§ 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 non-commercial 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 CMAS alerts. Such equipment and technologies must have the capability of allowing licensees and permittees of NCE and public broadcast television stations to receive CMAS alerts from the Alert Gateway over an alternate, secure interface and then to transmit such CMAS 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.

[73 FR 47558, Aug. 14, 2008]

§ 10.350 CMAS Testing requirements.

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

(a) Required monthly tests. Testing of the CMAS 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 CMAS 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 this periodic interface testing.

(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.

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...