TABLE 10.320(f)—CMSP PROFILE ON FEDERAL ALERT GATEWAY—Continued

Profile parameter	Parameter election	Description
If yes, list of states	CMAC Geocode for state	List can be state name or abbreviated state name.

[73 FR 43117, July 24, 2008, as amended at 78 FR 16808, Mar. 19, 2013]

§ 10.330 Provider infrastructure requirements.

This section specifies the general functions that a Participating CMS Provider is required to perform within their infrastructure. Infrastructure functions are dependent upon the capabilities of the delivery technologies implemented by a Participating CMS Provider.

(a) Distribution of Alert Messages to mobile devices.

(b) Authentication of interactions with mobile devices.

(c) Reference Points D & E. Reference Point D is the interface between a CMS Provider gateway and its infrastructure. Reference Point E is the interface between a provider's infrastructure and mobile devices including air interfaces. Reference Points D and E protocols are defined and controlled by each Participating CMS Provider.

§ 10.340 Digital television transmission towers retransmission capability.

Licensees and permittees of noncommercial educational broadcast television stations (NCE) or public broadcast television stations (to the extent such stations fall within the scope of those terms as defined in section 397(6) of the Communications Act of 1934 (47 U.S.C. 397(6))) are required to install on, or as part of, any broadcast television digital signal transmitter, equipment to enable the distribution of geographically targeted alerts by commercial mobile service providers that have elected to transmit WEA alerts. Such equipment and technologies must have the capability of allowing licensees and permittees of NCE and public broadcast television stations to receive WEA alerts from the Alert Gateway over an alternate, secure interface and then to transmit such WEA alerts to CMS Provider Gateways of participating CMS providers. This equipment must be installed no later than eighteen months from the date of receipt of funding permitted under section 606(b) of the WARN Act or 18 months from the effective date of these rules, whichever is later.

[78 FR 16808, Mar. 19, 2013]

§ 10.350 WEA Testing requirements.

This section specifies the testing that will be required, no later than the date of deployment of the WEA, of WEA components.

(a) *Required monthly tests.* Testing of the WEA from the Federal Alert Gateway to each Participating CMS Provider's infrastructure shall be conducted monthly.

(1) A Participating CMS Provider's Gateway shall support the ability to receive a required monthly test (RMT) message initiated by the Federal Alert Gateway Administrator.

(2) Participating CMS Providers shall schedule the distribution of the RMT to their WEA coverage area over a 24 hour period commencing upon receipt of the RMT at the CMS Provider Gateway. Participating CMS Providers shall determine the method to distribute the RMTs, and may schedule over the 24 hour period the delivery of RMTs over geographic subsets of their coverage area to manage traffic loads and to accommodate maintenance windows.

(3) A Participating CMS Provider may forego an RMT if the RMT is preempted by actual alert traffic or if an unforeseen condition in the CMS Provider infrastructure precludes distribution of the RMT. A Participating CMS Provider Gateway shall indicate such an unforeseen condition by a response code to the Federal Alert Gateway.

(4) The RMT shall be initiated only by the Federal Alert Gateway Administrator using a defined test message. Real event codes or alert messages shall not be used for the WEA RMT message.

(5) A Participating CMS Provider shall distribute an RMT within its

WEA coverage area within 24 hours of receipt by the CMS Provider Gateway unless pre-empted by actual alert traffic or unable due to an unforeseen condition.

(6) A Participating CMS Provider may provide mobile devices with the capability of receiving RMT messages.

(7) A Participating CMS Provider must retain an automated log of RMT messages received by the CMS Provider Gateway from the Federal Alert Gateway.

(b) *Periodic C interface testing.* In addition to the required monthly tests, a Participating CMS Provider must participate in periodic testing of the interface between the Federal Alert Gateway and its CMS Provider Gateway. This periodic interface testing is not intended to test the CMS Provider's infrastructure nor the mobile devices but rather is required to ensure the availability/viability of both gateway functions. Each CMS Provider Gateway shall send an acknowledgement to the Federal Alert Gateway upon receipt of such an interface test message. Real event codes or alert messages shall not be used for this periodic interface testing.

[73 FR 47558, Aug. 14, 2008, as amended at 78 FR 16808, Mar. 19, 2013]

Subpart D—Alert Message Requirements

§ 10.400 Classification.

A Participating CMS Provider is required to receive and transmit three classes of Alert Messages: Presidential Alert; Imminent Threat Alert; and Child Abduction Emergency/AMBER Alert.

(a) *Presidential Alert.* A Presidential Alert is an alert issued by the President of the United States or the President's authorized designee.

(b) *Imminent Threat Alert.* An Imminent Threat Alert is an alert that meets a minimum value for each of three CAP elements: Urgency, Severity, and Certainty.

(1) *Urgency.* The CAP Urgency element must be either Immediate (*i.e.*, responsive action should be taken immediately) or Expected (*i.e.*, responsive action should be taken soon, within the next hour).

(2) *Severity.* The CAP Severity element must be either Extreme (*i.e.*, an extraordinary threat to life or property) or Severe (*i.e.*, a significant threat to life or property).

(3) *Certainty.* The CAP Certainty element must be either Observed (*i.e.*, determined to have occurred or to be ongoing) or Likely (*i.e.*, has a probability of greater than 50 percent).

(c) *Child Abduction Emergency/AMBER Alert.* (1) An AMBER Alert is an alert initiated by a local government official based on the U.S. Department of Justice's five criteria that should be met before an alert is activated:

(i) Law enforcement confirms a child has been abducted;

(ii) The child is 17 years or younger;

(iii) Law enforcement believes the child is in imminent danger of serious bodily harm or death;

(iv) There is enough descriptive information about the victim and the abduction to believe an immediate broadcast alert will help; and

(v) The child's name and other data have been entered into the National Crime Information Center.

(2) There are four types of AMBER Alerts: Family Abduction; Non-family Abduction; Lost, Injured or Otherwise Missing; and Endangered Runaway.

(i) *Family Abduction.* A Family Abduction (FA) alert involves an abductor who is a family member of the abducted child such as a parent, aunt, grandfather, or stepfather.

(ii) *Nonfamily Abduction.* A Nonfamily Abduction (NFA) alert involves an abductor unrelated to the abducted child, either someone unknown to the child and/or the child's family or an acquaintance/friend of the child and/or the child's family.

(iii) *Lost, Injured, or Otherwise Missing.* A Lost, Injured, or Otherwise Missing (LIM) alert involves a case where the circumstances of the child's disappearance are unknown.

(iv) *Endangered Runaway.* An Endangered Runaway (ERU) alert involves a missing child who is believed to have run away and in imminent danger.