEA-C-RQMT-0840] When the CMSP Gateway has a new message (i.e., Link Test, Transmission Control – Cease, Transmission Control – Resume, and CAP Retrieval) to send to a particular Federal Alert Gateway and the CMSP Gateway does not have an IPsec tunnel and TCP connections to that particular Federal Alert Gateway, the CMSP Gateway shall attempt to establish an IPsec tunnel and a TCP connection with that particular Federal Alert Gateway.
WEA-C-RQMT-0850	[WEA-C-RQMT-0850] The CMSP Gateway shall accept new IPsec tunnel and TCP connection requests from any Federal Alert Gateway in its Federal Alert Gateway Profile if the CMSP Gateway has an IPsec tunnel and a TCP connection with less than two Federal Alert Gateways.
WEA-C-RQMT-0900	[WEA-C-RQMT-0900] The CMSP Gateway shall send the following message types to the Federal Alert Gateway per the CMAC protocol: • Transmission Control – Cease (Clause 7.5.8, *Transmission Control – Cease Message*) • Transmission Control – Resume (Clause 7.5.9, *Transmission Control – Resume Message*) • Link Test (Clause 7.5.6, *Link Test Message*) • Ack (Clause 7.5.4, *Ack Message*) • Error (Clause 7.5.5, *Error Message*).
WEA-C-RQMT-0910	[WEA-C-RQMT-0910] The CMSP Gateway shall send an Error message to a Federal Alert Gateway when a message has been received from that Federal Alert Gateway with an error.
WEA-C-RQMT-0920	[WEA-C-RQMT-0920] The CMSP Gateway shall send a Transmission Control – Cease message to a Federal Alert Gateway to discontinue the transmission of messages from that Federal Alert Gateway.
WEA-C-RQMT-0930	[WEA-C-RQMT-0930] The CMSP Gateway shall send a Transmission Control – Resume message to a Federal Alert Gateway to resume the transmission of messages from that Federal Alert Gateway.
WEA-C-RQMT-0940	[WEA-C-RQMT-0940] The CMSP Gateway shall send a Link Test message to the Federal Alert Gateway to determine the status of communication with the Federal Alert Gateway.
WEA-C-RQMT-0950	[WEA-C-RQMT-0950] The CMSP Gateway shall send an Ack message to a Federal Alert Gateway when a message has been received from that Federal Alert Gateway without error.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-1000	[WEA-C-RQMT-1000] The CMSP Gateway shall receive and process the following message types from the Federal Alert Gateway in the CMAC protocol: • Alert (Clause 7.5.1, *Alert Message*) • Update (Clause 7.5.2, *Update Message*) • Cancel (Clause 7.5.3, *Cancel Message*) • RMT (Clause 7.5.7, *RMT Message*) • Link Test (Clause 7.5.6, *Link Test Message*) • Ack (Clause 7.5.4, *Ack Message*) • Error (Clause 7.5.5, *Error Message*).
WEA-C-RQMT-1010	[WEA-C-RQMT-1010] The CMSP Gateway shall receive and log Alert messages from the Federal Alert Gateway.
WEA-C-RQMT-1020	[WEA-C-RQMT-1020] The CMSP Gateway shall receive and log Update messages from the Federal Alert Gateway.
WEA-C-RQMT-1030	[WEA-C-RQMT-1030] The CMSP Gateway shall receive and log Cancel messages from the Federal Alert Gateway.
WEA-C-RQMT-1040	[WEA-C-RQMT-1040] If the CMSP Gateway receives an “Update” message and cannot make an association with the “referenced message”, the CMSP Gateway shall process the “Update” as a new “Alert” message.
WEA-C-RQMT-1050	[WEA-C-RQMT-1050] The CMSP Gateway shall receive and log RMT messages from the Federal Alert Gateway.
WEA-C-RQMT-1060	[WEA-C-RQMT-1060] The CMSP Gateway shall receive and log Link Test Messages from the Federal Alert Gateway.
WEA-C-RQMT-1070	[WEA-C-RQMT-1070] The CMSP Gateway shall receive and log Ack messages from the Federal Alert Gateway.
WEA-C-RQMT-1080	[WEA-C-RQMT-1080] The CMSP Gateway shall receive and log Error messages from the Federal Alert Gateway.
WEA-C-RQMT-1090	[WEA-C-RQMT-1090] If in any given monthly RMT cycle more than one RMT message is received by the CMSP, the CMSP Gateway shall accept only the first RMT message and shall reject all subsequent RMT messages within that calendar month.
WEA-C-RQMT-1100	[WEA-C-RQMT-1100] If the CMSP Gateway determines that an RMT message is invalid (e.g., not originated by the Federal Alert Gateway Administrator), the CMSP Gateway shall reject the RMT message.
WEA-C-RQMT-1110	[WEA-C-RQMT-1110] If conditions at the CMSP Gateway preclude distribution of the RMT, the CMSP Gateway shall respond to the RMT message with an Error message (see Table 7.26 – *Definition of CMAC Response Codes*).
WEA-C-RQMT-1120	[WEA-C-RQMT-1120] If conditions at the CMSP Gateway preclude distribution of the State/Local WEA Test message, the CMSP Gateway shall respond to the State/Local WEA Test message with an Error message (see Table 7.26 – Definition of CMAC Response Codes).
WEA-C-RQMT-1150	[WEA-C-RQMT-1150] The CMSP Gateway shall log reception of Alert, Update, and Cancel messages, along with a timestamp when the message is received, and shall log Ack and Error responses sent from the CMSP Gateway along with a timestamp.
WEA-C-RQMT-1200	[WEA-C-RQMT-1200] A National alert received by the Federal Alert Gateway shall be sent to the CMSP Gateway before any other alerts that may be waiting in a message queue for processing.
WEA-C-RQMT-1210	[WEA-C-RQMT-1210] The Federal Alert Gateway shall send all alerts other than National alerts to the CMSP Gateway on a FIFO basis.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-1300	[WEA-C-RQMT-1300] The Federal Alert Gateway shall queue outgoing CMAC messages to a CMSP Gateway Group as long as the message is still valid for broadcast (up to 24 hours maximum) if it cannot send the message to any CMSP Gateway in the CMSP Gateway Group and receive an Ack/Error response.
WEA-C-RQMT-1310	[WEA-C-RQMT-1310] The Federal Alert Gateway shall remove messages from the queue that are no longer valid for broadcast (i.e., cancelled, updated, and expired).
WEA-C-RQMT-1320	[WEA-C-RQMT-1320] The Federal Alert Gateway shall send all queued messages in FIFO order, except National Alerts, to a CMSP Gateway when an IPsec tunnel and a TCP connection are established with that CMSP Gateway.
WEA-C-RQMT-1400	[WEA-C-RQMT-1400] Federal Alert Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.
WEA-C-RQMT-1410	[WEA-C-RQMT-1410] CMSP Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.
WEA-C-RQMT-1500	[WEA-C-RQMT-1500] The format for certificates between the CMSP Gateway and the Federal Alert Gateway shall be X.509 version 3 (X.509v3) certificate [Ref 19].
WEA-C-RQMT-1510	[WEA-C-RQMT-1510] The Federal Alert Gateway and the CMSP Gateway shall check the revocation status of the peer's X.509 certificate using the Online Certificate Status Protocol (OCSP), specified in RFC 6960 [Ref 34].
WEA-C-RQMT-1520	[WEA-C-RQMT-1520] Federal Alert Gateway and CMSP Gateways establishing security associations shall use OCSP over HTTP using the Nonce and Archive Cutoff options only.
WEA-C-RQMT-1600	[WEA-C-RQMT-1600] The identifiers for establishing an IPsec tunnel shall be the CMSP Gateway and Federal Alert Gateway Fully Qualified Domain Names or IP addresses.
WEA-C-RQMT-1610	[WEA-C-RQMT-1610] The Fully Qualified Domain Names and IP addresses shall be unique identifiers.
WEA-C-RQMT-1620	[WEA-C-RQMT-1620] The Federal Alert Gateway shall close the associated communication sockets, if the intended communication is with a CMSP Gateway and none of the distinguished names on the received certificate appear on the CMSP Gateway profile.
WEA-C-RQMT-1630	[WEA-C-RQMT-1630] The CMSP Gateway shall close the associated communication sockets, if the intended communication is with a Federal Alert Gateway and none of the distinguished names on the received certificate appear in the Federal Alert Gateway profile.
WEA-C-RQMT-1700	[WEA-C-RQMT-1700] IPsec version 3 (IPsec v3) [Refs 3, 10, 11, & 12] shall be used on the Federal Alert Gateway to CMSP Gateway Interface.
WEA-C-RQMT-1710	[WEA-C-RQMT-1710] An IPsec v3 tunnel shall be established to protect all messages when transmitted between the Federal Alert Gateway and the CMSP Gateway.
WEA-C-RQMT-1720	[WEA-C-RQMT-1720] The encrypted information shall include all CMAC messages as well as the associated keys.
WEA-C-RQMT-1800	[WEA-C-RQMT-1800] The Authentication Header (AH) option shall not be used.
WEA-C-RQMT-1810	[WEA-C-RQMT-1810] The IPsec protocol shall utilize ESP [Ref 13].
WEA-C-RQMT-1820	[WEA-C-RQMT-1820] The algorithms in Table 5.5 – *Required Algorithms for Implementation of ESP Encryption* shall be used to implement the ESP.
WEA-C-RQMT-1900	[WEA-C-RQMT-1900] The Federal Alert Gateway to CMSP Gateway Interface shall use key exchange per IKE v2 [Ref 12].

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-1910	[WEA-C-RQMT-1910] Manual keying shall not be used.
WEA-C-RQMT-1920	[WEA-C-RQMT-1920] The algorithms in Table 5.6 – *Required Algorithms for Implementation of IKE v2* shall be used to implement the IKE v2.
WEA-C-RQMT-1930	[WEA-C-RQMT-1930] All algorithms shall be upgradable with a new library and configuration change.
WEA-C-RQMT-1940	[WEA-C-RQMT-1940] Algorithm upgrades shall not require a full system hardware upgrade.
WEA-C-RQMT-1950	[WEA-C-RQMT-1950] All algorithm functions shall be implemented in according with the RFCs in Table 5.7 – *Summary of References for IPsec*.
WEA-C-RQMT-1960	[WEA-C-RQMT-1960] <Void>.
WEA-C-RQMT-2000	[WEA-C-RQMT-2000] The only valid IPsec SAs shall be between a CMSP Gateway and a Federal Alert Gateway.
WEA-C-RQMT-2010	[WEA-C-RQMT-2010] The Federal Alert Gateway and CMSP Gateway IPsec implementation shall be capable of supporting port-based traffic filtering policies.
WEA-C-RQMT-2100	[WEA-C-RQMT-2100] Outbound packets to destinations for which SAs are not allowed shall be discarded.
WEA-C-RQMT-2110	[WEA-C-RQMT-2110] Outbound IKEv2 message packets destined for port 500 shall not be IPsec encrypted.
WEA-C-RQMT-2120	[WEA-C-RQMT-2120] All outbound packets not destined for port 500 shall be IPsec encrypted using the cryptographic material for the SA with the destination address.
WEA-C-RQMT-2200	[WEA-C-RQMT-2200] Inbound IKEv2 message packets destined for port 500 shall not be IPsec decrypted.
WEA-C-RQMT-2210	[WEA-C-RQMT-2210] Inbound packets that are not destined for Port 500 shall be IPsec decrypted using the cryptographic material for the SA with the source address.
WEA-C-RQMT-2220	[WEA-C-RQMT-2220] Inbound packets not destined for Port 500 and for which there is no SA for the source shall be discarded.
WEA-C-RQMT-2300	[WEA-C-RQMT-2300] SA Renewal and Rekey shall be configurable by Federal Alert Gateway and CMSP Gateway system administrators.
WEA-C-RQMT-2310	[WEA-C-RQMT-2310] IPsec SA shall have a maximum lifetime of IPSec SA Maximum Lifetime.
WEA-C-RQMT-2320	[WEA-C-RQMT-2320] IKE SA shall have a maximum lifetime of IKE SA Maximum Lifetime.
WEA-C-RQMT-2330	[WEA-C-RQMT-2330] Federal Alert Gateway and CMSP Gateway shall support SA renewal after expiration.
WEA-C-RQMT-2340	[WEA-C-RQMT-2340] Federal Alert Gateway and CMSP Gateway shall support SA rekey before expiration.
WEA-C-RQMT-2400	[WEA-C-RQMT-2400] The XML Signature Method shall be RSA-SHA256 [Ref 7] for XML Signatures applied to CMAC messages.
WEA-C-RQMT-2410	[WEA-C-RQMT-2410] The Digest Method [Ref 45] shall be SHA-256 [Ref 7] for XML Signatures applied to CMAC messages.
WEA-C-RQMT-2420	[WEA-C-RQMT-2420] The Canonicalization Method [Ref 35] shall be Exclusive Canonicalization for XML Signatures applied to CMAC messages.
WEA-C-RQMT-2430	[WEA-C-RQMT-2430] The Enveloped Signature method [Ref 38] shall be used for XML Signatures applied to CMAC messages.
WEA-C-RQMT-2440	[WEA-C-RQMT-2440] The Federal Alert gateway shall implement non-repudiation as described in [Ref 45] for CMAC Alert, Update, Cancel, and RMT messages.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-2450	[WEA-C-RQMT-2450] The presence of an XML Signature [Ref 38] shall not cause the CMSP Gateway to fail to receive and process the message.
WEA-C-RQMT-2500	[WEA-C-RQMT-2500] The CMAC_protocol_version element shall be set to "2.0" for this version of the Standard.
WEA-C-RQMT-2510	[WEA-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables: • Table 7.8 – *CMAC_Digital_Signature Segment Element Definition* • Table 7.9 – *Elements of Alert Attributes Segment for Alert Message* • Table 7.10 – *Elements of Alert Info Segment for Alert Message* • Table 7.11 – *Elements of Alert Area Segment for Alert Message* • Table 7.12 – *Elements of Alert Text Segment for Alert Message.*
WEA-C-RQMT-2520	[WEA-C-RQMT-2520] Each Update message shall contain the mandatory message elements and associated values provided in the following tables: • Table 7.8 – *CMAC_Digital_Signature Segment Element Definition* • Table 7.9 – *Elements of Alert Attributes Segment for Update Message* • Table 7.10 – *Elements of Alert Info Segment for Update Message* • Table 7.11 – *Elements of Alert Area Segment for Update Message* • Table 7.12 – *Elements of Alert Text Segment for Alert Message.*
WEA-C-RQMT-2530	[WEA-C-RQMT-2530] The conditional CMAC_special_handling element shall be included in Alert, Update, and Cancel messages if the Federal Alert Gateway determines that the message is a National Alert, a Child Abduction/AMBER Alert, a Required Monthly Test, a Public Safety message, or a State/Local WEA Test message.
WEA-C-RQMT-2540	[WEA-C-RQMT-2540] The CMAC_Alert_Area shall contain at least one instance of <CMAC_cmas_geocode> element.
WEA-C-RQMT-2545$_{R3A}$	[WEA-C-RQMT-2545$_{R3A}$] The sum of the number of paired values of points (i.e., latitude/longitude pairs) used to define all the polygon(s) plus the number of circles is greater than the allowed maximum of 100 (see WEA-C-RQMT-2550), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2546$_{R3A}$	[WEA-C-RQMT-2546$_{R3A}$] If the total number of shapes is greater than the 10 shapes (e.g., polygons and circles) allowed (see WEA-C-RQMT-2551), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2550$_{R3M}$	[WEA-C-RQMT-2550$_{R3M}$] The sum of the number of paired values of points (i.e., latitude/longitude pairs) used to define the polygon in the CMAC_polygon elements plus the number of circles in the CMAC_circle elements shall be limited to a maximum of 100.
WEA-C-RQMT-2551$_{R3A}$	[WEA-C-RQMT-2551$_{R3A}$] The sum of CMAC_Alert_Areas shall contain a combined maximum of 10 polygons and circles.
WEA-C-RQMT-2553	[WEA-C-RQMT-2553] When one or more occurrences of the CMAC_Alert_Text segment is included, one occurrence shall be for English.
WEA-C-RQMT-2557	[WEA-C-RQMT-2557] When multiple occurrences of the CMAC_Alert_Text segment are included, each occurrence of the CMAC_Alert_Text segment shall have a different language.
WEA-C-RQMT-2560	[WEA-C-RQMT-2560] Each Cancel message shall contain the mandatory message elements and associated values provided in the following tables: • Table 7.8 – *CMAC_Digital_Signature Segment Element Definition* • Table 7.17 – *Elements of Alert Attributes Segment for Cancel Message.*
WEA-C-RQMT-2565	[WEA-C-RQMT-2565] The Cancel message shall discontinue the broadcast of all languages of the referenced Alert or Update message.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-2570	[WEA-C-RQMT-2570] Each RMT message shall contain the mandatory message elements and associated values provided in the following tables: • *Table 7.8 – CMAC_Digital_Signature Segment Element Definition* • Table 7.21 – *Elements of Alert Attributes Segment for RMT Message* • Table 7.22 – *Elements of Alert Info Segment for RMT Message.*
WEA-C-RQMT-2580	[WEA-C-RQMT-2580] Each Link Test Message shall contain the mandatory message elements and associated values provided in the following table: • Table 7.20 – *Elements of Alert Attributes Segment for Link Test Message.*
WEA-C-RQMT-2590	[WEA-C-RQMT-2590] Each Ack message shall contain the mandatory message elements and associated values provided in the following table: • Table 7.18 – *Elements of Alert Attributes Segment for Ack Message.*
WEA-C-RQMT-2600	[WEA-C-RQMT-2600] Each Error message shall contain the mandatory message elements and associated values provided in the following table: • Table 7.19– *Elements of Alert Attributes Segment for Error Message.*
WEA-C-RQMT-2610	[WEA-C-RQMT-2610] Each Transmission Control – Cease message shall contain the mandatory message elements and associated values provided in Table 7.24 – *Elements of Alert Attributes Segment for Transmission Control – Cease Message*.
WEA-C-RQMT-2620	[WEA-C-RQMT-2620] Each Transmission Control – Resume message shall contain the mandatory message elements and associated values provided in Table 7.25 – *Elements of Alert Attributes Segment for Transmission Control – Resume Message*.
WEA-C-RQMT-2630	[WEA-C-RQMT-2630] All CMAC messages shall adhere to the XML Schema [Refs 33, 43, & 44] in Clause 7.4, *CMAC Message XML Definition*.
WEA-C-RQMT-2640	[WEA-C-RQMT-2640] The value of the CMAC_message_number shall be increased monotonically for each and every message issued by the sending gateway.
WEA-C-RQMT-2650	[WEA-C-RQMT-2650] Each State/Local WEA Test message shall contain the mandatory message elements and associated values equivalent to those of an Imminent Threat message (Alert, Update, or Cancel) with the exception that the CMAC_special_handling element shall be set to "State Local WEA Test".
WEA-C-RQMT-2670	[WEA-C-RQMT-2670] Each Public Safety message shall contain the mandatory message elements and associated values equivalent to those of an Imminent Threat message (Alert, Update, or Cancel) with the exception that the CMAC_special_handling element shall be set to "Public Safety".
WEA-C-RQMT-2700	[WEA-C-RQMT-2700] HTTP communications shall be per RFC 7230 [Ref 15] and RFC 7231 [Ref 37].
WEA-C-RQMT-2710	[WEA-C-RQMT-2710] HTTP communications carrying CMAC messages shall be to port TCP 8080.
WEA-C-RQMT-2720	[WEA-C-RQMT-2720] HTTP communications for CAP message retrieval shall be to port TCP 80.
WEA-C-RQMT-2730	[WEA-C-RQMT-2730] HTTP methods shall be limited to POST when CMAC Alert, Update, Cancel, RMT, and Link Test messages are sent over HTTP.
WEA-C-RQMT-2740	[WEA-C-RQMT-2740] HTTP methods shall be limited to GET when HTTP is used without the CMAC protocol.
WEA-C-RQMT-2750	[WEA-C-RQMT-2750] The HTTP POST method shall use “*” as the Request_URI.
WEA-C-RQMT-2760	[WEA-C-RQMT-2760] The HTTP GET method shall contain a Host request_header, whose value shall be the host part of the CMAC_cap_alert_uri.
WEA-C-RQMT-2770	[WEA-C-RQMT-2770] All CMAC Ack and Error messages shall be sent in HTTP 200 OK response messages.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-2780	[WEA-C-RQMT-2780] An HTTP 4xx Client Error or 5xx Server Error response message shall be sent to indicate a failure of the Federal Alert Gateway to retrieve the requested CAP message.
WEA-C-RQMT-2800	[WEA-C-RQMT-2800] If the Federal Alert Gateway receives an invalid or malformed acknowledgement or error response message from the CMSP Gateway, the Federal Alert Gateway should log this condition and shall not reply to the CMSP Gateway with an error response.
WEA-C-RQMT-2810	[WEA-C-RQMT-2810] The CMSP Gateway shall respond to each message from the Federal Alert Gateway with one of the potential CMSP Gateway responses valid for that particular message type per Table 7.2 – *Federal Alert Gateway Initiated Messages*.
WEA-C-RQMT-2820	[WEA-C-RQMT-2820] The CMSP Gateway shall not send a message in response to an Ack or Error message from the Federal Alert Gateway.
WEA-C-RQMT-2830	[WEA-C-RQMT-2830] If the Federal Alert Gateway does not receive an expected response message (Ack or Error) from the CMSP Gateway within the Message Response Time, the Federal Alert Gateway shall retransmit the message additional times, per the Retransmit Number.
WEA-C-RQMT-2840	[WEA-C-RQMT-2840] The Federal Alert Gateway shall declare a CMSP Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.
WEA-C-RQMT-2850	[WEA-C-RQMT-2850] The Federal Alert Gateway shall send WEA Alert, Update, and RMT messages to the CMSP Gateway with both the 90-character maximum alert message text and the 360-character maximum alert message text for each language.
WEA-C-RQMT-2900	[WEA-C-RQMT-2900] If the CMSP Gateway receives an invalid or malformed acknowledgement or error response message from the Federal Alert Gateway, the CMSP Gateway should log this condition and shall not reply to the Federal Alert Gateway with an error response.
WEA-C-RQMT-2910	[WEA-C-RQMT-2910] The Federal Alert Gateway shall respond to each message from the CMSP Gateway with one of the potential Federal Alert Gateway responses valid for that particular message type per Table 7.3 – *CMSP Gateway Initiated Messages*.
WEA-C-RQMT-2920	[WEA-C-RQMT-2920] The Federal Alert Gateway shall not send a message in response to an Ack or Error message from the CMSP Gateway.
WEA-C-RQMT-2930	[WEA-C-RQMT-2930] The CMSP Gateway shall declare a Federal Alert Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.
WEA-C-RQMT-2940$_{R3A}$	[WEA-C-RQMT-2940$_{R3A}$] The Federal Alert Gateway shall be able to indicate that bypassing DBGF is requested in the CMAC alert or update.
WEA-C-RQMT-2950$_{R3A}$	[WEA-C-RQMT-2950$_{R3A}$] If DBGF bypass is requested in the CMAC alert or update and bypassing DBGF is allowed by regulatory policy, then the CMSP shall bypass DBGF procedures for the WEA.
WEA-C-RQMT-2960$_{R3A}$	[WEA-C-RQMT-2960$_{R3A}$] DBGF bypass requests shall be ignored for CMAC messages without polygon or circle elements.
WEA-C-RQMT-2964$_{R3A}$	[WEA-C-RQMT-2964$_{R3A}$] If the DBGF bypass is requested by an Alert Originator not authorized to make this request, the receiving Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2965$_{R3A}$	[WEA-C-RQMT-2965$_{R3A}$] If the DBGF is requested by an Alert Originator authorized to make this request, the receiving Federal Alert Gateway shall populate the CMAC_note field accordingly.
WEA-C-RQMT-2970$_{R3A}$	[WEA-C-RQMT-2970$_{R3A}$] If DBGF bypass is requested in the CMAC alert or update and DBGF bypass is not allowed by regulatory policy, the CMSP Gateway shall ignore the DBGF bypass request.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-3000	[WEA-C-RQMT-3000] The Federal Alert Gateway to CMSP Gateway interface shall be in accordance with RFC 1122 [Ref 27].
WEA-C-RQMT-3100	[WEA-C-RQMT-3100] Transmission Control Protocol (TCP) shall be implemented for the transport layer in accordance with RFC 793 [Ref 17].
WEA-C-RQMT-3110	[WEA-C-RQMT-3110] TCP connections shall be persistent.
WEA-C-RQMT-3200	[WEA-C-RQMT-3200] The interface shall support IP Version 4 for the network layer in accordance with IETF STD 5 (RFC 791) [Ref 28].
WEA-C-RQMT-3210	[WEA-C-RQMT-3210] The network layer shall support Internet Control Message Protocol (ICMP) in accordance with IETF STD 5 (RFC 792) for IP Version 4 [Ref 29].
WEA-C-RQMT-3220	[WEA-C-RQMT-3220] The interface shall support IP Version 6 for the network layer in accordance with RFC 8200 [Ref 30] and RFC 4291 [Ref 32].
WEA-C-RQMT-3300	[WEA-C-RQMT-3300] Any packets received in error shall be discarded at TCP level by the receiving gateway.
WEA-C-RQMT-3310	[WEA-C-RQMT-3310] When a packet is received in error, a correct packet shall be retransmitted by the sending gateway per TCP protocol.
WEA-C-RQMT-3320	[WEA-C-RQMT-3320] Both the CMSP Gateway and the Federal Alert Gateway shall log failures to establish a TCP session.
WEA-C-RQMT-3330	[WEA-C-RQMT-3330] Both the CMSP Gateway and the Federal Alert Gateway shall log failures to establish a secure IP tunnel.
WEA-C-RQMT-3400	[WEA-C-RQMT-3400] The Federal Alert Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response when the CMSP Gateway sends a CMAC message.
WEA-C-RQMT-3410	[WEA-C-RQMT-3410] The CMSP Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response.
WEA-C-RQMT-3420	[WEA-C-RQMT-3420] The Federal Alert Gateway shall reject HTTP methods other than GET with a 4xx Client Error response when the CMSP Gateway requests to retrieve a CAP message.
WEA-C-RQMT-3430	[WEA-C-RQMT-3430] The Federal Alert Gateway shall send a 4xx Client Error or 5xx Server Error response message when it is unable to retrieve the CAP message requested by a CMSP Gateway.
WEA-C-RQMT-3500	[WEA-C-RQMT-3500] Messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44] shall be logged and discarded.
WEA-C-RQMT-3510	[WEA-C-RQMT-3510] An Error message shall be sent in response to messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44].
WEA-C-RQMT-3600	[WEA-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.
WEA-C-RQMT-3610	[WEA-C-RQMT-3610] An Error message shall be sent in response to messages containing information that conflicts with the CMAC protocol.

Annex B
(normative)

Annex B Input CAP Messages

The following CAP messages are 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.

B.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>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <info>
   <language>en-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <responseType>Shelter</responseType>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 1]</expires>
   <senderName>NWS</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
   </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 1]</value>
   </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 1]</value>
     </parameter>
   <area>
     <areaDesc>FAIRFAX COUNTY IN VIRGINIA</areaDesc>
     <polygon>38.918361,-77.341233 38.903401,-77.289734 38.869194,-77.354279 38.918361,-
77.341233</polygon>
     <geocode>
      <valueName>SAME</valueName>
      <value>051059</value>
     </geocode>
   </area>
  </info>
  <info>
     <language>es-US</language>
     <category>Met</category>
     <event>SEVERE THUNDERSTORM WARNING</event>
     <responseType>Shelter</responseType>
     <urgency>Immediate</urgency>
     <severity>Severe</severity>
     <certainty>Observed</certainty>
     <eventCode>
           <valueName>SAME</valueName>
       <value>SVR</value>
     </eventCode>
    <expires>[Expires Date-Time 1]</expires>>
  <senderName>NWS</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
   <parameter>
       <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
     </parameter>
    <parameter>
           <valueName>CMAMtext</valueName>
           <value>[Short Spanish Test Message 1]</value>
     </parameter>
     <parameter>
           <valueName>CMAMlongtext</valueName>
           <value>[Long Spanish Test Message 1]</value>
     </parameter>
     <area>
           <areaDesc>FAIRFAX COUNTY IN VIRGINIA</areaDesc>
           <polygon>38.918361,-77.341233 38.903401,-77.289734 38.869194,-77.354279
38.918361,-77.341233</polygon>
           <geocode>
         <valueName>SAME</valueName>
            <value>051059</value>
           </geocode>
    </area>
   </info>
</alert>
```

B.2 CAP Message #2 – National Alert[9]

```
<?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 2]</identifier>
  <sender>[Message Sender 2]</sender>
  <sent>[CAP Sent Date-Time 2]</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <info>
```

[9] Presidential Alert has been renamed to National Alert. However, protocol encoding on the C-interface still uses the term "Presidential".

```
   <language>en-US</language>
   <category>Security</category>
   <event>Presidential Security Update</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>EAN</value>
   </eventCode>
   <expires>[Expires Date-Time 2]</expires>
   <senderName>U.S. Government, President</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Presidential</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 2]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 2]</value>
     </parameter>   <area>
     <areaDesc>U.S. Nationwide</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>000000</value>
     </geocode>
   </area>
  </info>
  <info>
   <language>es-US</language>
   <category>Security</category>
   <event>Presidential Security Update</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>EAN</value>
   </eventCode>
   <senderName>U.S. Government, President</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Presidential</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 2]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 2]</value>
     </parameter>
   <area>
```

```
     <areaDesc>U.S. Nationwide</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>000000</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.3 CAP Message #3 – AMBER 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 3]</identifier>
  <sender>[Message Sender 3]</sender>
  <sent>[CAP Sent Date-Time 3]</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <info>
   <language>en-US</language>
   <category>Rescue</category>
   <event>Child Abduction</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>CAE</value>
   </eventCode>
   <expires>[Expires Date-Time 3]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>Child Abduction</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 3]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 3]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>006037</value>
     </geocode>
   </area>
  </info>
<info>
   <language>es-US</language>
   <category>Rescue</category>
   <event>Child Abduction</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>CAE</value>
   </eventCode>

   <expires>[Expires Date-Time 3]</expires>
  <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
   <parameter>
      <valueName>WEAHandling</valueName>
      <value>Child Abduction</value>
    </parameter>
    <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 3]</value>
    </parameter>
    <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 3</value>
          </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>006037</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.4 CAP Message #4 – Imminent Threat Update

```
<?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 4]</identifier>
  <sender>[Message Sender 4]</sender>
  <sent>[CAP Sent Date-Time 4]</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 1],[CAP Message ID 1],[CAP Sent Date-Time 1]
   </references>
  <info>
     <language>en-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 4]</expires>
   <senderName>NWS</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
      <valueName>WEAHandling</valueName>
      <value>Imminent Threat</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 4]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 4]</value>
     </parameter>
   <area>
     <areaDesc>FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>051059</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>051013</value>
     </geocode>
   </area>
  </info>
  <info>
     <language>es-US</language>
     <category>Met</category>
     <event>SEVERE THUNDERSTORM WARNING</event>
     <responseType>Shelter</responseType>
     <urgency>Immediate</urgency>
     <severity>Severe</severity>
     <certainty>Observed</certainty>
     <eventCode>
          <valueName>SAME</valueName>
       <value>SVR</value>
     </eventCode>
   <expires>[Expires Date-Time 4]</expires>
   <senderName>NWS</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
       <value>Imminent Threat</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 4]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 4]</value>
     </parameter>
     <area>
     <areaDesc>FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>051059</value>
     </geocode>
     <geocode>
```

```
      <valueName>SAME</valueName>
      <value>051013</value>
     </geocode>
   </area>
   </info>
</alert>
```

B.5 CAP Message #5 – National Update

```
<?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 5]</identifier>
  <sender>[Message Sender 5]</sender>
  <sent>[CAP Sent Date-Time 5]</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 2],[CAP Message ID 2],[CAP Sent Date-Time 2]
   </references>
  <info>
   <language>en-US</language>
   <category>Security</category>
   <event>Presidential Security Update</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>EAN</value>
   </eventCode>
   <expires>[Expires Date-Time 5]</expires>
   <senderName>U.S. Government, President</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Presidential</value>
          </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
       <value>[Short English Test Message 5]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 5]</value>
     </parameter>
   <area>
     <areaDesc>U.S. Nationwide</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>000000</value>
     </geocode>
   </area>
  </info>
  <info>
   <language>es-US</language>
   <category>Security</category>
   <event>Presidential Security Update</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>EAN</value>
   </eventCode>
   <expires>[Expires Date-Time 5]</expires>
   <senderName>U.S. Government, President</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>Presidential</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
       <value>[Short Spanish Test Message 5]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 5]</value>
     </parameter>
   <area>
     <areaDesc>U.S. Nationwide</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>000000</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.6 CAP Message #6 – AMBER Update

```
<?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 6]</identifier>
  <sender>[Message Sender 6]</sender>
  <sent>[CAP Sent Date-Time 6]</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 3],[CAP Message ID 3],[CAP Sent Date-Time 3]
   </references>
  <info>
   <language>en-US</language>
   <category>Rescue</category>
   <event>Child Abduction</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>CAE</value>
   </eventCode>
   <expires>[Expires Date-Time 6]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
```

```
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>Child Abduction</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
       <value>[Short English Test Message 6]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 6]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County and San Bernardino County</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>006037</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>006071</value>
     </geocode>
   </area>
  </info>
  <info>
   <language>es-US</language>
   <category>Rescue</category>
   <event>Child Abduction</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>CAE</value>
   </eventCode>
   <expires>[Expires Date-Time 6]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Child Abduction</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
       <value>[Short Spanish Test Message 6]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 6]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>006037</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.7 CAP Message #7 – Invalid CMAS Criteria Update

```
<?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 7]</identifier>
  <sender>[Message Sender 7]</sender>
  <sent>[CAP Sent Date-Time 7]</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 4],[CAP Message ID 4],[CAP Sent Date-Time 4]
   </references>
  <info>
   <language>en-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Past</urgency>
   <severity>Moderate</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 7]</expires>
     <senderName>NWS</senderName>
     <headline> Test Update Message only Disregard please.</headline>
   <description> THIS is NOT an Actual Message. It is only a test Update. This is
Descriptive text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a test update. This is where
the call to action for those receiving the message should be provided.</instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 7]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 7]</value>
     </parameter>
   <area>
     <areaDesc>FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>051059</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>051013</value>
     </geocode>
   </area>
  </info>
  <info>
     <language>es-US</language>
   <category>Met</category>
     <event>SEVERE THUNDERSTORM WARNING</event>
   <responseType>Shelter</responseType>
     <urgency>Past</urgency>
   <severity>Moderate</severity>
     <certainty>Observed</certainty>
```

```
           <eventCode>
           <valueName>SAME</valueName>
           <value>SVR</value>
      </eventCode>
   <expires>[Expires Date-Time 7]</expires>
      <senderName>NWS</senderName>


      <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
      <parameter>
           <valueName>WEAHandling</valueName>
           <value>Imminent Threat</value>
   </parameter>
      <parameter>
           <valueName>CMAMtext</valueName>
           <value>[Short Spanish Test Message 7]</value>
   </parameter>
      <parameter>
           <valueName>CMAMlongtext</valueName>
           <value>[Long Spanish Test Message 7]</value>
   </parameter>
      <area>
     <areaDesc>FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA</areaDesc>
     <geocode>
       <valueName>SAME</valueName>
       <value>051059</value>
     </geocode>
     <geocode>
       <valueName>SAME</valueName>
       <value>051013</value>
     </geocode>
   </area>
    </info>
</alert>
```

B.8 CAP Message #8 – Imminent Threat Cancel

```
<?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 8]</identifier>
  <sender>[Message Sender 8]</sender>
  <sent>[CAP Sent Date-Time 8]</sent>
  <status>Actual</status>
  <msgType>Cancel</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 1],[CAP Message ID 1],[CAP Sent Date-Time 1]</references>
</alert>
```

B.9 CAP Message #9 – Imminent Threat Alert for Geo Location Filtering

```
<?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 9]</identifier>
  <sender>[Message Sender 9]</sender>
  <sent>[CAP Sent Date-Time 9]</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <info>
   <language>en-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 9]</expires>
   <senderName>NWS</senderName>
     <headline> Test Update Message only Disregard please.</headline>
   <description> THIS is NOT an Actual Message. It is only a test Update. This is
Descriptive text that defines the alert</description>
   <instruction>This is not an Actual message. It is only a test update. This is where
the call to action for those receiving the message should be provided.</instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 9]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 9] </value>
     </parameter>
   <area>
     <areaDesc>TEST AREA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #1]</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #2]</value>
     </geocode>
   </area>
  </info>
  <info>
   <language>es-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 9]</expires>
   <senderName>NWS</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
   </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 9]</value>
   </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 9]</value>
   </parameter>
   <area>
     <areaDesc>TEST AREA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #1]</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #2]</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.10 CAP Message #10 – Imminent Threat Update for Geo Location Filtering

```
<?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 10]</identifier>
  <sender>[Message Sender 10]</sender>
  <sent>[CAP Sent Date-Time 10]</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 9],[CAP Message ID 9],[CAP Sent Date-Time 9]
   </references>
  <info>
   <language>en-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time 10]</expires>
   <senderName>NWS</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test Update. This is
Descriptive text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test Update. This is where
the call to action for those receiving the message should be provided.</instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
   </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 10]</value>
   </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 10] </value>
   </parameter>
   <area>
     <areaDesc>TEST AREA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #1]</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #2]</value>
     </geocode>
   </area>
  </info>
  <info>
   <language>es-US</language>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM WARNING</event>
   <urgency>Immediate</urgency>
   <severity>Extreme</severity>
   <certainty>Observed</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>SVR</value>
   </eventCode>
   <expires>[Expires Date-Time]</expires>
   <senderName>NWS</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
     <parameter>
          <valueName>WEAHandling</valueName>
          <value>Imminent Threat</value>
   </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 10]</value>
   </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 10]</value>
   </parameter>
   <area>
     <areaDesc>TEST AREA</areaDesc>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #1]</value>
     </geocode>
     <geocode>
      <valueName>SAME</valueName>
      <value>[County Code #2]</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.11 CAP Message #11 – Imminent Threat Cancel for Geo Location Filtering

```
<?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 11]</identifier>
  <sender>[Message Sender 11]</sender>
  <sent>[CAP Sent Date-Time 11]</sent>
  <status>Actual</status>
  <msgType>Cancel</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <references>[Message Sender 10],[CAP Message ID 10],[CAP Sent Date-Time 10]
   </references>
</alert>
```

B.12 CAP Message #12 – Public Safety 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 12]</identifier>
  <sender>[Message Sender 12]</sender>
  <sent>[CAP Sent Date-Time 12]</sent>
  <status>Actual</status>
   <msgType>Alert</msgType>
   <scope>Public</scope>
   <code>IPAWSv1.0</code>
   <info>
          <language>en-US</language>
          <category>Safety</category>
          <event>Local Area Emergency</event>
          <responseType>Monitor</responseType>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
                 <valueName>SAME</valueName>
                 <value>LAE</value>
          </eventCode>
          <expires>[Expires Date-Time 12]</expires>
          <senderName>Fairfax County EMA</senderName>
   <headline> Test Message only Disregard please.</headline>
          <description> THIS is NOT an Actual Message. It is only a test. This is
Descriptive text that defines the alert.</description>
          <instruction>This is not an Actual message. It is only a Test. This is where
the call to action for those receiving the message should be provided.</instruction>
          <parameter>
                 <valueName>WEAHandling</valueName>
                 <value>Public Safety</value>
          </parameter>
       <parameter>
              <valueName>CMAMtext</valueName>
              <value>[Short English Test Message 12] </value>
       </parameter>
       <parameter>
              <valueName>CMAMlongtext</valueName>
              <value>[Long English Test Message 12]</value>
       </parameter>
          <area>
                 <areaDesc>Los Angeles County</areaDesc>
                 <geocode>
                        <valueName>SAME</valueName>
                        <value>006037</value>
                 </geocode>
          </area>
   </info>
   <info>
          <language>es-US</language>
          <category>Safety</category>
          <event>Local Area Emergency</event>
          <responseType>Monitor</responseType>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
                 <valueName>SAME</valueName>
                 <value>LAE</value>
          </eventCode>
          <expires>[Expires Date-Time 12]</expires>
          <senderName>Fairfax County EMA</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje. </instruction>
          <parameter>
                 <valueName>WEAHandling</valueName>
                 <value>Public Safety</value>
          </parameter>
       <parameter>
              <valueName>CMAMtext</valueName>
              <value>[Short Spanish Test Message 12]</value>
       </parameter>
       <parameter>
              <valueName>CMAMlongtext</valueName>
              <value>[Long Spanish Test Message 12]</value>
       </parameter>
          <area>
                 <areaDesc>Los Angeles County</areaDesc>
                 <geocode>
                        <valueName>SAME</valueName>
                        <value>006037</value>
                 </geocode>
          </area>
   </info>
</alert>
```

B.13 CAP Message #13 – State/Local WEA Test 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 13]</identifier>
  <sender>[Message Sender 13]</sender>
  <sent>[CAP Sent Date-Time 13]</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>IPAWSv1.0</code>
  <info>
   <language>en-US</language>
   <category>Rescue</category>
   <event>Required Weekly Test</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>RWT</value>
   </eventCode>
   <expires>[Expires Date-Time 13]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>WEA Test</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 13]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 13]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
       <valueName>SAME</valueName>
       <value>006037</value>
     </geocode>
   </area>
  </info>
<info>
   <language>es-US</language>
   <category>Rescue</category>
   <event>Required Weekly Test</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>RWT</value>
   </eventCode>
   <expires>[Expires Date-Time 13]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>WEA Test</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 13]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 13]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
       <valueName>SAME</valueName>
       <value>006037</value>
     </geocode>
   </area>
  </info>
</alert>
```

B.14 CAP Message #14 – Public Safety Update

```
<?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 14]</identifier>
  <sender>[Message Sender 14]</sender>
  <sent>[CAP Sent Date-Time 14]</sent>
  <status>Actual</status>
   <msgType>Update</msgType>
   <scope>Public</scope>
   <code>IPAWSv1.0</code>
  <references> [Message Sender 12],[CAP Message ID 12],[CAP Sent Date-Time 12]
   </references>
   <info>
          <language>en-US</language>
          <category>Rescue</category>
          <event>Local Area Emergency</event>
          <responseType>Monitor</responseType>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
                 <valueName>SAME</valueName>
                 <value>LAE</value>
          </eventCode>
          <expires>[Expires Date-Time 14]</expires>
          <senderName>Fairfax County EMA</senderName>
   <headline> Test Message only Disregard please.</headline>
          <description> THIS is NOT an Actual Message. It is only a test. This is
Descriptive text that defines the alert.</description>
          <instruction>This is not an Actual message. It is only a Test. This is where
the call to action for those receiving the message should be provided.</instruction>
          <parameter>
                 <valueName>WEAHandling</valueName>
                 <value>Public Safety</value>
          </parameter>
       <parameter>
              <valueName>CMAMtext</valueName>
              <value>[Short English Test Message 14]</value>
       </parameter>
       <parameter>
              <valueName>CMAMlongtext</valueName>
              <value>[Long English Test Message 14]</value>
       </parameter>
          <area>
       <areaDesc>Los Angeles County</areaDesc>
       <geocode>
        <valueName>SAME</valueName>
        <value>006037</value>
       </geocode>
          </area>
   </info>
   <info>
          <language>es-US</language>
          <category>Rescue</category>
          <event>Local Area Emergency</event>
          <responseType>Monitor</responseType>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
                 <valueName>SAME</valueName>
                 <value>LAE</value>
          </eventCode>
          <expires>[Expires Date-Time 14]</expires>
          <senderName>Fairfax County EMA</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje.</instruction>
          <parameter>
                 <valueName>WEAHandling</valueName>
                 <value>Public Safety</value>
          </parameter>
       <parameter>
              <valueName>CMAMtext</valueName>
              <value>[Short Spanish Test Message 14]</value>
       </parameter>
       <parameter>
              <valueName>CMAMlongtext</valueName>
              <value>[Long Spanish Test Message 14]</value>
       </parameter>
          <area>
       <areaDesc>Los Angeles County</areaDesc>
       <geocode>
        <valueName>SAME</valueName>
        <value>006037</value>
     </geocode>
   </area>
   </info>
</alert>
```

B.15 CAP Message #15 – State/Local WEA Test Update

```
<?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 15]</identifier>
    <sender>[Message Sender 15]</sender>
    <sent>[CAP Sent Date-Time 15]</sent>
    <status>Actual</status>
    <msgType>Update</msgType>
    <scope>Public</scope>
    <code>IPAWSv1.0</code>
    <references> [Message Sender 13],[CAP Message ID 13],[CAP Sent Date-Time 13]
     </references>
    <info>
     <language>en-US</language>
     <category>Rescue</category>
     <event>Required Weekly Test</event>
     <urgency>Immediate</urgency>
     <severity>Severe</severity>
     <certainty>Likely</certainty>
     <eventCode>
       <valueName>SAME</valueName>
       <value>RWT</value>
     </eventCode>
     <expires>[Expires Date-Time 15]</expires>
```

```
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Test Message only Disregard please.</headline>
     <description> THIS is NOT an Actual Message. It is only a test. This is Descriptive
text that defines the alert.</description>
   <instruction>This is not an Actual message. It is only a Test. This is where the call
to action for those receiving the message should be provided.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>WEA Test</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short English Test Message 15]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long English Test Message 15]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
       <valueName>SAME</valueName>
       <value>006037</value>
     </geocode>
   </area>
  </info>
<info>
   <language>es-US</language>
   <category>Rescue</category>
   <event>Required Weekly Test</event>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Likely</certainty>
   <eventCode>
     <valueName>SAME</valueName>
     <value>RWT</value>
   </eventCode>
   <expires>[Expires Date-Time 15]</expires>
   <senderName>Los Angeles Police Dept - LAPD</senderName>
     <headline> Mensaje de prueba solo No tener en cuenta, por favor.</headline>
   <description> ESTO NO ES un mensaje real. Es solo una prueba. Este es un texto
descriptivo que define la alerta. </description>
   <instruction> Este no es un mensaje real. Es solo una prueba. Aqui es donde debe
proporcionarse el llamado a la accion para quienes reciben el mensaje.</instruction>
   <parameter>
          <valueName>WEAHandling</valueName>
          <value>WEA Test</value>
     </parameter>
     <parameter>
          <valueName>CMAMtext</valueName>
          <value>[Short Spanish Test Message 15]</value>
     </parameter>
     <parameter>
          <valueName>CMAMlongtext</valueName>
          <value>[Long Spanish Test Message 15]</value>
     </parameter>
   <area>
     <areaDesc>Los Angeles County</areaDesc>
     <geocode>
       <valueName>SAME</valueName>
       <value>006037</value>
     </geocode>
   </area>
  </info>
</alert>
```

Annex C
(normative)

Annex C Expected CMAC Messages

The following messages are the expected CMAC messages that result from executing test cases in Clause 5. Some of the element values are based on default or sample values from the CAP messages in Annex B, *Input CAP Messages*. The elements and element values 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 CMAC Message #1 – Expected Results of CAP Message #1

This clause contains the various CMAC messages that are the result of CAP Message #1.

C.1.1 CMAC Message #1 – Imminent Threat Alert (Expected Result of CAP 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:2.0">
  <CMAC_protocol_version>2.0</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_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_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>Met</CMAC_category>
   <CMAC_severity>Severe</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_Alert_Area>
     <CMAC_area_description>FAIRFAX COUNTY IN VIRGINIA</CMAC_area_description>
     <CMAC_polygon>38.918361,-77.341233 38.903401,-77.289734 38.869194,-77.354279
38.918361,-77.341233</CMAC_polygon>
     <CMAC_cmas_geocode>51059</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 1]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 1]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 1]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 1]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 1]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 1]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 1]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 1]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 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 C.1: CMAC Message #1 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	"2.0"
<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 Coordinated Universal Time (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_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> of 1st CMAC_Alert_Text segment	"English"
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message>	[Short English Text Message 1] of 1st CMAC_Alert_Text segment not exceeding 90 characters
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 1] of 1st CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	"Spanish"
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.

CMAC Element	Value
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 1] of 2nd CMAC_Alert_Text segment not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 1] of 2nd CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_area_description>	FAIRFAX COUNTY IN VIRGINIA
<CMAC_polygon>	38.918361,-77.341233 38.903401,-77.289734 38.869194,-77.354279 38.918361,-77.341233
<CMAC_cmas_geocode>	51059

C.1.2 CMAC Message #1A – Imminent Threat Alert with Expanded Digital Signature Segment (Expected Result of CAP 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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 1A]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 1A]</CMAC_message_number>
  <CMAC_sender>[Message Sender 1]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 1A]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 1A]</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>Met</CMAC_category>
   <CMAC_severity>Severe</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_Alert_Area>
     <CMAC_area_description>FAIRFAX COUNTY IN VIRGINIA</CMAC_area_description>
     <CMAC_polygon>38.918361,-77.341233 38.903401,-77.289734 38.869194,-77.354279
38.918361,-77.341233</CMAC_polygon>
     <CMAC_cmas_geocode>51059</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 1A]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 1A]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 1A]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 1A]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 1A]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 1A]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
```

```
      [Long Spanish Text Message Length 1A]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 1A]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
</CMAC_alert_info>
  <CMAC_Digital_Signature>
  <Signature xmlns=”http://www.w3.org/2000/09/xmldsig#”>
  <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/TR/xml-exc-c14n/"/>
   <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
     <Reference>
     <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <DigestValue>[Digest Value 1A]</DigestValue>
     </Reference>
  </SignedInfo>
  <SignatureValue>[Signature Value 1A]</SignatureValue>
  <KeyInfo>
     <X509Data>[X509 Data 1A]</X509Data>
  </KeyInfo>
  </Signature>
  </CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.2 CMAC Message #2 – National Alert (Expected Result of CAP Message #2)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 2]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 2]</CMAC_message_number>
  <CMAC_special_handling>Presidential</CMAC_special_handling>
  <CMAC_sender>[Message Sender 2]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 2]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 2]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 2]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 2]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Security</CMAC_category>
   <CMAC_severity>Extreme</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 2]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description>U.S. Nationwide</CMAC_area_description>
     <CMAC_cmas_geocode>00000</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 2]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 2]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 2]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 2]
```

```
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 2]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 2]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 2]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 2]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 2]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.3 CMAC Message #3 – AMBER Alert (Expected Result of CAP Message #3)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 3]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 3]</CMAC_message_number>
  <CMAC_special_handling>Child Abduction</CMAC_special_handling>
  <CMAC_sender>[Message Sender 3]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 3]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 3]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 3]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 3]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 3]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 3]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 3]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 3]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 3]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 3]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 3]
```

```
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 3]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 3]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 3]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.4 CMAC Message #4 – Imminent Threat Update (Expected Result of CAP Message #4)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 4]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 4]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 1]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 1]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_sender>[Message Sender 4]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 4]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Update</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 4]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 4]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 4]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Met</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Observed</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 4]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description>FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA
      </CMAC_area_description>
     <CMAC_cmas_geocode>51059</CMAC_cmas_geocode>
     <CMAC_cmas_geocode>51013</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 4]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 4]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 4]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 4]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 4]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 4]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 4]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 4]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
  <CMAC_Digital_Signature>[Digital Signature Elements 4]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #4 of the logged CMAC message:

Table C.2: CMAC Message #4 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 4]
<CMAC_message_number>	[CMAC Message Number 4]
<CMAC_referenced_message_number>	[CMAC Message Number 1] from CMAC Message #1
<CMAC_referenced_message_cap_ identifier>	[CAP Message ID 1] from CAP Message #1
<CMAC_sender>	[Message Sender 4] from CAP Message #4
<CMAC_sent_date_time>	[CMAC Sent Date-Time 4] in UTC in XML dateTime format
<CMAC_status>	“Actual”
<CMAC_message_type>	“Update”
<CMAC_cap_alert_uri>	[Message URI 4]
<CMAC_cap_identifier>	[CAP Message ID 4] from CAP Message #4
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 4] from CAP Message #4
<CMAC_category>	“Met”
<CMAC_severity>	“Severe”
<CMAC_urgency>	“Immediate”
<CMAC_certainty>	“Observed”
<CMAC_expires_date_time>	[Expires Date-Time 4] from CAP Message #4 in UTC in XML dateTime format
<CMAC_text_language> of 1st CMAC_Alert_Text segment	“English”
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 4] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message>	[Short English Text Message 4] of 1st CMAC_Alert_Text segment not exceeding 90 characters
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 4] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 4] of 1st CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	“Spanish”
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 4] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 4] of 2nd CMAC_Alert_Text segment not exceeding 90 characters.

CMAC Element	Value
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 4] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 4] of 2nd CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_area_description>	FAIRFAX AND ARLINGTON COUNTIES IN VIRGINIA
<CMAC_cmas_geocode>	51059
<CMAC_cmas_geocode>	51013

C.5 CMAC Message #5 – National Update (Expected Result of CAP Message #5)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 5]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 5]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 2]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 2]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_special_handling>Presidential</CMAC_special_handling>
  <CMAC_sender>[Message Sender 5]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 5]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Update</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 5]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 5]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 5]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Security</CMAC_category>
   <CMAC_severity>Extreme</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Observed</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 5]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description>U.S. Nationwide</CMAC_area_description>
     <CMAC_cmas_geocode>00000</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 5]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 5]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 5]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 5]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 5]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 5]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
```

```
      [Long Spanish Text Message Length 5]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 5]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
  <CMAC_Digital_Signature>[Digital Signature Elements 5]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #5 of the logged CMAC message:

Table C.3: CMAC Message #5 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	"2.0"
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 5]
<CMAC_message_number>	[CMAC Message Number 5]
<CMAC_referenced_message_number>	[CMAC Message Number 2] from CMAC Message #2
<CMAC_referenced_message_cap_ identifier>	[CAP Message ID 2] from CAP Message #2
<CMAC_special_handling>	"Presidential"[10]
<CMAC_sender>	[Message Sender 5] from CAP Message #5
<CMAC_sent_date_time>	[CMAC Sent Date-Time 5] in UTC in XML dateTime format
<CMAC_status>	"Actual"
<CMAC_message_type>	"Update"
<CMAC_cap_alert_uri>	[Message URI 5]
<CMAC_cap_identifier>	[CAP Message ID 5] from CAP Message #5
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 5] from CAP Message #5
<CMAC_category>	"Security"
<CMAC_severity>	"Extreme"
<CMAC_urgency>	"Immediate"
<CMAC_certainty>	"Observed"
<CMAC_expires_date_time>	[Expires Date-Time 5] from CAP Message #5 in UTC in XML dateTime format
<CMAC_text_language> of 1st CMAC_Alert_Text segment	"English"
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 5] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message>	[Short English Text Message 5] of 1st CMAC_Alert_Text segment not exceeding 90 characters
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 5] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 5] of 1st CMAC_Alert_Text segment not exceeding 360 characters.

[10] Presidential Alert has been renamed to National Alert. However, protocol encoding on the C-interface still uses the term "Presidential".

CMAC Element	Value
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	"Spanish"
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 5] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 5] of 2nd CMAC_Alert_Text segment not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 5] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 5] of 2nd CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_area_description>	"U.S. Nationwide"
<CMAC_cmas_geocode>	"00000"

C.6 CMAC Message #6 – AMBER Update (Expected Result of CAP Message #6)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 6]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 6]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 3]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 3]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_special_handling>Child Abduction</CMAC_special_handling>
  <CMAC_sender>[Message Sender 6]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 6]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Update</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 6]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 6]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 6]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Observed</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 6]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County and San Bernardino County
      </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
     <CMAC_cmas_geocode>06071</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 6]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 6]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 6]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 6]
```

```
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 6]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short Spanish Text Message 6]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 6]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 6]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
  <CMAC_Digital_Signature>[Digital Signature Elements 6]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #6 of the logged CMAC message:

Table C.4: CMAC Message #6 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 6]
<CMAC_message_number>	[CMAC Message Number 6]
<CMAC_referenced_message_number>	[CMAC Message Number 3] from CMAC Message #3
<CMAC_referenced_message_cap_ identifier>	[CAP Message ID 3] from CAP Message #3
<CMAC_special_handling>	“Child Abduction”
<CMAC_sender>	[Message Sender 6] from CAP Message #6
<CMAC_sent_date_time>	[CMAC Sent Date-Time 6] in UTC in XML dateTime format
<CMAC_status>	“Actual”
<CMAC_message_type>	“Update”
<CMAC_cap_alert_uri>	[Message URI 6]
<CMAC_cap_identifier>	[CAP Message ID 6] from CAP Message #6
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 6] from CAP Message #6
<CMAC_category>	“Rescue”
<CMAC_severity>	“Severe”
<CMAC_urgency>	“Immediate”
<CMAC_certainty>	“Observed”
<CMAC_expires_date_time>	[Expires Date-Time 6] from CAP Message #6 in UTC in XML dateTime format
<CMAC_text_language> of 1st CMAC_Alert_Text segment	“English”
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 6] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message>	[Short English Text Message 6] of 1st CMAC_Alert_Text segment not exceeding 90 characters.

CMAC Element	Value
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 6] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 6] of 1st CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	“Spanish”
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 6] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 6] of 2nd CMAC_Alert_Text segment not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 6] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 6] of 2nd CMAC_Alert_Text segment not exceeding 360 characters.
<CMAC_area_description>	“Los Angeles County and San Bernardino County”
<CMAC_cmas_geocode>	“06037”
<CMAC_cmas_geocode>	“06071”

C.7 CMAC Message #7 – Invalid WEA Criteria Cancel (Expected Result of CAP Message #7)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 7]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 7]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 4]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 4]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_sender>[Message Sender 7]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 7]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Cancel</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 7]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 7]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 7]</CMAC_cap_sent_date_time>
  <CMAC_Digital_Signature>[Digital Signature Elements 7]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.8 CMAC Message #8 – Imminent Threat Cancel (Expected Result of CAP Message #8)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 8]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 8]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 1]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 1]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_sender>[Message Sender 8]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 8]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Cancel</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 8]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 8]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 8]</CMAC_cap_sent_date_time>
  <CMAC_Digital_Signature>[Digital Signature Elements 8]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #8 of the logged CMAC message:

Table C.5: CMAC Message #8 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 8]
<CMAC_message_number>	[CMAC Message Number 8]
<CMAC_referenced_message_number>	[CMAC Message Number 1] from CMAC Message #1
<CMAC_referenced_message_cap_identifier>	[CAP Message ID 1] from CAP Message #1
<CMAC_sender>	[Message Sender 8] from CAP Message #8
<CMAC_sent_date_time>	[CMAC Sent Date-Time 8] in UTC in XML dateTime format
<CMAC_status>	“Actual”
<CMAC_message_type>	“Cancel”
<CMAC_cap_alert_uri>	[Message URI 8]
<CMAC_cap_identifier>	[CAP Message ID 8] from CAP Message #8
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 8] from CAP Message #8

C.9 CMAC Message #9 – RMT

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 9]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 9]</CMAC_message_number>
  <CMAC_special_handling>Required Monthly Test</CMAC_special_handling>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 9]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>RMT</CMAC_message_type>
  <CMAC_alert_info>
   <CMAC_category>Other</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Expected</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 9]</CMAC_expires_date_time>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 9]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 9]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 9]
      </CMAC_long_text_alert_message_length>
```

```
        <CMAC_long_text_alert_message>[Long English Text Message 9]
          </CMAC_long_text_alert_message>
      </CMAC_Alert_Text>
    </CMAC_alert_info>
    <CMAC_Digital_Signature>[Digital Signature Elements 9]</CMAC_Digital_Signature>
  </CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #9 of the logged CMAC message:

Table C.6: CMAC Message #9 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 9]
<CMAC_message_number>	[CMAC Message Number 9]
<CMAC_special_handling>	“Required Monthly Test”
<CMAC_sent_date_time>	[CMAC Sent Date-Time 9] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“RMT”
<CMAC_category>	“Other”
<CMAC_severity>	“Severe”
<CMAC_urgency>	“Expected”
<CMAC_certainty>	“Likely”
<CMAC_expires_date_time>	[Expires Date-Time 9] from RMT CAP Message in UTC in XML dateTime format.
<CMAC_text_language>	“English”
<CMAC_short_text_alert_message_length>	[Short English Text Message Length 9] equal to the number of characters in <CMAC_short_text_alert_message> value.
<CMAC_short_text_alert_message>	[Short English Text Message 9] not exceeding 90 characters.
<CMAC_long_text_alert_message_length>	[Long English Text Message Length 9] equal to the number of characters in <CMAC_long_text_alert_message> value.

C.10 CMAC Message #10 – Federal Alert Gateway Initiated Link Test

```
  <?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:2.0">
    <CMAC_protocol_version>2.0</CMAC_protocol_version>
    <CMAC_sending_gateway_id>[Federal Alert Gateway ID 10]</CMAC_sending_gateway_id>
    <CMAC_message_number>[CMAC Message Number 10]</CMAC_message_number>
    <CMAC_sent_date_time>[CMAC Sent Date-Time 10]</CMAC_sent_date_time>
    <CMAC_status>System</CMAC_status>
    <CMAC_message_type>Link Test</CMAC_message_type>
  </CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #10 of the logged CMAC message:

Table C.7: CMAC Message #10 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 10]
<CMAC_message_number>	[CMAC Message Number 10]
<CMAC_sent_date_time>	[CMAC Sent Date-Time 10] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“Link Test”

C.11 CMAC Message #11 – CMSP Gateway Initiated Link Test

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 11]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 11]</CMAC_message_number>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 11]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Link Test</CMAC_message_type>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #11 of the logged CMAC message:

Table C.8: CMAC Message #11 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[CMSP Gateway ID 11]
<CMAC_message_number>	[CMAC Message Number 11]
<CMAC_sent_date_time>	[CMAC Sent Date-Time 11] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“Link Test”

C.12 CMAC Message #12 – Transmission Control – Cease

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 12]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 12]</CMAC_message_number>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 12]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Transmission Control - Cease</CMAC_message_type>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #12 of the logged CMAC message:

Table C.9: CMAC Message #12 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[CMSP Gateway ID 12]
<CMAC_message_number>	[CMAC Message Number 12]
<CMAC_sent_date_time>	[CMAC Sent Date-Time 12] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“Transmission Control - Cease”

C.13 CMAC Message #13 – Transmission Control – Resume

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 13]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 13]</CMAC_message_number>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 13]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Transmission Control - Resume</CMAC_message_type>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #13 of the logged CMAC message:

Table C.10: CMAC Message #13 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[CMSP Gateway ID 13]
<CMAC_message_number>	[CMAC Message Number 13]
<CMAC_sent_date_time>	[CMAC Sent Date-Time 13] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“Transmission Control - Resume”

C.14 CMAC Message #14 – Public Safety Alert (Expected Result of CAP Message #12)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 14]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 14]</CMAC_message_number>
  <CMAC_special_handling>Public Safety</CMAC_special_handling>
  <CMAC_sender>[Message Sender 14]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 14]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 14]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 14]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 14]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 14]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 14]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 14]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 14]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 14]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 14]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 14]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 14]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 14]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 14]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.15 CMAC Message #15 – State/Local WEA Test Alert (Expected Result of CAP Message #13)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 15]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 15]</CMAC_message_number>
  <CMAC_special_handling>State Local WEA Test</CMAC_special_handling>
  <CMAC_sender>[Message Sender 15]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 15]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Alert</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 15]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 15]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 15]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 15]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 15]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 15]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 15]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 15]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 15]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 15]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 15]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 15]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 15]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

C.16 CMAC Message #16 – Public Safety Update (Expected Result of CAP Message #14)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 16]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 16]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 14]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 14]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_special_handling>Public Safety</CMAC_special_handling>
  <CMAC_sender>[Message Sender 14]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 16]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Update</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 14]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 14]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 14]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 14]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 16]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 16]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 16]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 16]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 16]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 16]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 16]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 16]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 16]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #16 of the logged CMAC message:

Table C.11: CMAC Message #16 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 16]
<CMAC_message_number>	[CMAC Message Number 16]
<CMAC_referenced_message_number>	[CMAC Message Number 14] from CMAC Message #14
<CMAC_referenced_message_cap_ identifier>	[CAP Message ID 14] from CAP Message #14
<CMAC_special_handling>	“Public Safety”
<CMAC_sender>	[Message Sender 14] from CAP Message #14
<CMAC_sent_date_time>	[CMAC Sent Date-Time 6] in UTC in XML dateTime format
<CMAC_status>	“Actual”
<CMAC_message_type>	“Update”
<CMAC_cap_alert_uri>	[Message URI 14]
<CMAC_cap_identifier>	[CAP Message ID 14] from CAP Message #14
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 14] from CAP Message #14
<CMAC_category>	“Rescue”
<CMAC_severity>	“Severe”
<CMAC_urgency>	“Immediate”
<CMAC_certainty>	“Observed”
<CMAC_expires_date_time>	[Expires Date-Time 14] from CAP Message #14 in UTC in XML dateTime format
<CMAC_text_language> of 1st CMAC_Alert_Text segment	“English”

CMAC Element	Value
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 1st CMAC_Alert_Text segment	[Short English Text Message 1] not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 1] not exceeding 360 characters.
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	“Spanish”
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 1] not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 1] not exceeding 360 characters.
<CMAC_area_description>	“Los Angeles County and San Bernardino County”
<CMAC_cmas_geocode>	“06037”
<CMAC_cmas_geocode>	“06071”

C.17 CMAC Message #17 – State/Local WEA Test Update (Expected Result of CAP Message #15)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 17]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Message Number 17]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 15]
   </CMAC_referenced_message_number>
  <CMAC_referenced_message_cap_identifier>[CAP Message ID 15]
   </CMAC_referenced_message_cap_identifier>
  <CMAC_special_handling>State Local WEA Test</CMAC_special_handling>
  <CMAC_sender>[Message Sender 15]</CMAC_sender>
  <CMAC_sent_date_time>[CMAC Sent Date-Time 17]</CMAC_sent_date_time>
  <CMAC_status>Actual</CMAC_status>
  <CMAC_message_type>Update</CMAC_message_type>
  <CMAC_cap_alert_uri>[Message URI 15]</CMAC_cap_alert_uri>
  <CMAC_cap_identifier>[CAP Message ID 15]</CMAC_cap_identifier>
  <CMAC_cap_sent_date_time>[CAP Sent Date-Time 15]</CMAC_cap_sent_date_time>
  <CMAC_alert_info>
   <CMAC_category>Rescue</CMAC_category>
   <CMAC_severity>Severe</CMAC_severity>
   <CMAC_urgency>Immediate</CMAC_urgency>
   <CMAC_certainty>Likely</CMAC_certainty>
   <CMAC_expires_date_time>[Expires Date-Time 15]</CMAC_expires_date_time>
   <CMAC_Alert_Area>
     <CMAC_area_description> Los Angeles County </CMAC_area_description>
     <CMAC_cmas_geocode>06037</CMAC_cmas_geocode>
   </CMAC_Alert_Area>
   <CMAC_Alert_Text>
    <CMAC_text_language>English</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short English Text Message Length 17]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 17]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long English Text Message Length 17]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long English Text Message 17]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
   <CMAC_Alert_Text>
    <CMAC_text_language>Spanish</CMAC_text_language>
    <CMAC_short_text_alert_message_length>
      [Short Spanish Text Message Length 17]
      </CMAC_short_text_alert_message_length>
    <CMAC_short_text_alert_message>[Short English Text Message 17]
      </CMAC_short_text_alert_message>
    <CMAC_long_text_alert_message_length>
      [Long Spanish Text Message Length 17]
      </CMAC_long_text_alert_message_length>
    <CMAC_long_text_alert_message>[Long Spanish Text Message 17]
      </CMAC_long_text_alert_message>
   </CMAC_Alert_Text>
  </CMAC_alert_info>
   <CMAC_Digital_Signature>[Digital Signature Elements 17]</CMAC_Digital_Signature>
</CMAC_Alert_Attributes>
```

The following table contains the expected message elements and values of the CMAC Message #17 of the logged CMAC message:

Table C.12: CMAC Message #17 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	"2.0"
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 17]
<CMAC_message_number>	[CMAC Message Number 17]
<CMAC_referenced_message_number>	[CMAC Message Number 15] from CMAC Message #15
<CMAC_referenced_message_cap_identifier>	[CAP Message ID 15] from CAP Message #15
<CMAC_special_handling>	"Public Safety"
<CMAC_sender>	[Message Sender 14] from CAP Message #15
<CMAC_sent_date_time>	[CMAC Sent Date-Time 6] in UTC in XML dateTime format
<CMAC_status>	"Actual"
<CMAC_message_type>	"Update"
<CMAC_cap_alert_uri>	[Message URI 15]
<CMAC_cap_identifier>	[CAP Message ID 14] from CAP Message #15
<CMAC_cap_sent_date_time>	[CAP Sent Date-Time 14] from CAP Message #15
<CMAC_category>	"Rescue"
<CMAC_severity>	"Severe"
<CMAC_urgency>	"Immediate"
<CMAC_certainty>	"Observed"

CMAC Element	Value
<CMAC_expires_date_time>	[Expires Date-Time 15] from CAP Message #15 in UTC in XML dateTime format
<CMAC_text_language> of 1st CMAC_Alert_Text segment	"English"
<CMAC_short_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Short English Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 1st CMAC_Alert_Text segment	[Short English Text Message 1] not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 1st CMAC_Alert_Text segment	[Long English Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 1st CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 1st CMAC_Alert_Text segment	[Long English Text Message 1] not exceeding 360 characters.
<CMAC_text_language> of 2nd CMAC_Alert_Text segment	"Spanish"
<CMAC_short_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message Length 1] equal to the number of characters in <CMAC_short_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_short_text_alert_message> of 2nd CMAC_Alert_Text segment	[Short Spanish Text Message 1] not exceeding 90 characters.
<CMAC_long_text_alert_message_length> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message Length 1] equal to the number of characters in <CMAC_long_text_alert_message> value of 2nd CMAC_Alert_Text segment.
<CMAC_long_text_alert_message> of 2nd CMAC_Alert_Text segment	[Long Spanish Text Message 1] not exceeding 360 characters.
<CMAC_area_description>	"Los Angeles County and San Bernardino County"
<CMAC_cmas_geocode>	"06037"
<CMAC_cmas_geocode>	"06071"

Annex D
(normative)

Annex D Expected ACK Messages

The following messages are the expected CMAC Ack messages sent by the CMSP Gateway in response to the CMAC Alert messages in Annex C, *Expected CMAC Messages*. Some of the element values are based on default or sample values from the CMAC messages. The elements and element values 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 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:2.0">
  <CMAC_protocol_version>2.0</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 D.1: Ack Message #1 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<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”

D.2 Ack Message #2 (Expected Result of CMAC Message #2)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 2]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Ack Message Number 2]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 2]
   </CMAC_referenced_message_number>
  <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 2]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Ack</CMAC_message_type>
</CMAC_Alert_Attributes>
```

D.3 Ack Message #3 (Expected Result of CMAC Message #3)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 3]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Ack Message Number 3]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 3]
   </CMAC_referenced_message_number>
  <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 3]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Ack</CMAC_message_type>
</CMAC_Alert_Attributes>
```

D.4 Ack Message #4 (Expected Result of CMAC Message #11)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[Federal Alert Gateway ID 4]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Ack Message Number 4]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 11]
   </CMAC_referenced_message_number>
  <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 4]</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 #4 of the logged CMAC message:

Table D.2: Ack Message #4 Expected Messages & Values

CMAC Element	Value
<CMAC_protocol_version>	“2.0”
<CMAC_sending_gateway_id>	[Federal Alert Gateway ID 4]
<CMAC_message_number>	[CMAC Ack Message Number 4]
<CMAC_referenced_message_number>	[CMAC Message Number 11] from CMAC Message #11
<CMAC_sent_date_time>	[CMAC Ack Sent Date-Time 4] in UTC in XML dateTime format
<CMAC_status>	“System”
<CMAC_message_type>	“Ack”

D.5 Ack Message #5 (Expected Result of CMAC Message #14)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 5]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Ack Message Number 5]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 5]
   </CMAC_referenced_message_number>
  <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 5]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Ack</CMAC_message_type>
```

```
</CMAC_Alert_Attributes>
```

D.6 Ack Message #6 (Expected Result of CMAC Message #15)

```
<?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:2.0">
  <CMAC_protocol_version>2.0</CMAC_protocol_version>
  <CMAC_sending_gateway_id>[CMSP Gateway ID 6]</CMAC_sending_gateway_id>
  <CMAC_message_number>[CMAC Ack Message Number 6]</CMAC_message_number>
  <CMAC_referenced_message_number>[CMAC Message Number 6]
   </CMAC_referenced_message_number>
  <CMAC_sent_date_time>[CMAC Ack Sent Date-Time 6]</CMAC_sent_date_time>
  <CMAC_status>System</CMAC_status>
  <CMAC_message_type>Ack</CMAC_message_type>
</CMAC_Alert_Attributes>
```

Annex E

(informative)

Annex E Requirements Not Verified by Tests in This Specification

As explained in Clause 1.1, *Scope*, and Clause 1.2, *Purpose*, this specification is not intended to provide test cases to verify every requirement of the C-Interface. The focus is on the operational tests, intended to verify the establishment of the interface between the Federal Alert Gateway and the CMSP Gateway; demonstrate the ability to transmit, receive, and acknowledge Alert, Update, Cancel, and RMT messages; control the flow of messages through the use of geo-filtering, transmission control, and message queuing; and verify the use of Link Tests and CAP retrieval.

The requirements listed in Table E.1: *List of C-Interface Requirements Not Verified by Test Cases Contained in This Specification* are primarily in the areas related to security, HTTP connections, and handling of certain error conditions and they are not suitable for operational testing. These requirements are not covered by the test cases in this specification. It is expected that these requirements have been verified by other test procedures prior to operational testing.

Table E.1: List of C-Interface Requirements Not Verified by Test Cases Contained in This Specification

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-0320	[WEA-C-RQMT-0320] The Federal Alert Gateway shall try establishing an IPsec tunnel and a TCP connection at least per Reconnect Number times.
WEA-C-RQMT-0470	[WEA-C-RQMT-0470] The Federal Alert Gateway shall send an Error message to the CMSP Gateway when a CMSP Gateway message has been received with any error.
WEA-C-RQMT-0493	[WEA-C-RQMT-0493] The Federal Alert Gateway shall support versions 1.0 and 2.0 CMAC messages (defined in Clause 7.4).
WEA-C-RQMT-0550	[WEA-C-RQMT-0550] The Federal Alert Gateway shall receive and log Error messages from the CMSP Gateway.
WEA-C-RQMT-0820	[WEA-C-RQMT-0820] If the CMSP Gateway is unable to establish an IPsec tunnel and a TCP connection with the Federal Alert Gateways, the CMSP Gateway shall go down the list of Federal Alert Gateways in the Federal Alert Gateway Profile until it establishes an IPsec tunnel and a TCP connection or completes the list without establishing the connections.
WEA-C-RQMT-0830	[WEA-C-RQMT-0830] The CMSP Gateway shall try establishing an IPsec tunnel and a TCP connection with each Federal Alert Gateway at least per Reconnect Number times before moving to the next Gateway in the list.
WEA-C-RQMT-0910	[WEA-C-RQMT-0910] The CMSP Gateway shall send an Error message to a Federal Alert Gateway when a message has been received from that Federal Alert Gateway with an error.
WEA-C-RQMT-1040	[WEA-C-RQMT-1040] If the CMSP Gateway receives an “Update” message and cannot make an association with the “referenced message”, the CMSP Gateway shall process the “Update” as a new “Alert” message.
WEA-C-RQMT-1080	[WEA-C-RQMT-1080] The CMSP Gateway shall receive and log Error messages from the Federal Alert Gateway.
WEA-C-RQMT-1090	[WEA-C-RQMT-1090] If in any given monthly RMT cycle more than one RMT message is received by the CMSP, the CMSP Gateway shall accept only the first RMT message and shall reject all subsequent RMT messages within that calendar month.
WEA-C-RQMT-1100	[WEA-C-RQMT-1100] If the CMSP Gateway determines that an RMT message is invalid (e.g., not originated by the Federal Alert Gateway Administrator), the CMSP Gateway shall reject the RMT message.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-1120	[WEA-C-RQMT-1120] If conditions at the CMSP Gateway preclude distribution of the State/Local WEA Test message, the CMSP Gateway shall respond to the State/Local WEA Test message with an Error message (see Table 7.26 – Definition of CMAC Response Codes).
WEA-C-RQMT-1400	[WEA-C-RQMT-1400] Federal Alert Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.
WEA-C-RQMT-1410	[WEA-C-RQMT-1410] CMSP Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.
WEA-C-RQMT-1500	[WEA-C-RQMT-1500] The format for certificates between the CMSP Gateway and the Federal Alert Gateway shall be X.509 version 3 (X.509v3) certificate [Ref 19].
WEA-C-RQMT-1510	[WEA-C-RQMT-1510] The Federal Alert Gateway and the CMSP Gateway shall check the revocation status of the peer's X.509 certificate using the Online Certificate Status Protocol (OCSP), specified in RFC 6960 [Ref 34].
WEA-C-RQMT-1520	[WEA-C-RQMT-1520] Federal Alert Gateway and CMSP Gateways establishing security associations shall use OCSP over HTTP using the Nonce and Archive Cutoff options only.
WEA-C-RQMT-1600	[WEA-C-RQMT-1600] The identifiers for establishing an IPsec tunnel shall be the CMSP Gateway and Federal Alert Gateway Fully Qualified Domain Names or IP addresses.
WEA-C-RQMT-1610	[WEA-C-RQMT-1610] The Fully Qualified Domain Names and IP addresses shall be unique identifiers.
WEA-C-RQMT-1620	[WEA-C-RQMT-1620] The Federal Alert Gateway shall close the associated communication sockets, if the intended communication is with a CMSP Gateway and none of the distinguished names on the received certificate appear on the CMSP Gateway profile.
WEA-C-RQMT-1630	[WEA-C-RQMT-1630] The CMSP Gateway shall close the associated communication sockets, if the intended communication is with a Federal Alert Gateway and none of the distinguished names on the received certificate appear in the Federal Alert Gateway profile.
WEA-C-RQMT-1710	[WEA-C-RQMT-1710] An IPsec v3 tunnel shall be established to protect all messages when transmitted between the Federal Alert Gateway and the CMSP Gateway.
WEA-C-RQMT-1720	[WEA-C-RQMT-1720] The encrypted information shall include all CMAC messages as well as the associated keys.
WEA-C-RQMT-1800	[WEA-C-RQMT-1800] The Authentication Header (AH) option shall not be used.
WEA-C-RQMT-1910	[WEA-C-RQMT-1910] Manual keying shall not be used.
WEA-C-RQMT-1930	[WEA-C-RQMT-1930] All algorithms shall be upgradable with a new library and configuration change.
WEA-C-RQMT-1940	[WEA-C-RQMT-1940] Algorithm upgrades shall not require a full system hardware upgrade.
WEA-C-RQMT-1960	[WEA-C-RQMT-1960] <Void>.
WEA-C-RQMT-2000	[WEA-C-RQMT-2000] The only valid IPsec SAs shall be between a CMSP Gateway and a Federal Alert Gateway.
WEA-C-RQMT-2010	[WEA-C-RQMT-2010] The Federal Alert Gateway and CMSP Gateway IPsec implementation shall be capable of supporting port-based traffic filtering policies.
WEA-C-RQMT-2100	[WEA-C-RQMT-2100] Outbound packets to destinations for which SAs are not allowed shall be discarded.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-2110	[WEA-C-RQMT-2110] Outbound IKEv2 message packets destined for port 500 shall not be IPsec encrypted.
WEA-C-RQMT-2120	[WEA-C-RQMT-2120] All outbound packets not destined for port 500 shall be IPsec encrypted using the cryptographic material for the SA with the destination address.
WEA-C-RQMT-2200	[WEA-C-RQMT-2200] Inbound IKEv2 message packets destined for port 500 shall not be IPsec decrypted.
WEA-C-RQMT-2210	[WEA-C-RQMT-2210] Inbound packets that are not destined for Port 500 shall be IPsec decrypted using the cryptographic material for the SA with the source address.
WEA-C-RQMT-2220	[WEA-C-RQMT-2220] Inbound packets not destined for Port 500 and for which there is no SA for the source shall be discarded.
WEA-C-RQMT-2300	[WEA-C-RQMT-2300] SA Renewal and Rekey shall be configurable by Federal Alert Gateway and CMSP Gateway system administrators.
WEA-C-RQMT-2310	[WEA-C-RQMT-2310] IPsec SA shall have a maximum lifetime of IPSec SA Maximum Lifetime.
WEA-C-RQMT-2320	[WEA-C-RQMT-2320] IKE SA shall have a maximum lifetime of IKE SA Maximum Lifetime.
WEA-C-RQMT-2330	[WEA-C-RQMT-2330] Federal Alert Gateway and CMSP Gateway shall support SA renewal after expiration.
WEA-C-RQMT-2340	[WEA-C-RQMT-2340] Federal Alert Gateway and CMSP Gateway shall support SA rekey before expiration.
WEA-C-RQMT-2400	[WEA-C-RQMT-2400] The XML Signature Method shall be RSA-SHA256 [Ref 7] for XML Signatures applied to CMAC messages.
WEA-C-RQMT-2545$_{R3A}$	[WEA-C-RQMT-2545$_{R3A}$] The sum of the number of paired values of points (i.e., latitude/longitude pairs) used to define all the polygon(s) plus the number of circles is greater than the allowed maximum of 100 (see WEA-C-RQMT-2550), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2546$_{R3A}$	[WEA-C-RQMT-2546$_{R3A}$] If the total number of shapes is greater than the 10 shapes (e.g., polygons and circles) allowed (see WEA-C-RQMT-2551), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2550$_{R3M}$	[WEA-C-RQMT-2550$_{R3M}$] The number of paired values of points (i.e., latitude/longitude pairs) used to define the polygon in the CMAC_polygon element shall be limited to a maximum of 100.
WEA-C-RQMT-2551$_{R3A}$	[WEA-C-RQMT-2551$_{R3A}$] The sum of CMAC_Alert_Areas shall contain a combined maximum of 10 polygons and circles.
WEA-C-RQMT-2565	[WEA-C-RQMT-2565] The Cancel message shall discontinue the broadcast of all languages of the referenced Alert or Update message.
WEA-C-RQMT-2600	[WEA-C-RQMT-2600] Each Error message shall contain the mandatory message elements and associated values provided in the following table: • Table 7.19 – *Elements of Alert Attributes Segment for Error Message*
WEA-C-RQMT-2710	[WEA-C-RQMT-2710] HTTP communications carrying CMAC messages shall be to port TCP 8080.
WEA-C-RQMT-2720	[WEA-C-RQMT-2720] HTTP communications for CAP message retrieval shall be to port TCP 80.
WEA-C-RQMT-2730	[WEA-C-RQMT-2730] HTTP methods shall be limited to POST when CMAC Alert, Update, Cancel, RMT, and Link Test messages are sent over HTTP.
WEA-C-RQMT-2740	[WEA-C-RQMT-2740] HTTP methods shall be limited to GET when HTTP is used without the CMAC protocol.
WEA-C-RQMT-2750	[WEA-C-RQMT-2750] The HTTP POST method shall use "*" as the Request_URI.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-2760	[WEA-C-RQMT-2760] The HTTP GET method shall contain a Host request_header, whose value shall be the host part of the CMAC_cap_alert_uri.
WEA-C-RQMT-2770	[WEA-C-RQMT-2770] All CMAC Ack and Error messages shall be sent in HTTP 200 OK response messages.
WEA-C-RQMT-2780	[WEA-C-RQMT-2780] An HTTP 4xx Client Error or 5xx Server Error response message shall be sent to indicate a failure of the Federal Alert Gateway to retrieve the requested CAP message.
WEA-C-RQMT-2800	[WEA-C-RQMT-2800] If the Federal Alert Gateway receives an invalid or malformed acknowledgement or error response message from the CMSP Gateway, the Federal Alert Gateway should log this condition and shall not reply to the CMSP Gateway with an error response.
WEA-C-RQMT-2830	[WEA-C-RQMT-2830] If the Federal Alert Gateway does not receive an expected response message (Ack or Error) from the CMSP Gateway within the Message Response Time, the Federal Alert Gateway shall retransmit the message additional times, per the Retransmit Number.
WEA-C-RQMT-2840	[WEA-C-RQMT-2840] The Federal Alert Gateway shall declare a CMSP Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.
WEA-C-RQMT-2900	[WEA-C-RQMT-2900] If the CMSP Gateway receives an invalid or malformed acknowledgement or error response message from the Federal Alert Gateway, the CMSP Gateway should log this condition and shall not reply to the Federal Alert Gateway with an error response.
WEA-C-RQMT-2930	[WEA-C-RQMT-2930] The CMSP Gateway shall declare a Federal Alert Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.
WEA-C-RQMT-2940$_{\text{R3A}}$	[WEA-C-RQMT-2940$_{\text{R3A}}$] The Federal Alert Gateway shall be able to indicate that bypassing DBGF is requested in the CMAC alert or update.
WEA-C-RQMT-2950$_{\text{R3A}}$	[WEA-C-RQMT-2950$_{\text{R3A}}$] If DBGF bypass is requested in the CMAC alert or update and bypassing DBGF is allowed by regulatory policy, then the CMSP shall bypass DBGF procedures for the WEA.
WEA-C-RQMT-2960$_{\text{R3A}}$	[WEA-C-RQMT-2960$_{\text{R3A}}$] DBGF bypass requests shall be ignored for CMAC messages without polygon or circle elements.
WEA-C-RQMT-2964$_{\text{R3A}}$	[WEA-C-RQMT-2964$_{\text{R3A}}$] If the DBGF bypass is requested by an Alert Originator not authorized to make this request, the receiving Federal Alert Gateway shall not forward the alert to the CMSP Gateway.
WEA-C-RQMT-2965$_{\text{R3A}}$	[WEA-C-RQMT-2965$_{\text{R3A}}$] If the DBGF is requested by an Alert Originator authorized to make this request, the receiving Federal Alert Gateway shall populate the CMAC_note field accordingly.
WEA-C-RQMT-2970$_{\text{R3A}}$	[WEA-C-RQMT-2970$_{\text{R3A}}$] If DBGF bypass is requested in the CMAC alert or update and DBGF bypass is not allowed by regulatory policy, the CMSP Gateway shall ignore the DBGF bypass request.
WEA-C-RQMT-3110	[WEA-C-RQMT-3110] TCP connections shall be persistent.
WEA-C-RQMT-3400	[WEA-C-RQMT-3400] The Federal Alert Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response when the CMSP Gateway sends a CMAC message.
WEA-C-RQMT-3410	[WEA-C-RQMT-3410] The CMSP Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response.
WEA-C-RQMT-3420	[WEA-C-RQMT-3420] The Federal Alert Gateway shall reject HTTP methods other than GET with a 4xx Client Error response when the CMSP Gateway requests to retrieve a CAP message.
WEA-C-RQMT-3430	[WEA-C-RQMT-3430] The Federal Alert Gateway shall send a 4xx Client Error or 5xx Server Error response message when it is unable to retrieve the CAP message requested by a CMSP Gateway.

ATIS-0700037 Requirement Number [Ref 1]	ATIS-0700037 Requirement Text [Ref 1]
WEA-C-RQMT-3500	[WEA-C-RQMT-3500] Messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44] shall be logged and discarded.
WEA-C-RQMT-3510	[WEA-C-RQMT-3510] An Error message shall be sent in response to messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44].
WEA-C-RQMT-3600	[WEA-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.
WEA-C-RQMT-3610	[WEA-C-RQMT-3610] An Error message shall be sent in response to messages containing information that conflicts with the CMAC protocol.