SUPPORTING STATEMENT

A. Justification:

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection.

The information collection is a necessary element of Wireless Emergency Alerts (WEA), a mechanism under which Commercial Mobile Service (CMS) providers may elect to transmit emergency alerts to the public. As required by Congress in the Warning Alert and Response Network (WARN) Act, the Commission completed rulemaking proceedings to, *inter alia*: (1) adopt technical requirements necessary to enable CMS alerting capability for CMS providers that voluntarily elect to transmit emergency alerts; (2) provide an administrative process for CMS licensees to elect to transmit WEA alerts to subscribers, and (3) require technical testing for CMS providers that elect to transmit WEA alerts.

On December 14, 2007, the Commission adopted and released a Notice of Proposed Rulemaking (NPRM) – one of a series of rulemakings to establish WEA as required by the WARN Act. Among other sections of the WARN Act, the NPRM sought comment on section 602(f) of the WARN Act, which requires that the Commission "shall require by regulation technical testing for commercial mobile service providers that elect to transmit emergency alerts and for the devices and equipment used by such providers for transmitting such alerts." In the NPRM, the Commission sought comment on what type of testing regime it should require. The Commission noted that the Commercial Mobile Service Alert Advisory Committee (CMSAAC) recommended that, in order to assure the reliability and performance of this new system, certain procedures for logging WEA alerts at the Alert Gateway and for testing the system at the Alert Gateway and on an end-to-end basis should be implemented. The Commission sought comment on these recommended procedures and asked whether they satisfied the requirements of section 602(f) of the WARN Act. The Commission also sought comment on whether there should be some form of testing of WEA in which WEA sends test messages to the mobile device and the subscriber. The Commission asked how subscribers should be made aware of such tests if testing were to involve subscribers.

Commenters generally supported the testing regime recommended by the CMSAAC, as well as some sort of logging of results as a part of the ultimate testing process. In *ex parte* comments submitted on May 23, 2008, CTIA submitted a proposal for testing requirements that were developed together with Alltel, AT&T, Sprint Nextel, T-Mobile and Verizon Wireless. Under CTIA's proposal, participating CMS providers would participate in monthly testing of the WEA system. The monthly test would be initiated by the federally-administered Alert Gateway at a set day and time and would be distributed through the commercial mobile service provider infrastructure and by participating CMS providers over their networks. Upon receipt of the test

message, participating CMS providers would have a 24-hour window to distribute the test message in their WEA coverage areas in a manner that avoids congestion or other adverse effects on their networks. Under CTIA's proposal, mobile devices supporting WEA would not be required to support reception of the required monthly test and participating CMS providers would not be required to deliver required monthly tests to subscriber handsets, but a participating CMS provider may provide mobile devices with the capability for receiving these tests. CTIA's testing proposal also features regular testing from the "C" interface to ensure the ability of the Federal Alert Gateway to communicate with the CMS Provider Gateway.

The Commission agreed with the CMSAAC and most commenters that periodic testing of all components of WEA, including the CMS provider's components would serve the public interest and is consistent with the WARN Act. Further, the Commission adopted the procedure recommended by CTIA and several CMS providers.

In the Second Report and Order, FCC 08-164, the Commission adopted rules requiring each participating CMS provider to participate in monthly testing of WEA message delivery from the Federal Alert Gateway to the CMS provider's infrastructure. CMS Provider Gateways must support the ability to receive required monthly test messages initiated by the Federal Alert Gateway Administrator. CMS providers must receive these required monthly test messages and must also distribute those test messages to their WEA coverage area within 24 hours of receipt of the test message by the CMS Provider Gateway. CMS providers may determine how this delivery will be accomplished and may stagger the delivery of the required monthly test message over time and over geographic subsets of their coverage area to manage the traffic loads and accommodate maintenance windows. A participating CMS provider may forego these monthly tests if pre-empted by actual alert traffic or in the event of unforeseen conditions in the CMS provider's infrastructure that preclude distribution of the monthly test message, but shall indicate this unforeseen condition by a response code to the Federal Alert Gateway.

Participating CMS Providers must keep an automated log of Required Monthly Test messages received by the CMS Provider Gateway from the Federal Alert Gateway. WEA required monthly tests will be initiated only by the Federal Alert Gateway Administrator using a defined test message; real event codes and alert messages may not be used for test messages. A Participating CMS Provider may provide mobile devices with the capability of receiving monthly test message. Although the Commission did not require Participating CMS Providers to provide mobile devices that support reception of the required monthly test, it stated that CMS providers that choose not to make the required monthly test available to subscribers must find alternate methods of ensuring that subscriber handsets will be able to receive WEA alert messages.

The Commission also adopted CTIA's recommendation that, in addition to the Required Monthly Test, there should be periodic testing of the interface between the Federal Alert Gateway and each CMS Provider Gateway to ensure the availability and viability of both

gateway functions. Under the Commission's rules, CMS Provider Gateways must send an acknowledgement to the Federal Alert Gateway upon receipt of these interface test messages.

CMS providers must comply with these testing requirements no later than the date of deployment of WEA, which is the date that WEA development is complete, and the WEA is functional and capable of providing alerts to the public.

Present Information Collection Requirements:

Consistent with our statutory authority under WARN Act Section 602(f), and in light of developments in the WEA system and the evolving public safety needs of communities, we established logging requirements for WEA messages consistent with the WEA Trust Model established by the CMSAAC. We also established requirements and procedures to facilitate state and local WEA testing and proficiency training, required testing of the broadcast-based backup to the C-interface, and required Participating CMS Providers to disclose information about their approach to geo-targeting.

We required Participating CMS Providers to log and maintain basic Alert Message attributes, and to make those logs available upon request to the Commission and FEMA, and to emergency management agencies that offer confidentiality protection at least equal to that provided by the federal Freedom of Information Act (FOIA) insofar as those logs pertain to alerts initiated by that emergency management agency. Specifically, Participating CMS Providers are required to provide a mechanism to log the CMAC attributes of all Alert Messages received at the CMS Provider Alert Gateway, along with 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 is rejected, a Participating CMS Provider is required to log the specific error code generated by the rejection. 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 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 FOIA upon request, but only insofar as those logs pertain to alerts initiated by that emergency management agency. We encouraged, but did not require, Participating CMS Providers to work with alert origination software vendors to automate transmission of alert log data to emergency managers' alert origination software.

We improved WEA testing by requiring Participating CMS Providers to ensure their systems support the receipt of end-to-end "State/Local WEA Tests" initiated by state and local alert originators and processed by the Federal Alert Gateway Administrator, and distributed to the desired test area in a manner consistent with our WEA geo-targeting requirement. We require that Participating CMS Providers provide their subscribers with the option to opt-in to receiving State/Local WEA Tests. Finally, we adopted requirements for testing the public broadcast-based backup to the C-interface consistent with our requirements for periodic testing of the C-interface itself.

We also required that, upon request from an emergency management agency, a Participating CMS Provider will disclose information regarding its capabilities for geo-targeting Alert

Messages (*e.g.*, whether they are using network-based technology to "best approximate" the target area, or whether they are using device-based geo-fencing). A Participating CMS Provider is only required to disclose this information to an emergency management agency insofar as it would pertain to Alert Messages initiated by that emergency management agency, and only so long as the emergency management agency offers confidentiality protection at least equal to that provided by the federal FOIA.

Statutory authority for this information collection is contained in 47 U.S.C. sections 151, 152, 154(i) and (o), 301, 301(r), 303(v), 307, 309, 335, 403, 544(g), 606 and 615 of the Communications Act of 1934, as amended, as well as by sections 602(a), (b), (c), (f), 603, 604 and 606 of the WARN Act.

This information collection does not affect individuals or households; thus there are no impacts under the Privacy Act.

2. Indicate how, by whom and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

This information collection will be and has been used by the Commission to satisfy the statutory requirement of the WARN Act that the Commission "shall require by regulation technical testing for commercial mobile service providers that elect to transmit emergency alerts and for the devices and equipment used by such providers for transmitting such alerts." Our logging requirements and our geo-targeting disclosure requirement are anticipated to bring WEA further into alignment with the WEA Trust Model established by the CMSAAC, and moreover, to enhance system reliability, security and resiliency. The availability of alert logs and information about geo-targeting has potential to increase emergency managers' confidence that WEA will work as intended when needed. This increased confidence in system availability will encourage emergency managers that do not currently use WEA to become authorized. Alert logs are also necessary to establish a baseline for system integrity against which future iterations of WEA can be evaluated. Without records that can be used to describe the quality of system integrity, and the most common causes of message transmission failure, it will be difficult to evaluate how any changes to WEA that we may adopt subsequent to this *Report and Order* affect system integrity.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g. permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

Much of the logging and sending acknowledgement of receipt of alerts is done automatically, i.e., via computer software and electronic transmission. In order to minimize burden on participants, much of the testing, acknowledgment, and logging process is automated. We anticipate that this will continue to be the case for our logging requirements.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in item 2 above.

These requirements are unique to WEA and are not duplicated elsewhere.

5. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden.

These requirements have been carefully designed to minimize the time required by the information collections as well as the amount of data needed for the Commission to achieve its objectives as stated in item 1 above. Further, we allow non-nationwide Participating CMS Providers additional time within which to comply with our alert logging requirements and make appropriate exceptions for Participating CMS Providers' provision of the capability to receive State/Local WEA Tests on legacy devices.

6. Describe the consequences to a Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

Failure to conduct testing of the WEA as required by the WARN Act would constitute a violation of a Congressional mandate to the Commission. Further, the ability of the Commission to develop and deploy an effective WEA would be jeopardized if the Commission is unable to require that the participants test the system and log information about the system in an effective manner. Emergency management agencies' ability to utilize WEA would be dramatically reduced if they could not find out how accurately their alerts were being geo-targeted.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner inconsistent with the criteria listed in the supporting statement.

The information collection requirements contained in the supporting statement are consistent with the guidelines in 5 CFR § 1320.

8. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information prior to submission to OMB. (See Attachment).

-Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

The Commission published a 60-day notice in the Federal Register on November 14, 2019 (84 FR 61901) seeking comments on the information collection requirements contained in the supporting statement. No comments have been received to date.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No payment or gift to respondents has been or will be made with this information collection.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

Participating CMS Providers are only required to disclose alert log data and information about geo-targeting to emergency management agencies insofar as those agencies offer confidentiality protection at least equal to that provided by the federal FOIA.

11. Provide additional justification for any questions of a sensitive nature.

There are currently no questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should: indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance.

Total Number of Respondents: 76.

Frequency of response: Monthly and on occasion reporting requirements and recordkeeping requirement.

Total Number of Responses Annually: 429,020

(4,851 alerts logged per year + 12 required monthly tests logged per year) + 782 responses to requests for alert log data or information about geo-targeting = 5,645 responses per year x 76 Participating CMS Providers = 429,020

Total Annual Burden: 119,121 hours (rounded up)

(0.000694 hours [2.5 seconds] x 4,851 Alert Message logs per year) + (0.000694 hours x 12 Required Monthly Test logs per year) = 3.375 hours x 76 Participating CMS Providers = 257 hours (rounded up)

2 hours x 782 information requests per year = 1,564 hours x 76 Participating CMS Providers = 118,864 hours

Method of estimation of burden: The burden estimate for this information collection is based solely on our estimate of the actual time needed for data entry and submission. In making our time estimate, we have taken into account similar requirements that the Commission required in its Part 11 Emergency Alert System testing rules. In sum, we estimate the total annual time needed to satisfy this information collection to be no more than 119,121 hours annually.

To estimate the hourly wage of a full-time employee who will be maintaining alert log data, we use the most recent salary table for GS 13 Step 5 in locality pay area of Washington-Baltimore-Arlington, DC-MD-VA-WV-PA, or $116,353 per year which is $55.75 per hour. We add 50% of this wage, or $27.88 for benefits, for a compensation estimate of $83.63 per hour.

To estimate the hourly wage of a full-time employee who will be responding to requests for alert log data and information about geo-targeting, we use the crowdsourced data on the average hourly compensation of a clerical employee, $14.28 per hour. We then add 50% to that figure, or $7.14 per hour, to account for employee benefits, for a total of $21.42 per hour.

To estimate the total number of respondents, we reference the docket in which Participating CMS Providers have filed their elections to participate in WEA.

0.000694 hours x salary of the person responsible for compiling logs ($83.63) x total number of Alert Messages and Required Monthly Tests expected per year (4,851 + 12) = $282.24 x 76 Participating CMS Providers = $21,450.

2 hours x salary of the person responsible for compiling reports ($21.42) x total number of requests for alert log data and information about geo-targeting (782) = $33,500 x 76 Participating CMS Providers = $2,546,066.

Total Annual In-house Costs to the Respondent: $2,567,516

13. Provide estimate for the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in items 12 and 14).

There are no outside costs to the respondents for this collection of information.

14. Provide estimates of annualized costs to the Federal government. Also provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expenses that would not have been incurred without this collection of information.

There are no costs to the Commission beyond what we consider to be part of the FCC's normal operating costs.

15. Explain the reasons for any program changes or adjustments to this information collection.

Since the last submission to OMB, Commission is reporting adjustments/decreases to this information collection. The number of CMS providers participating in WEA has decreased by 4;

the total annual responses decreased by 22,580 and the total annual burden hours decreased by 6,269. This is due to wireless providers' modifications of their participation status, and due to the Commission's adoption of a methodology for counting participating entities that better aligns with the filings in the WEA election docket, PS 08-146 and the Master CMAS Registry. There are no program changes to this collection.

16. For collections of information whose results will be published, outline plans for tabulation and publication.

The FCC does not plan to publish the results of this information collection.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

The Commission does not intend to seek approval not to display the OMB expiration date of the information collection. The Commission publishes in 47 CFR 0.408, a list of all OMB-approved information collections displaying their OMB Control Number(s), titles, and OMB expiration date(s).

18. Explain any exceptions to the Certification Statement identified in Item 19, "Certification of Paperwork Reduction Act Submissions."

When the 60-day notice was published in the Federal Register on November 14, 2019 (84 FR 61901), the Commission inadvertently reported the total burden hours as 119,021 opposed to 119,121 total hours.

There are no other exceptions to the Certification Statement.

B. Collections of Information Employment Statistical Methods:

This information collection does not employ any statistical methods.