Mobile Service provider is required to support and perform at its CMS provider gateways.

(a) *General*. The CMS provider gateway must provide secure, redundant, and reliable connections to receive Alert Messages from the Federal alert gateway. Each CMS provider gateway must be identified by a unique IP address or domain name.

(b) *Authentication and validation*. The CMS provider gateway must authenticate interactions with the Federal alert gateway, and validate Alert Message integrity and parameters. The CMS provider gateway must provide an error message immediately to the Federal alert gateway if a validation fails.

(c) *Security*. The CMS provider gateway must support standardized IP-based security mechanisms such as a firewall, and support the defined WEA ''C'' interface and associated protocols between the Federal alert gateway and the CMS provider gateway.

(d) *Geographic targeting*. The CMS provider gateway must determine whether the provider has elected to transmit an Alert Message within a specified alert area and, if so, map the Alert Message to an associated set of transmission sites.

(e) *Message management*—(1) *Formatting*. The CMS provider gateway is not required to perform any formatting, reformatting, or translation of an Alert Message, except for transcoding a text, audio, video, or multimedia file into the format supported by mobile devices.

(2) Reception. The CMS provider gateway must support a mechanism to stop and start Alert Message deliveries from the Federal alert gateway to the CMS provider gateway.

(3) Prioritization. The CMS provider gateway must process an Alert Message on a first in-first out basis except for Presidential Alerts, which must be processed before all non-Presidential alerts.

(4) Distribution. A Participating CMS provider must deploy one or more CMS provider gateways to support distribution of Alert Messages and to manage Alert Message traffic.

(5) Retransmission. The CMS provider gateway must manage and execute Alert Message retransmission, and support a mechanism to manage congestion within the CMS provider's infrastructure.

(f) *CMS provider profile*. The CMS provider gateway will provide profile information on the CMS provider for the Federal alert gateway to maintain at the Federal alert gateway. This profile information must be provided by an authorized CMS provider representative to the Federal alert gateway administrator. The profile information must include the data listed in Table 10.320(f) and must comply with the following procedures:

(1) The information must be provided 30 days in advance of the date when the CMS provider begins to transmit WEA alerts.

(2) Updates of any CMS provider profiles must be provided in writing at least 30 days in advance of the effective change date.

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

Profile parameter	Parameter election	Description
CMSP Name		Unique identification of CMSP.
CMSP gateway Address	IP address or Domain Name.	
	Alternate IP address	Optional and subject to implementation.
Geo-Location Filtering	<yes/no>	If ''yes'' the only CMAM issued in the listed states will be sent to the CMSP gateway.
		If ''no'', all CMAM will be sent to the CMSP gateway.
If yes, list of states	CMAC Geocode for state	List can be state name or abbreviated state name.

(g) *Alert logging*. The CMS provider gateway must perform the following functions:

(1) *Logging requirements*. Log the CMAC attributes of all Alert Messages received at the CMS Provider Alert Gateway, including time stamps that verify when the message is received,

and when it is retransmitted or rejected by the Participating CMS Provider Alert Gateway. If an Alert Message is rejected, a Participating CMS Provider is required to log the specific error code generated by the rejection.

(2) *Maintenance of logs.* Participating CMS Providers are required to maintain a log of all active and cancelled Alert Messages for at least 12 months after receipt of such alert or cancellation.

(3) *Availability of logs.* Participating CMS Providers are required to make their alert logs available to the Commission and FEMA upon request. Participating CMS Providers are also required to make alert logs available to emergency management agencies that offer confidentiality protection at least equal to that provided by the federal Freedom of Information Act (FOIA) upon request, but only insofar as those logs pertain to Alert Messages initiated by that emergency management agency.

[73 FR 43117, July 24, 2008, as amended at 78 FR 16808, Mar. 19, 2013; 81 FR 75725, Nov. 1, 2016]

§ 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 and proficiency training requirements.

This section specifies the testing that is required of Participating CMS Providers.

(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