



Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

## **FCC White Paper**

---

The Capacity of the Integrated Public  
Alert and Warning System to Deliver  
Sensor-Based  
Earthquake Early Warnings:  
An Engineering Analysis

**Public Safety and Homeland  
Security Bureau**

**December 5, 2016**

---

# The Capacity of the Integrated Public Alert and Warning System to Deliver Sensor-Based Earthquake Early Warnings: An Engineering Analysis

The Public Safety and Homeland Security Bureau of the Federal Communications Commission has performed a technical analysis of the journey of an earthquake early warning (EEW) alert, starting with the transmission of the alert from the earthquake alert center (EAC) and ending with receipt by the public from one of the primary Integrated Public Alert and Warning System (IPAWS) alerting platforms: the Wireless Emergency Alerts (WEA) system, the Emergency Alert System (EAS), or the various Internet-based services that obtain alerts from the IPAWS “public feed.” This analysis identifies the measures necessary to deliver EEW alerts through IPAWS within three seconds.

This analysis shows:

- Distribution of EEW alerts through IPAWS to the public within three seconds appears achievable over WEA, provided that certain technical modifications are made to, and certain operational parameters are established for, IPAWS and commercial mobile service provider networks.
- Distribution of EEW alerts through IPAWS to the public within three seconds is not reasonably achievable over the EAS as it is currently configured. Achieving three-second EEW alert delivery over the EAS would require alteration to the EAS architecture. Adding EEW to future EAS design objectives would be appropriate, but care should be taken to ensure that the simplicity and robustness of the current system endures.
- Distribution of EEW alerts through IPAWS to the public within three seconds appears achievable over Internet-based services interconnected with IPAWS (via the IPAWS Public Feed), provided that the output connections of IPAWS are modified to enable the fastest, technically feasible method for disseminating EEW alerts from IPAWS to such services.
- EEW alerts could be distributed directly from the EAC to alerting platforms by importing into the EAC certain functions currently performed within IPAWS. Such an alternative approach may offer time expenditure savings and provide other benefits, such as increased flexibility and scalability, as compared to an IPAWS-centric alerting model.

David G. Simpson<sup>1</sup>  
Rear Admiral, USN (Ret.)  
Chief, Public Safety and Homeland Security Bureau

---

<sup>1</sup> The authors of this paper are Gregory M. Cooke, Austin Randazzo, Rasoul Safavian, Behzad Ghaffari, Steven Carpenter and Yoon Chang.

## TABLE OF CONTENTS

<u>1.</u>	<u>INTRODUCTION</u> .....	4
<u>2.</u>	<u>KEY FINDINGS</u> .....	5
<u>3.</u>	<u>BACKGROUND</u> .....	6
<u>4.</u>	<u>ANALYSES AND KEY FINDINGS</u> .....	7
<u>4.1.</u>	<u>Earthquake Alert Center</u> .....	8
<u>4.1.1.</u>	<u>Optimizing the EAC for EEW Alerts</u> .....	9
<u>4.2.</u>	<u>IPAWS Analysis Summary</u> .....	9
<u>4.2.1.</u>	<u>Optimizing the Current IPAWS for EEW Alerts</u> .....	10
<u>4.2.2.</u>	<u>EEW Alerting in an Alternative EEW System</u> .....	10
<u>4.3.</u>	<u>Alert Dissemination Channels</u> .....	12
<u>4.3.1.</u>	<u>Wireless Emergency Alerts (WEA)</u> .....	12
<u>4.3.1.1.</u>	<u>Optimizing WEA for EEW Alerts</u> .....	13
<u>4.3.1.2.</u>	<u>Optimizing UMTS Using the Earthquake and Tsunami Warning System (ETWS)</u> .....	14
<u>4.3.2.</u>	<u>Emergency Alert System</u> .....	14
<u>4.3.2.1.</u>	<u>Optimizing EAS for EEW Alerts</u> .....	16
<u>4.3.3.</u>	<u>IPAWS Public (All-Hazard) Feed</u> .....	17
<u>4.3.4.</u>	<u>General Cybersecurity Concerns</u> .....	18
<u>5.</u>	<u>CONCLUSION</u> .....	18

- Appendix A: List of Commenting Parties**
- Appendix B: Functions and Latencies in the Earthquake Alert Center**
- Appendix C: Functions and Latencies in the Integrated Public Alert and Warning System**
- Appendix D: Functions and Latencies in Wireless Emergency Alerts**
- Appendix E: Earthquake and Tsunami Warning System (ETWS)**
- Appendix F: Functions and Latencies in the Emergency Alert System**

## 1. INTRODUCTION

Promoting safety of life and property is an essential component of the Federal Communication Commission's (Commission's) core mission.<sup>2</sup> To this end, the Commission is committed to further improving the alerting systems under its jurisdiction by integrating effective and timely earthquake alerts within the ambit of those systems.<sup>3</sup> Earthquakes can have devastating costs to life and property. For example, the 6.9 magnitude "Loma Prieta" earthquake in 1989 that struck the Santa Cruz Mountains in 1989 caused 63 deaths, 3,757 injuries, and \$6 billion in property damage.<sup>4</sup> Timely, effective emergency alerts may potentially mitigate some of the damage attributed to earthquakes annually, and efforts have been underway to develop earthquake early warning (EEW) systems both here in the U.S. and abroad for some time. In the U.S., the United States Geological Survey (USGS) and its partners are developing an EEW system called the ShakeAlert system, covering the West Coast of the U.S.<sup>5</sup> Overseas EEW development efforts include Japan's Earthquake and Tsunami Warning System, which has been deployed since 2007. Japan's EEW system during the 9.0 magnitude earthquake in 2011 provided early earthquake warnings to the public between 10 and 30 seconds prior to the arrival of the first tremors.<sup>6</sup> An EEW system similar to Japan's has been deployed in Chile, which proved effective in expediting evacuations and mitigating loss of lives associated with the 8.3 magnitude earthquake that occurred near Chile's capitol in 2015.<sup>7</sup> Smaller EEW systems that operate on the same P wave detection principles but are installed on a building-by-building basis have been deployed in several countries around the world.<sup>8</sup>

This white paper provides summaries of the technical analyses and optimization measures that apply to each discrete section of the journey of an EEW alert, starting with (i) the transmission of the EEW alert

---

<sup>2</sup> See 47 USC § 151.

<sup>3</sup> See, e.g., *Wireless Emergency Alerts*, PS Docket No. 15-91, Notice of Proposed Rulemaking, 30 FCC Rcd 13781 (2015); *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, Wireless Emergency Alerts*, PS Docket Nos. 15-94, 15-91, Notice of Proposed Rulemaking, 31 FCC Rcd 594 (2016).

<sup>4</sup> United States Geological Survey, *Historic Earthquakes* (Apr. 6, 2016), [http://earthquake.usgs.gov/earthquakes/states/events/1989\\_10\\_18.php](http://earthquake.usgs.gov/earthquakes/states/events/1989_10_18.php). In the conterminous United States a total of 592 earthquakes with magnitudes of 4.0 and higher. See United States Geological Survey, *Search Earthquake Archives*, <http://earthquake.usgs.gov/earthquakes/search/> (last visited Aug. 25, 2016) (providing number of earthquakes when searching for all earthquakes with magnitudes of at least 4.0, 4.5, and 5.0 in the conterminous United States between midnight on January 1, 2011, and 11:59:59 pm on December 31, 2015).

<sup>5</sup> See D.D. Given, et al., *Technical Implementation Plan for the ShakeAlert Production System - An Earthquake Early Warning System for the Western United States*, United States Geological Survey 12 (2014) at 4. USGS is working with various regional institutions, including Caltech, UC Berkeley, the California Geological Survey, and the California Office of Emergency Services, and utilizing regional seismic networks in California and the Pacific Northwest. See *id.*

<sup>6</sup> See, e.g., Jean Kumagi, IEEE Spectrum, *In Japan Earthquake, Early Warnings Helped* (Mar. 15, 2011), <http://spectrum.ieee.org/tech-talk/computing/networks/japans-earthquake-earlywarning-system-worked>.

<sup>7</sup> See, e.g., Cat DiStasio, inhabitat, *Cell phone warning system keeps Chile safe through 8.3 magnitude earthquake* (Sept. 17, 2015), <http://inhabitat.com/cell-phone-warning-system-keeps-chile-safe-through-8-3-magnitude-earthquake/>.

<sup>8</sup> See, e.g., summary of ongoing deployment projects of early earthquake warning systems manufactured by secty electronics, <https://www.secty-electronics.de/en/projects/overview-about-projects-and-references.html>. P-waves, or primary waves, travel at high speeds outward from the earthquake source, but rarely cause damage. S-waves, or secondary waves, travel more slowly, lag behind P-waves, and result in more intense ground shaking that causes damage. See D.D. Given, et al., *Technical Implementation Plan for the ShakeAlert Production System - An Earthquake Early Warning System for the Western United States*, United States Geological Survey 12 (2014) at 3.

from the earthquake alert center (EAC), which generates the EEW alert, to the Integrated Public Alert and Warning System (IPAWS); then (ii) through the processing of the EEW alert within IPAWS; then (iii) to the primary IPAWS alerting platforms: (a) the Wireless Emergency Alerts (WEA) system,<sup>9</sup> (b) the Emergency Alert System (EAS), and (c) the various Internet-based services that obtain alerts from the IPAWS “public feed.”<sup>10</sup> These summaries identify measures necessary to deliver EEW alerts through IPAWS within three seconds. Full technical analyses covering EEW alert processing in IPAWS, WEA, the EAS and IPAWS’s Internet-based “Public Feed” services are provided in the appendices.

## 2. KEY FINDINGS

The following is a list of specific key findings of this white paper.

### IPAWS

- Certain optimization measures involving the connection of the EEW into and from IPAWS,<sup>11</sup> as well as the IPAWS internal processing of the EEW alert can reduce the overall EAC-to-alerting platform (WEA, EAS and IPAWS Public Feed) time expenditure to less than one second.

### WEA

- Distribution of EEW alerts through IPAWS to the public within three seconds appears achievable over WEA and 4G/LTE networks, provided that certain technical modifications are made to, and certain operational parameters are established for, IPAWS (such as modification of input and output connections, and internal alert processing routines), and commercial mobile service provider (CMSP) networks (such as optimization of operational parameters, such as Paging DRX cycle time values and SIB-12 periodicity).<sup>12</sup>

---

<sup>9</sup> WEA was formerly known as the Commercial Mobile Alert System (CMAS). In 2013, the Public Safety and Homeland Security Bureau amended its Part 10 rules to change the name “Commercial Mobile Alert System” (CMAS) to “Wireless Emergency Alert” (WEA). See *Commercial Mobile Alert System*, PS Docket No. 07-287, Order, 28 FCC Rcd 1460 (PSHSB 2013).

<sup>10</sup> This white paper does not include the time that the EAC requires to generate the EEW as part of its three second analysis. The *EEW Public Notice* asked where our examination of transmission and processing times should start and, in particular, whether alert sensing, detection and alert message creation times should be considered as part of the three second overall latency analyses. See *EEW Public Notice*, 31 FCC Rcd at 3463. The United States Geological Survey (USGS) responded that “alert delivery [should] be measured starting from the time the alert is sent by the USGS to IPAWS system via the A-interface and at every step until it is received by end users.” USGS Comments at 2. Although Seismic Warning Systems, Inc., argues that “... latency must be measured from the point of earthquake detection [sensing] to final delivery to the intended recipient,” see *Seismic Warning Systems Comments* at 5, we agree with USGS. The actual structure of an EEW is being still being determined by USGS and others. There are numerous factors that contribute to the process of creating the EEW, such as sensor density, transmission technologies, the number of sensor inputs and detection algorithms used, and the preset false alarm and miss probabilities, which in combination make it impossible at this early stage to assign a reliable time value to the EEW’s formation. Accordingly, the starting point of this white paper’s analysis will be from the moment the EEW alert is ready to be transmitted from the EEW alert originator – *i.e.*, the earthquake alert center (EAC) – to IPAWS. That being said, of course, the actual time that the EAC takes to create an EEW must be factored into the public safety value of EEWs.

<sup>11</sup> The term “IPAWS” is used throughout the white paper generically to refer specifically to IPAWS-OPEN, which collectively represents the IPAWS Aggregator and IPAWS Gateway.

<sup>12</sup> DRX stands for Discontinuous Reception. The end user device or user equipment (UE), when in idle mode, goes into sleep to save battery life time and wakes up for a short period of time (called “On” time) during designated

- In anticipation of future 5G network deployments, EEW-specific requirements should be built-in to the technical standards work of the 3GPP,<sup>13</sup> which is working on standards for the next generation (5G) wireless networks, including provisions for “Critical Communications” that would provide low latency, and high availability and reliability.<sup>14</sup>

## **EAS**

- Distribution of EEW alerts through IPAWS to the public within three seconds is not reasonably achievable over the EAS as it is currently configured.
- Achieving three-second EEW alert delivery over the EAS would require significant alteration to the EAS architecture, at substantial cost, that could interfere with the simplicity and robustness that the current system offers and thus may not represent the best allocation of limited resources.

## **IPAWS Public Feed**

- Distribution of EEW alerts through IPAWS to the public within three seconds appears achievable over Internet-based services interconnected with IPAWS (via the IPAWS Public Feed), provided that the output connections of IPAWS are modified to enable the fastest, technically feasible method for disseminating EEW alerts from IPAWS to such services.

## **Alternative Alerting and Warning Methods**

- EEW alerts could be distributed directly from the EAC to WEA (via the CMSP gateways) and/or other alerting platforms that may become available over time (thus, bypassing IPAWS altogether) by importing into the EAC certain functions currently performed within IPAWS. Such an alternative approach may offer time expenditure savings and provide other benefits, such as increased flexibility and scalability, as compared to an IPAWS-centric alerting model.

## **3. BACKGROUND**

The white paper is based on comments received in response to a Public Notice (*EEW Public Notice*) filed in PS Docket No. 16-32.<sup>15</sup> The Bureau received input from commercial mobile wireless service industry entities, EAS equipment manufacturers, trade organizations, entities endorsing particular EEW

---

times to check if it is paged or if there are any new system change information addressed to the UE. If it is not paged and there are no system information change messages, it goes back to sleep (“Off” time). A complete cycle is called the Paging DRX Cycle. SIB stands for the System Information Block type. SIB-12 Periodicity is the frequency at which SIB-12 messages are transmitted. SIB-12 periodicity can be set at 80 ms 160 ms 320 ms, 640 ms, 1.28 s, 2.56 s or 5.12 s.

<sup>13</sup> The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. See <http://www.3gpp.org/about-3gpp>.

<sup>14</sup> See 3GPP TR 22.891 V14.1.0 (2016-06). Also, 3GPP is planning to consolidate all the requirements into a single Stage 1 Technical Specification (TS 22.261). The draft version of this document is expected for December 2016 release, and approved version is planned for March 2017 release.

<sup>15</sup> *Public Safety and Homeland Security Bureau Seeks Comment on Ways to Facilitate Earthquake-Related Emergency Alerts*, Public Notice, 31 FCC Rcd 3459 (PSHSB 2016) (*EEW Public Notice*).

approaches, and a few individuals.<sup>16</sup> The Bureau also held *ex parte* meetings with eleven entities, including equipment manufacturers and service providers.<sup>17</sup> The Bureau analyzed the processing times associated with IPAWS, WEA, EAS, and other alerting platforms, using data from filed comments, outreach to stakeholders, public documents, and relevant technical standards.

#### 4. ANALYSES AND KEY FINDINGS

IPAWS is the nation’s federal alert and warning system, and is administered by the Federal Emergency Management Agency (FEMA).<sup>18</sup> IPAWS performs two main functions: (1) IPAWS performs an alert aggregation function, by which it receives, authenticates and aggregates alert messages that have been formatted in the Common Alerting Protocol (CAP)<sup>19</sup> from state, local, tribal and territorial alerting entities; and (2) IPAWS performs a “gateway” function by which it distributes the alerts over its primary IPAWS alerting platforms, the EAS and WEA, as well as a public “all hazards” Internet feed that is available to services such as Facebook.<sup>20</sup>

As depicted in Figure 1 below, the EEW alert’s journey from the EAC to the public over IPAWS is composed of several discreet sections, each representing a specific function with its own unique timeframe. For example, processing the EEW alert within IPAWS represents one discreet section of the alert journey, as does processing the alert within the CMSP network. We examine each section in turn, noting how the time expenditures for each may be minimized via optimization measures to produce the lowest overall end-to-end alert delivery timeframe. Specifically, this white paper examines the transmission of the EEW alert from the EAC to IPAWS (T1 in Figure 1); the processing of the EEW alert within IPAWS (P1 in Figure 1); and then delivery to and processing within the alerting platforms of WEA, the EAS, and delivery through the IPAWS public feed to various Internet-based services (this encompasses T2 and the various overall processing timelines associated with each platform). Full technical analyses of each leg in this journey are provided in the appendices.

---

<sup>16</sup> See Appendix A.

<sup>17</sup> See *id.*

<sup>18</sup> See INTEGRATED PUBLIC ALERT & WARNING SYSTEM, <https://www.fema.gov/integrated-public-alert-warning-system> (last visited Aug. 25, 2016).

<sup>19</sup> As detailed in Appendix B, CAP is a standardized and diversified Extensible Markup Language (XML)-based message format used for relaying alert information that can include many type of information, including audio, video or data files; images; multilingual translations of alerts; and links providing more detailed information.

<sup>20</sup> See FEMA, Integrated Public Alert & Warning System Open Platform for Emergency Networks, <https://www.fema.gov/integrated-public-alert-warning-system-open-platform-emergency-networks> (last visited Aug. 25, 2016). IPAWS-OPEN can distribute CAP-formatted alerts to National Weather Service dissemination systems, such as National Oceanic and Atmospheric Administration (NOAA) Weather Radio and HazCollect, as well as IPAWS-configured state or locally owned and operated warning systems, such as sirens, highway signs, or emergency telephone notification systems. See *id.*

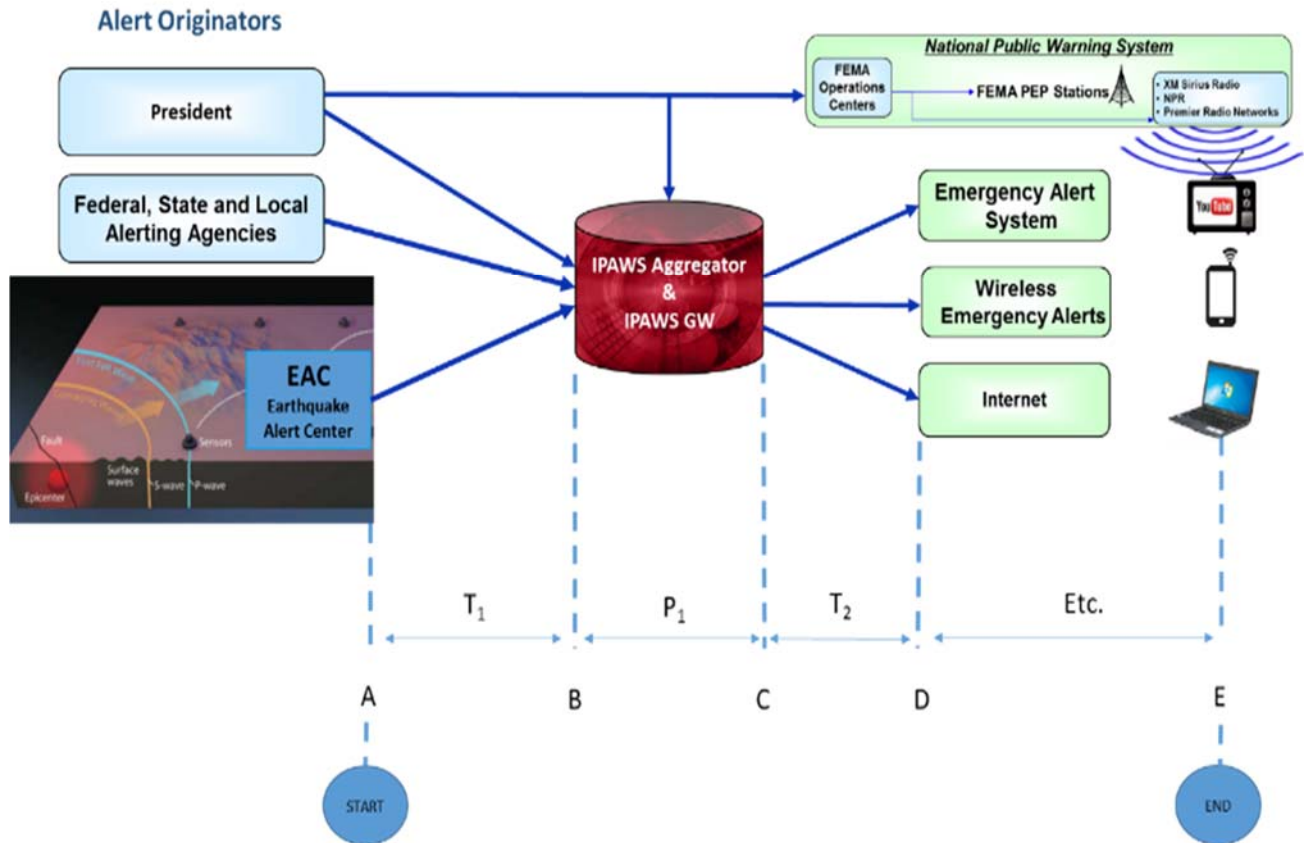


Figure 1 – End-to-End Alert Delivery via IPAWS

(“T” stands for the Transmission time and “P” for the Processing time)

#### 4.1. Earthquake Alert Center

*Key Finding:* The time expenditure for transmitting the EEW alert from the EAC to IPAWS can be reduced from a typical public Internet connection timeframe of around 200 milliseconds (ms) to 50 ms by utilizing a permanent connection, such as a nailed-up Virtual Private Network (VPN) connection or other persistent connection, between the EAC and IPAWS.<sup>21</sup>

*Basic EAC functions.* The EAC takes seismic data generated by ground sensors installed near active faults and, using algorithms to identify and characterize the data, calculates the likely intensity of ground shaking and direction of seismic waves likely to result.<sup>22</sup> Based on these calculations, the EAC then creates the EEW in the CAP format, and transmits the alert to the public via systems such as IPAWS.

<sup>21</sup> The transmission time in a “nailed-up” VPN (*i.e.*, a permanent connection) would be the time for physical transmission between two points. As explained in Appendix B, the physical transmission time should not exceed 50 ms. See *infra* note 59.

<sup>22</sup> See n. 8, *supra*, and surrounding text for a more detailed discussion of how this algorithm is generated from P-waves.



#### 4.1.1. Optimizing the EAC for EEW Alerts

We note that most alert originators are connected to the IPAWS via HTTPS. The typical setup and transmission time for an alert from the EAC to IPAWS using standard public Internet connections is approximately 200 ms.<sup>23</sup> Approximately 150 ms of this 200 ms timeframe involves establishing a secure link with IPAWS, using the public Internet Secure HTTP (HTTPS)/Transport Layer Security (TLS) protocol. There are several ways to minimize this time expenditure. One solution would be to have the EAC start the persistent HTTPS connection as soon as the first EEW alert sensor data is received at the EAC for processing. While the EAC is processing sensor data, and perhaps before any final calculations are made, the persistent HTTPS connection can be established. Alternatively, a VPN or other “always on” connection with IPAWS can be established.<sup>24</sup> To further facilitate reductions in latency and increase resiliency, the EAC function should be distributed across a cloud-based storage system, with redundant virtual servers, load balanced and positioned in close proximity to deployed ground sensor networks and the intended EEW alert recipients.

#### 4.2. IPAWS Analysis Summary

*Key Finding:* The time expenditure associated with internal processing by IPAWS of EEW alerts bound for delivery over WEA, EAS or the IPAWS Public Feed can be reduced from an average of 1.667 seconds to 900 ms or less by streamlining both the EEW CAP alert contents and the alert processing routines currently employed within IPAWS for typical WEA alerts.

*Basic IPAWS functions.* As discussed above, IPAWS receives, authenticates and aggregates alert messages that have been formatted in CAP from state, local, tribal and territorial alerting entities, and redistributes them to EAS, WEA and/or Internet-based services connected with the IPAWS Public Feed. Several factors influence the total time expended on processing any given alert within IPAWS, including whether the alert includes audio, text length and number of alerting platforms over which the alert is intended to be distributed.<sup>25</sup> According to FEMA data, the average processing time for these functions incurred within IPAWS for a CAP WEA-bound alert is 1.667 seconds.<sup>26</sup>

---

<sup>23</sup> See Appendix B.

<sup>24</sup> More broadly, communications links from the ground sensors to the EAC, the EAC to IPAWS, and IPAWS to the CMSP gateway should all be secure, reliable and “always-on” connections, with priority and quality-of-service (QoS) performance capabilities. Some of these concepts are present in the TSP (Telecommunications Service Priority) and GETS/PAS (Government Emergency Telecommunications Service/Wireless Priority Access Service) and should be extended to IP-based networks for machine-to-machine communications.

<sup>25</sup> See FEMA *ex parte* filing, PS Docket 16-32.

<sup>26</sup> *Id.*

#### 4.2.1. Optimizing the Current IPAWS for EEW Alerts

The following optimization measures could reduce the average total IPAWS processing time expenditure to less than one second.

**Customize IPAWS to receive simple EEW alerts.** Customize IPAWS’s internal processing routines to handle EEW alert messages received from the EAC differently than standard IPAWS alerts. According to FEMA, for example, a “stripped down EEW alert would not require EAS validation, references to current or expired alerts, or mp3 audio attachments.”<sup>27</sup>

**Select a single dissemination channel.** The EAC can reduce the IPAWS processing time by selecting only one dissemination channel, such as WEA.

**Simplify geo-targeting.** Specify the area affected by the EEW alert using the location codes described in the American National Standards Institute (ANSI) standard, ANSI INCITS 31-2009, currently used for EAS alerts, instead of complex polygons.<sup>28</sup>

**Simplify EEW alert message content.** There is a correlation between alert message complexity and IPAWS processing time. Accordingly, the EEW CAP alert message should be streamlined to include only the bare essential information, and exclude URL links, images audio/video files, excessive text and other non-essential elements.

**Prioritize EEW alerts.** Delays within IPAWS associated with alert messaging queuing can be eliminated by prioritizing EEW alerts, second only to Presidential alerts, so that EEW alerts do not have to wait in line at the IPAWS output queue (except for Presidential alerts) before they are distributed by IPAWS to their alerting platform.

#### 4.2.2. EEW Alerting in an Alternative EEW System

We observe that there are other alternative approaches for delivery of time-sensitive alerts. In particular, we observe that while the primary elements of the national alerting structure – IPAWS and EAS – can be optimized to some extent to expedite EEW alerts, they were not originally designed to distribute alerts within seconds of their origination.<sup>29</sup> Further, in any warning scenario involving an imminent threat, the overarching objective is to get the warning out to as many people as quickly as possible, using as many communication mediums as technically feasible. To that end, we observe that an EEW alerting paradigm

---

<sup>27</sup> *Id.*

<sup>28</sup> ANSI standard, ANSI INCITS 31-2009 (“Information technology—Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas”) identifies geographic areas at the county and sub-count levels. *See* 47 CFR § 11.31(c).

<sup>29</sup> For example, national activation of the EAS for a Presidential alert message, initiated by the transmission of an Emergency Action Notification (EAN) event code, is designed to provide the President the capability to transmit an alert message (in particular, an audio alert message) to the American public within ten minutes from any location at any time. *See, e.g., Review of the Emergency Alert System*, EB Docket No. 04-296, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd. 18625, 18628, para. 8 (2005) (*First Report and Order and Further Notice of Proposed Rulemaking*). *See also, e.g.,* FEDERAL GOVERNANCE, EXECUTIVE ORDER (E.O.) 13407 (“In the event of a national emergency, the President may use IPAWS to communicate to the public quickly, easily, and simultaneously via multiple communications pathways with only 10 minutes notice.”), <http://www.fema.gov/federal-governance> (last visited July 19, 2016). The EAS rules require State and local EAS alerts to be broadcast within 15 minutes of receipt. *See* 47 CFR § 11.51(n).

that incorporates multiple platforms and mediums, and new technologies, all emanating directly from the EAC in a one-to-many ecosystem may offer an alternative methodology for distributing EEW alerts.

While IPAWS serves a critical role in aggregating alerts from multiple sources and redistributing those based on alerting platform and type, we find that if this processing function is not necessary, an alternative approach is to have the EAC transmit the EEW alert in CAP WEA format directly to the CMSP Gateway over a VPN. By bypassing IPAWS, the time expenditures associated with both IPAWS processing and T2 transmission can be eliminated. Under this paradigm, functions such as validation and verification served by IPAWS can be exported to the EAC system, with management and administration for such functions overseen by FEMA personnel. This EAC-to-CMSP Gateway structure largely mirrors the structure for EEW alerting currently employed in Japan's EEW system.<sup>30</sup>

New technologies can be incorporated into this EEW ecosystem as they mature. For example, the AWARN Alliance has proposed using Advanced Television Systems Committee (ATSC) 3.0 standardized broadcasts and end user devices to deliver EEW alerts.<sup>31</sup> The ATSC 3.0 standard enables use of a subcarrier in TV broadcasters' RF signal to "distribute text and rich media alerts simultaneously to an unlimited number of ATSC 3.0-enabled fixed, mobile, and hand-held devices, indoors or outdoors across an entire metropolitan area."<sup>32</sup> The AWARN Alliance indicates that "[c]onceptually, AWARN could enable EEWs to be received by the public in fewer than three seconds."<sup>33</sup> Global Security Systems indicates that the satellite-based, FM radio-delivered emergency alert system, ALERT FM, could be used to deliver CAP-formatted EEW alerts in under six seconds.<sup>34</sup> Since current 3GPP 5G requirements target low-latency, high-resiliency and high-availability for critical communications, it is anticipated that 5G network parameters may also permit processing of EEW alerts that include more information and capabilities than that currently feasible under WEA, such as leveraging multiple sensors for machine-to-machine communication.<sup>35</sup>

---

<sup>30</sup> See, e.g., Will Knight, MIT Technology Review, How Japan's Earthquake and Tsunami Warning Systems Work (March 11, 2011), <https://www.technologyreview.com/s/423279/how-japans-earthquake-and-tsunami-warning-systems-work/>; Lucy Birmingham, Time, Japan's Earthquake Warning System Explained (Mar. 18, 2011), <http://content.time.com/time/world/article/0,8599,2059780,00.html>.

<sup>31</sup> See AWARN Alliance Comments at 1. According to the AWARN website:

AWARN, utilizing ATSC 3.0 Advanced Emergency Alerting, represents a major upgrade to America's emergency communication system. AWARN uses next-generation terrestrial broadcasting to deliver rich-media, geo-targeted public alerts. AWARN wakes up devices, delivering alerts even when the cellular network is jammed or the power grid is down.  
<http://awarn.org/>

<sup>32</sup> *Id.* A Petition for a Rulemaking to authorize permissive use of the ATSC 3.0 standard is currently pending before the Commission. See Joint Petition for Rulemaking of America's Public Television Stations, The AWARN Alliance, The Consumer Technology Association, and The National Association of Broadcasters, GN Docket No. 16-142 (filed Apr. 13, 2016).

<sup>33</sup> *Id.* at 2.

<sup>34</sup> See Global Security Systems/ALERT FM Comments at 1.

<sup>35</sup> Earthquake sensors are one category of devices that should receive priority in a fully realized Internet of Things.

### 4.3. Alert Dissemination Channels

#### 4.3.1. Wireless Emergency Alerts (WEA)

*Key Finding:* The distribution of EEW alerts to the public within three seconds may potentially be achievable over WEA and 4G/LTE networks, provided that certain technical modifications are made to, and certain operational parameters are established for, IPAWS and CMSP networks.

*Basic WEA functions.* WEA is an alerting system through which authorized federal, state and local government entities can geographically target Presidential, Imminent Threat, and AMBER Alerts to WEA-capable mobile devices of Participating CMS Providers' subscribers. In 2008, pursuant to processes required by the Warning, Alert and Response Network (WARN) Act,<sup>36</sup> the Commission adopted rules allowing CMSPs to voluntarily deliver timely and accurate emergency alerts to subscribers' mobile devices.<sup>37</sup> Since WEA was launched on April 7, 2012,<sup>38</sup> the system has been used to issue over 21,000 timely and accurate emergency alerts, including severe weather warnings, evacuate and shelter-in place alerts, and America's Missing: Broadcast Emergency Response (AMBER) Alerts.<sup>39</sup> Many CMSPs, including the four nationwide wireless carriers, elected to participate in WEA, at least in part.<sup>40</sup> Moreover, wireless technologies have evolved since WEA's adoption, and present possibilities for expanding WEA's capabilities in such areas as alert geo-targeting, provision of multilingual content, embedded references (*i.e.*, URLs and phone numbers), and text length.<sup>41</sup>

Our analysis indicates that the typical, non-optimized end-to-end (from EAC to device) transmission and processing time expenditure of an EEW WEA alert delivered over an LTE network is 3.30 to 4.27

---

<sup>36</sup> On October 13, 2006, the President signed the Security and Accountability for Every Port (SAFE Port) Act into law. Title VI of the SAFE Port Act, also known as the WARN Act, establishes a process for the creation of a national mobile alerting system, now known as WEA, whereby Participating CMS Providers transmit emergency alerts to their subscribers. *See* Warning, Alert and Response Network (WARN) Act, Title VI of the Security and Accountability For Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (2006) (WARN Act).

<sup>37</sup> *See* 47 CFR § 10; *see also* *The Commercial Mobile Alert System*, PS Docket No. 07-287, First Report and Order, 23 FCC Rcd 6144 (2008) (*WEA First Report and Order*); *The Commercial Mobile Alert System*, PS Docket No. 07-287, Second Report and Order and Further Notice of Proposed Rulemaking, 23 FCC Rcd 10765 (*WEA Second Report and Order*); *Commercial Mobile Alert System*, PS Docket 07-287, Third Report and Order, 23 FCC Rcd 12561, (2008) revised by Erratum (dated Sept. 5, 2008) (*WEA Third Report and Order*).

<sup>38</sup> *See* FCC's Public Safety and Homeland Security Bureau Sets Timetable in Motion for Commercial Mobile Service Providers To Develop a System That Will Deliver Alerts to Mobile Devices, PS Docket No. 07-287, Public Notice, 24 FCC Rcd 14388 (PSHSB 2009).

<sup>39</sup> *See* E-mail From Alfred Kenyon, IPAWS Program Office, National Continuity Programs, Department of Homeland Security, FEMA, to Gregory Cooke, Associate Division Chief, Policy & Licensing Division, Public Safety and Homeland Security Bureau, FCC (Oct. 13, 2015) (on file with author). *See also* CTIA, *Wireless Emergency Alerts*, <http://www.ctia.org/your-wireless-life/consumer-tips/wireless-emergency-alerts> (last visited Apr. 30, 2015). The AMBER (America's Missing: Broadcast Emergency Response) program is a nationwide alerting program designed to help bring missing children to safety. *See* Office of Justice Programs, *About AMBER Alert*, <http://www.amberalert.gov/about.htm> (last visited May 7, 2015).

<sup>40</sup> *See* FCC, *Master CMAS Registry*, <https://www.fcc.gov/pshs/docs/services/ctia/CMASRegistry.xls> (last visited Oct. 21, 2015); *see also* PS Docket No. 08-146 (containing a record of all Participating CMS Providers' elections to participate in WEA).

<sup>41</sup> The Commission released a Notice of Proposed Rulemaking in November, 2015, that sought comment on several improvements to WEA's performance in these areas. *See* *Wireless Emergency Alerts*, PS Docket No. 15-91, Notice of Proposed Rulemaking, 30 FCC Rcd 13781 (2015).

seconds.<sup>42</sup> The typical, non-optimized end-to-end transmission and processing time expenditure of an EEW WEA alert delivered over a UMTS network is 4.66 to 5.63 seconds.<sup>43</sup>

#### 4.3.1.1. Optimizing WEA for EEW Alerts

Several network optimization measures, when combined with EAC and IPAWS optimization measures described above, can reduce the end-to-end transmission and processing time expenditure for EEW WEA alert delivery to under three seconds. For instance, reducing SIB12 frequency from 320 ms to 80 ms and IPAWS processing time from 1667 ms to 750 ms or 900 ms can reduce the end-to-end transmission and processing time expenditure for delivering an EEW WEA alert over an LTE network to a range of 1.90 to 2.69 seconds.<sup>44</sup> Similarly, the end-to-end transmission and processing time expenditure for delivering an EEW WEA alert over a UMTS network can be reduced to a range of 3.74 to 4.53 seconds.<sup>45</sup> Based upon these figures, we recommend using LTE networks to deliver WEA EEWs whenever and wherever possible.

***Optimize 4G/LTE Networks for EEW by shortening message length.*** A short EEW alert message (less than 90 characters) would minimize transmission time, as it requires only one SIB-12 message segment. The SIB-12 frequency can be set at the minimum setting value of 80 ms, thus minimizing the transmission time to the mobile device. If allowing one extra SIB-12 period to cover bad channel conditions, the corresponding total transmission time would be 160 ms.<sup>46</sup>

With these operational optimizations, the transmission and processing time range for delivering a WEA EEW over LTE can be improved to a range of from 1.90 to 2.69 seconds.<sup>47</sup> Accordingly, with the proposed optimizations, WEA for LTE could provide CMSP-related (*i.e.*, CMSP Gateway to device) transmission and processing times of 1.05 seconds to 1.69 seconds<sup>48</sup>. With potential operational optimizations addressed earlier, the UMTS end-to-end transmission and processing time range can be improved to be 3.74 seconds to 4.53 seconds<sup>49</sup>.

---

<sup>42</sup> See Appendix D.

<sup>43</sup> *Id*

<sup>44</sup> See Appendix D, Section “Processing Time with Transmitting an EEW Alert via WEA.” The 1900 ms end-to-end delay corresponds to T1=50 ms, P1= 750 ms, T2=50 ms, (P2+T3+P3+T4+P4+T5+P5) = 250 ms, T6=160 ms and P6 = 640 ms. And, the 2690 ms end-to-end delay would correspond to T1=50 ms, P1=900 ms, T2=50 ms, (P2+T3+P3+T4+P4+T5+P5)=250 ms, T6=160 ms and P6=1280 ms.

<sup>45</sup> See Appendix D, Section “Processing Time with Transmitting an EEW Alert via WEA” for details. The 3740 ms end-to-end delay corresponds to T1=50 ms, P1= 750 ms, T2=50 ms, (P2+T3+P3+T4+P4+T5+P5) = 250 ms, T6=2000 ms and P6 = 640 ms. And, the 4530 ms end-to-end delay would correspond to T1=50 ms, P1=900 ms, T2=50 ms, (P2+T3+P3+T4+P4+T5+P5)=250 ms, T6=2000 ms and P6=1280 ms.

<sup>46</sup> In other words, if SIB-12 transmission frequency is 80 ms, and due to channel conditions the first transmission is not received at the device, then the EEW can be retransmitted 80 ms later, the additional transmission making the total delay 160 ms.

<sup>47</sup> See *supra* note 41.

<sup>48</sup> These numbers correspond to the delay between the CMSP gateway and the device, and exclude T1, P1 and T2 delays. Therefore, 1050 ms = 1900 ms – (50 + 750 + 50) ms and 1690 ms = 2690 ms – (50 + 900 + 50) ms.

<sup>49</sup> See *supra* note 42.

#### 4.3.1.2. Optimizing UMTS Using the Earthquake and Tsunami Warning System (ETWS)

While the transmission and processing time expenditure for EEW WEA alerts delivered over UMTS exceeds three seconds, an alternative to UMTS may be found by using a competing technology called the Earthquake and Tsunami Warning System (ETWS). ETWS is a 3GPP standards-based warning system, originally initiated and currently deployed in Japan. The original ETWS technical specifications were developed for UMTS and part of the 3GPP Release-8. Subsequently, ETWS technical specifications for LTE were released.<sup>50</sup> ETWS is designed to accommodate two basic types of earthquake and tsunami related alert messages: (i) the primary notification, which contains minimum, urgently required information (for example, “Warning! Earthquake in your area”) and (ii) the secondary notification, which provides supplementary information not contained in the primary notification (such as seismic intensity, epicenter, *etc.*). The original ETWS specifications require that the Primary notification be delivered within four seconds to the end user devices in the target notification area, even in situations of network congestion.<sup>51</sup>

Given that ETWS for UMTS could provide end-to-end transmission and processing time, including that caused by IPAWS, of 1.74 to 2.53 seconds, our recommendation is that the ETWS “dual-stack” solution be deployed, where EEW Alerts are delivered via ETWS and other types of alerts are delivered through WEA.<sup>52</sup>

#### 4.3.2. Emergency Alert System

*Key Finding:* We find that although the EAS has great value as a public warning system in many instances, distribution of EEW alerts via IPAWS over the EAS to the public in fewer than three seconds is not reasonably achievable using the current EAS architecture.<sup>53</sup> Further, although we identify certain optimization measures below that would be required to bring EEW alert delivery at or near to the three-second delivery threshold, we question whether applying such measures now would be a prudent use of resources, as any such approach could diminish the resilience – and non-EEW value – of the current system.

*Basic EAS functions.* The EAS is a national public warning system through which broadcasters, cable systems, and other service providers (“EAS Participants”) deliver alerts to the public to warn them of impending emergencies and dangers to life and property.<sup>54</sup> The primary purpose of the EAS is to provide the President with “the capability to provide immediate communications and information to the general

---

<sup>50</sup> See 3GPP TS 23.041

<sup>51</sup> See 3GPP TS 22.168 V8.1.0 (2008-06). See also Appendices D and E. Also, ETWS for UMST requires the delay to be less than 4 seconds. As indicated above, it could be 1.74 to 2.53 seconds.

<sup>52</sup> See Appendix E for the definition of “Dual-Stack” and the delay calculations.

<sup>53</sup> See Appendix F.

<sup>54</sup> See *Review of the Emergency Alert System; Independent Spanish Broadcasters Association, The Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, ET Docket No. 04 296, Fifth Report and Order, 27 FCC Rcd 642, 646 para. 6 (2012) (*Fifth Report and Order*). A more detailed history of the EAS is summarized in the first Notice of Proposed Rulemaking in this docket. See *Review of the Emergency Alert System*, EB Docket No. 04-296, Notice of Proposed Rulemaking, 19 FCC Rcd 15775, 15776-77, paras. 6-8 (2004). In addition, an overview of the present organization and functioning of the EAS system is included in the Second Report and Order. See *Second Report and Order*, 22 FCC Rcd 13275, 13280-83, paras. 11-14 (2007).

public at the National, State and Local Area levels during periods of national emergency.”<sup>55</sup> The EAS also is used to distribute alerts issued by state and local governments, as well as the National Weather Service (NWS).<sup>56</sup> According to NWS, about 90 percent of all EAS activations are generated by NWS and relate to short-term weather events.<sup>57</sup> Although EAS Participants are required to broadcast Presidential alerts, they participate in broadcasting state and local EAS alerts on a voluntary basis.<sup>58</sup> The Commission, FEMA and the NWS implement the EAS at the federal level.

The core missions of the EAS, *i.e.*, providing the President with a means to address the American public and distributing state and local alerts, are vital to the national interest. The current EAS architecture serves this function extremely well, largely due to its simple yet resilient structure. Some of the EAS’s features that render it less than ideal for ultra-fast alert delivery, such as its legacy distribution methodology for distributing alerts over-the-air from one EAS Participant to another, retain a robustness whose resilience lies in this relatively primitive design. Thus, altering this design for the sole purpose of delivering EEW alerts in three seconds or less, may have a negative effect on the underlying value of the EAS and, therefore, may not merit the significant resources and expense that such a redesign likely would entail.

Based on the data submitted in the record, we estimate the end-to-end time expenditure of an EEW alert from the EAC to the output of the EAS device would take at least 3.717 seconds – a time figure that does not include the time required to acquire the EEW CAP alert from IPAWS.<sup>59</sup> Acquiring the EEW CAP alert from the IPAWS “Atom feed”<sup>60</sup> adds another 250 ms to 34 seconds for typical EAS device configurations.<sup>61</sup> Even if this figure could be lowered to something on the order of 100 ms (by switching to a “push” system at the IPAWS output connection) – thus, making the EAC-to-EAS device output

---

<sup>55</sup> 47 CFR § 11.1.

<sup>56</sup> See, e.g., *Review of the Emergency Alert System; Independent Spanish Broadcasters Association, The Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, ET Docket No. 04 296, Third Further Notice of Proposed Rulemaking, 26 FCC Rcd 8149, 8152-53, para. 3 (2011) (*Third Further Notice of Proposed Rulemaking*).

<sup>57</sup> See NWS Fact Sheet, *NOAA’s National Weather Service (NWS) and the Emergency Alert System* (Jan. 2014), [http://www.nws.noaa.gov/os/dissemination/EAS\\_factsheet.pdf](http://www.nws.noaa.gov/os/dissemination/EAS_factsheet.pdf).

<sup>58</sup> See *Review of the Emergency Alert System*, First Report and Order and Further Notice of Proposed Rule Making, 20 FCC Rcd 18625, 18628, para. 8 (2005).

<sup>59</sup> Specifically, this time frame consists of 50ms for T1 (we assume that the T1 connection has been optimized), 1.667 seconds for IPAWS processing (P1), and two seconds for EAS device processing (P2). We observe that the figure for EAS device processing (P2) was a rough average of processing times reported by EAS device manufactures, based on a plain CAP message with little or no text, and no embedded audio or streaming audio, and could exceed two seconds in various instances. See Trilithic *Ex Parte* Letter at 2 (indicating that “[a]fter a CAP message and the audio resource has been retrieved, the Trilithic EASyCAP Encoder/Decoder can process the alert, produce the content, and retransmit the emergency message in under a half second,” but noting that “[p]roducing [TTS] audio, if required, can take 1-8 seconds depending on the text length.”); Sage Comments at 4 (“In the typical case, an EEW alert using [TTS] would be ready to air in two seconds or less.”); Monroe Reply Comments at 7 (“The entire process of retrieving a CAP XML message [from the IPAWS-OPEN Atom feed], extracting the audio (if embedded [file]), and preparing for playout or forwarding to downstream systems can be accomplished within approximately 2-3 seconds,” but that if the EAS device has to render TTS (because no audio file is embedded and no audio streaming source is identified), the process “may take up to 2-4 seconds, depending on the length of the message to be converted to speech.”).

<sup>60</sup> IPAWS’s Atom feed is a message distribution system to which remote devices periodically interconnect (or “poll”) to check for and acquire (or “pull”) new CAP EAS alerts. See Appendix F.

<sup>61</sup> See Trilithic *ex parte*, 1, Sage *ex parte* 2.

figure at least 3.817 seconds – the EEW alert information would still be subject to downstream equipment delays prior to broadcast, the processing time for which can vary from 5 seconds to 120 seconds.<sup>62</sup>

#### 4.3.2.1. Optimizing EAS for EEW Alerts

There are several elements that contribute heavily to the overall EAS EEW alert delivery time and that could be modified to improve speed of delivery, albeit not sufficiently to achieve the three-second delivery threshold.<sup>63</sup>

**Implementing a “smart push” mechanism.** The mechanism through which EAS devices acquire alerts from IPAWS could be changed from the current polling (or “pull”) system. Specifically, EAS Participants currently poll the IPAWS Atom feed in a configurable regular interval, typically set at 30 seconds, and then “pull” relevant EAS alert messages from the IPAWS feed.<sup>64</sup> One approach to avoid this polling time is to use a “smart push” mechanism for EEW alerts (but retain the pull mechanism for all other EAS alerts), under which EEW alerts would be “pushed” out to the EAS devices as soon as the alert was processed within IPAWS. To avoid some of the potential large-scale push mechanism related issues, the non-EEW EAS alerts can continue using the existing “pull” mechanism. Furthermore, the IPAWS Gateway can utilize smart heuristics to only “push” EEWs to the EAS devices in affected States.

**Removing EAS Header Codes.** All EAS alerts begin with the transmission of the EAS header codes (broadcast as audible tones) that take approximately seven seconds to broadcast before the Attention Signal (if the EAS Participant elects to broadcast it) and audio message is broadcast. If the EEW alert is not going to be further distributed over the EAS from one EAS Participant to another, then the EAS Header Codes could be eliminated.<sup>65</sup> However, because these audio tones also alert viewers and listeners that an alert is in progress, some form of very brief attention signal may be prudent for radio services.

**Shortening message length and simplifying message content.** Limiting the EEW alert message to a short, simple text message would minimize processing time. To minimize audio processing time, the EEW alert should not include embedded audio or specify streaming audio, but rather should rely on Text-to-Speech (TTS) in the EAS device to generate audio from the brief text (this would require that all EAS devices be equipped with TTS software). The EEW alert should also be processed in the same manner by IPAWS, EAS devices, and downstream equipment as Presidential alerts.

---

<sup>62</sup> See, e.g., Trilithic *Ex Parte* at 2; Sage *Ex Parte* at 5; Monroe Reply Comments at 7. This wide variance is due to the fact that the entities over whose facilities the EAS alert is transmitted are composed of many different services (TV broadcast, coax, fiber and wireless cable service, radio, etc.), each deployed over very different types of facilities. EAS alerts are processed and broadcast over TV broadcast facilities, for example, in an entirely different manner than they are over cable facilities. These services also are governed by different families of equipment standards. Moreover, even within service categories, there are multiple equipment configurations that may result in different processing delays. For example, the transmission equipment configuration of an automated radio station that broadcasts pre-composed programming may be largely differentiated from that of a manned radio station that broadcasts live programming.

<sup>63</sup> Because we envision a total time expenditure of 950 ms covering the EEW alert from the EAC to the IPAWS output connection, achieving the three-second mark would require the EAS device to acquire the alert, process and output the EAS information, and for the downstream equipment to further process such information and transmit it over the service’s main public transmission within 2.050 seconds.

<sup>64</sup> See Appendix F.

<sup>65</sup> Because these audio tones also alert viewers and listeners that an alert is in progress, some form of very brief attention signal may be prudent for radio services.



***Improving EAS performance as incorporated into a new EEW paradigm.*** As discussed in Section 4.2.2, an alternative EEW system would resemble a one-to-many alerting ecosystem whereby EEW alerts were disseminated directly from the EAC over multiple alert dissemination platforms. EAS devices are configured with Internet connections, and likely could be updated to process EEW alerts transmitted to them by the EAC on a priority basis. These EEW alerts could be engineered to minimize processing time by EAS devices. EAS device manufacturers have opined on similar potential approaches for minimizing EAS processing. For example, Monroe observes that “in an [EEW system], it may be desirable for the audio information for the alert to be pre-recorded and pre-positioned at the edge of the network (for instance in an EAS device that can support EEWS, or other EEWS solution), rather than provided by the originator or compiled at the edge as text-to-speech.”<sup>66</sup> Monroe further observes that two of its equipment models can “be potentially configured to produce a modified alerting output for an EEW mission,” that would include “pre-positioned audio and textual messages for automatic playout[,] . . . additional USGS alerting information that may not be included in the current IPAWS CAP Profile[, and] . . . transmission of EEW alerts immediately upon receipt [subject to downstream equipment processing delays].”<sup>67</sup> While processing timelines associated with transmission equipment downstream from the EAS device will continue to delay speed-of-transmission, this equipment is itself changed out over time, and as newer technologies and standardized equipment forms are developed and deployed, downstream EEW alert processing can be streamlined. Moreover, this optimization would not diminish operation of the legacy EAS or fulfillment of the EAS’s missions.

#### **4.3.3. IPAWS Public (All-Hazard) Feed**

*Key Finding:* The distribution of EEW alerts through IPAWS to the public within three seconds appears achievable over Internet-based services interconnected with IPAWS (via the IPAWS Public Feed), provided that the output connections of IPAWS are modified to enable the fastest, technically feasible method for disseminating EEW alerts from IPAWS to such services.

*Basic IPAWS Public Feed functions.* Current IPAWS architecture allows the alerts marked “public” and processed to be delivered to the IPAWS All-Hazards public information feed. Authorized Internet-Service alert providers can access and monitor this feed through a simple PIN-controlled interface to receive the CAP formatted alerts and send them to the public via Internet-connected services and systems.<sup>68</sup>

Similar to IPAWS’s Atom feed used for CAP alert dissemination to EAS devices, the All-Hazards information feed currently operates based on a polling mechanism where the polling interval is user-configurable. To secure this recurring connection, a new HTTPS connection must be re-established for every polling event, which adds approximately 500 ms to the overall alert delivery time.<sup>69</sup>

Once the alert is retrieved from the All-Hazard information feed by the Internet-Service alert provider, it has to be sent to the end user. The precise mechanisms, and the associated transmission and processing times, depend on the specifics of the service involved, which in general are not regulated by the Commission.

---

<sup>66</sup> Monroe Reply Comments at 10-11.

<sup>67</sup> *Id.* at 12.

<sup>68</sup> Currently there are 77 FEMA authorized Internet-Service Alert providers, notably Facebook, Public Broadcast Service (PBS), and the Weather Channel. See FEMA, Integrated Public Alert & Warning System. <http://www.fema.gov/integrated-public-alert-warning-system> (last visited Aug. 25, 2016).

<sup>69</sup> See Appendix F for a description of message delivery time frames using a polling system.

**Implement a “push” mechanism.** If Internet-Service is to be used for EEW alerting, the current “Pull” mechanism used by IPAWS for disseminating CAP messages to Internet services must be changed to a “Push” mechanism. For the push service, the average transmission and processing time to deliver an EEW alert from the EAC to the Internet alert provider is 1717 ms. To enable three-second EEW alert distribution over Internet services via IPAWS, the transmission and processing time incurred by the various Internet-Service dissemination channels (e.g., Facebook, PBS, etc.) would have to be less than 1283 (3000-1717) ms.

We find that if the alert message delivery mechanism used by IPAWS for disseminating CAP messages to Internet services is changed from a “pull” to a “push” mechanism, and depending upon the operating parameters and technical design of the dissemination channel, it may be feasible to deliver EEW alerts in fewer than three seconds.

#### 4.3.4 General Cybersecurity Concerns

To mitigate the risk from Internet protocol dependencies, the cybersecurity of the system (e.g., through deployment of Confidentiality, Integrity and Availability throughout the end-to-end EEW chain), may need to be considered.<sup>70</sup>

## 5. CONCLUSION

The analyses in this white paper indicate that EEW alerts can be delivered through IPAWS over the WEA platform in a timely manner, and with various optimization steps described above, theoretically in fewer than three seconds. Delivery of EEW alerts through IPAWS over the EAS in its current architecture in fewer than three seconds appears to be largely unfeasible. However, it is important to keep in mind that, while faster is always better in the alerting paradigm, the EEW alert does not need to be broadcast in fewer than three seconds to have immense value. As indicated, the first public EEW warnings broadcast to the public during the 2011 Japan earthquake did not occur until 8.6 seconds after detection of the P wave yet still provided 15 seconds of advanced warning before the main shock arrived at the coast city of Sendai. Further, there are several non-communications factors that contribute to the overall effectiveness of any given EEW alert, such as distance from the earthquake epicenter, detection efficiency, and forecasting software. An effective EEW system, therefore, represents a warning ecosystem composed of many parts, all finely tuned to each other. As EAS capabilities evolve, there should be no technical hurdle in a benign security environment that would prevent attainment of the three second objective. The Commission should consider adding EEW to the policy objectives for future EAS upgrades.

In light of the systemic nature of the EEW concept, the analyses in this white paper, and the various efforts now underway by the USGS and others to develop a fully functioning EEW system, we believe that integrating EEW alerting through IPAWS on a national scale seems very promising. Because much of the EEW system itself is still under development, and because optimization of WEA, EAS and other potential EEW alert delivery platforms entails highly technical determinations across multiple communications services, we recommend the following:

---

<sup>70</sup> Confidentiality refers to the protection of data from unauthorized access and disclosure, both while at rest and in transit. *See, e.g.*, ATIS, ATIS Telecom Glossary, <http://www.atis.org/glossary/definition.aspx?id=6609>. Integrity refers to the protection against the unauthorized modification or destruction of information. *See, e.g.*, ATIS, ATIS Telecom Glossary, <http://www.atis.org/glossary/definition.aspx?id=4584>. Availability refers to the accessibility and usability of a network upon demand. *See, e.g.*, ATIS, ATIS Telecom Glossary, <http://www.atis.org/glossary/definition.aspx?id=5637>.

- USGS should continue its work on Sensors and EAC(s).
- The Commission should take up the technical issues raised in this white paper in a forum composed of expert stakeholders such as the Communications Security, Reliability and Interoperability Council (CSRIC), or other Federal Advisory Committee (FACA) chartered specifically for EEW Warning Message Distribution implementation recommendations.
- The Commission, in partnership with USGS should disseminate objectives to 3GPP and other 5G Standards Development Organizations to facilitate inclusion of EEW capabilities in the design of 5G networks and devices.

**APPENDIX A**  
**List of Commenting**  
**Parties**

**Initial Comments**

- 1) AT&T Services Inc.
- 2) AWARN Alliance
- 3) Frank W. Bell
- 4) Art Botterell
- 5) CTIA
- 6) Global Security Systems/ALERT FM
- 7) Nikolaus E. Leggett
- 8) Sage Alerting Systems, Inc.
- 9) US Geological Survey (late filed)

**Reply Comments**

- 1) Alliance for Telecommunications Industry Solutions (ATIS)
- 2) America's Public Television Stations ("APTS"), the Corporation for Public Broadcasting ("CPB"), National Public Radio ("NPR") and the Public Broadcasting Service ("PBS") (filing jointly)
- 3) Monroe Electronics, Inc.
- 4) National Cable & Telecommunications Association

**Ex Parte Meeting**

- 1) Alliance for Telecommunications Industry Solutions (ATIS)
- 2) AT&T Services Inc.
- 3) BlackBerry Corporation
- 4) Comtech Telecommunications Corp.
- 5) Federal Emergency Management Agency
- 6) Microsoft Corporation
- 7) Monroe Electronics, Inc.
- 8) Sage Alerting Systems, Inc.
- 9) SEISMIC WARNING SYSTEMS, INC.
- 10) Trilithic, Inc.
- 11) Verizon

## APPENDIX B

### Functions and Latencies in the Earthquake Alert Center

Most alerts, including the proposed EEW alerts are delivered in CAP.<sup>1</sup> CAP is an open, interoperable standard, developed within the OASIS standards process, that can be used as an Extensible Markup Language (XML) document (or other coding schemes) for web publication.<sup>2</sup> CAP-formatted alerts can include audio, video or data files; images; multilingual translations of alerts; and links providing more detailed information than what is contained in the initial alert (such as streaming audio or video).<sup>3</sup> CAP utilizes standardized fields that facilitate interoperability between and among devices.<sup>4</sup> CAP also is utilized for various state and local alerting systems. CAP provides each alert with a unique alert identifier and supports alert authentication through the provision of a digital signature and an encryption field that enables greater protection of the CAP message.<sup>5</sup>

Upon the creation of CAP-formatted earthquake alert message, the EAC will transmit the alert message to IPAWS. Typically, alert originators transmit their alert messages via secure public Internet using Transport Layer Security (TLS)/HTTPS protocol. Each TLS connection begins with a handshake between the client and the server. During this handshake, the Public Key Infrastructure (PKI) suite is used to authenticate the server (and sometime the client) and to generate cryptographic session keys to create a secure channel for data transmission. Establishing an end-to-end connection, using the Transmission Control Protocol (TCP), would require a delay of three Round Trip Times (RTT) between source and destination because of the TCP handshake. The total time required for HTTPS setup, among other things, would depend on the server performance, the geographic distance between the client and the server, the strength of the cryptographic key used, and the time required to verify the server's certificate. The performance of the HTTPS setup time is typically optimized using various techniques such as session key caching.<sup>6</sup> Once the alert message arrives at the IPAWS successfully, IPAWS will start processing the alert, while at the same time sending back to the EAC an acknowledgement ("ACK").

Publically available data show that the secure link setup time could take a few hundred milliseconds (ms),

---

<sup>1</sup> As detailed in Appendix F, the EAS architecture uses the Specific Area Message Encoding (SAME) protocol to distribute emergency alerts between the various broadcast stations, cable systems and other entities that process EAS alerts. However, alert originators can use CAP-formatted alert messages to initiate EAS alerts.

<sup>2</sup> See OASIS, *Common Alerting Protocol Version 1.2* (July 1, 2010), <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>.

<sup>3</sup> See *Review of the Emergency Alert System; Independent Spanish Broadcasters Association, The Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, Second Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 13275, 13285-88, paras. 22-25 (2007) ("*Second Report and Order*"). See also OASIS Common CAP Standard v1.2, § 3.2.

<sup>4</sup> The CAP standard specifies what fields an alert message can contain and what information can be included in the particular fields, such as message type, scope, incident, and event information. See OASIS Common CAP Standard v1.2, § 3.2.

<sup>5</sup> See OASIS, *Common Alerting Protocol Version 1.2* (July 1, 2010), <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>.

<sup>6</sup> See Brian Jackson, *Analyzing HTTPS Performance Overhead* (July 22, 2016), <https://www.keycdn.com/blog/https-performance-overhead/> (analyzing latencies associated with moving to HTTPS).

and on average, about 150 ms.<sup>7</sup> In addition to the setup time, the transmission of the alert message would take very little additional time (depending on the distance and transmission medium, and typically less than 50 ms, for one-way transmission time).<sup>8</sup> Transmission latency also would be impacted by the character length of the alert. Typical setup and transmission time would thus be around 200 ms. Data provided by FEMA indicates that transmission time between a FEMA test originator and IPAWS average 141ms.<sup>9</sup>

---

<sup>7</sup> *Id.* (increased load time with HTTPS). Furthermore, while any communication through the public Internet can potentially experience rare and exceptionally long excessive delays, in this analysis we focus on the regular Internet behavior and not on those rare events. We recommend that the rare events be treated separately and as “exceptions.”

<sup>8</sup> Transmission time would depend on the type of media (copper, fiber, *etc.*) and physical distance. In the continental U.S., the maximum distance between two points is 2892 miles. The propagation speed in fiber and copper are typically around 0.6 times and 0.75 times the speed light, respectively. From these two facts, one can easily compute the maximum transmission time due to distance. Additional transmission time is incurred due to the number of hops, router queuing and encryption/decryption in TLS or Internet Protocol Security (IPSec). *See Site-by-monthly History Table for Average Round Trip Time by-node with 100 byte packets to United States seen from EDU.SLAC.STANFORD.PINGER, excluding none*, [http://www-wanmon.slac.stanford.edu/cgi-wrap/pingtable.pl?file=average\\_rtt&by=by-node&size=100&tick=monthly&from=EDU.SLAC.STANFORD.PINGER&to=United+States&ex=none&only=all&dataset=hep&percentage=any](http://www-wanmon.slac.stanford.edu/cgi-wrap/pingtable.pl?file=average_rtt&by=by-node&size=100&tick=monthly&from=EDU.SLAC.STANFORD.PINGER&to=United+States&ex=none&only=all&dataset=hep&percentage=any) (last visited Aug. 25, 2016) (providing average round trip times and standard deviations).

<sup>9</sup> *See* FEMA *ex parte* filing, PS Docket 16-32

## APPENDIX C

### Functions and Latencies in the Integrated Public Alert and Warning System

IPAWS is divided into two functional areas: IPAWS Aggregator and IPAWS Gateway, which collectively are referred to as IPAWS. We discuss each of these functional areas below, in turn.

#### **IPAWS Aggregator:**

The IPAWS Aggregator performs the following three core functions: (1) it authenticates the alert originator by checking to see if the message sender has a valid certificate; (2) it checks to see if the alert originator has authority to create the given message and send it to the specified dissemination channels; and (3) it validates, parses and analyzes the message to ensure it is compliant with CAP1.2 and appropriate for the specified dissemination channels (*i.e.*, WEA, EAS, and/or Internet-based platforms IPAWS serves). While the amount of processing time in authentication and authorization process in steps 1 and 2 of the IPAWS Aggregator may be typically constant, the processing time in step 3 could vary based on the content of the CAP message. For instance, the number of different dissemination channels specified (WEA alone, or WEA and EAS, or WEA, EAS and Internet), type of geo-targeting (FIPS specification, polygons or circle specification), presence of multi-media files (none, audio, or audio/video), and the presence of URLs could significantly affect the processing time in the IPAWS OPEN.<sup>1</sup>

Upon completion of the above functions, the IPAWS Aggregator forwards the alert message (via the B-interface in WEA) to the IPAWS Gateways. As the IPAWS Gateways and IPAWS Aggregator are collocated, there is no significant transmission time.

#### **IPAWS Gateway:**

The IPAWS Gateway processes the alert messages differently, depending on whether the alerting dissemination channel over which they are intended to be distributed will be WEA, the EAS, or alerts delivered over the IPAWS Public Feed.

For the EAS and miscellaneous Internet-based platforms, the IPAWS Gateway validates and queues the alert messages, then forwards the messages to the appropriate EAS and IPAWS Internet feeds, providing capabilities for the receiving entities to poll these feeds to receive updates. Typical processing times associated with posting alert messages to the Internet feeds were not available at the time of this white paper but should be negligible based on IPAWS architecture.

For WEA alerts, the IPAWS Gateway validates the received alert messages and maintains a log of alert messages received from the alert aggregator and delivered to and rejected by the CMSP Gateway. The IPAWS Gateway also implements and supports pre-defined 'service profiles' specifying alert message formats containing information elements required by CMSPs for the delivery of alert messages to wireless devices. The IPAWS Gateway also stores CMSPs' profiles including the CMSP election within a specific service area, supported technologies including any associated service profiles, characteristics, restrictions, limitations, or parameters. Furthermore, the IPAWS Gateway converts the alert message

---

<sup>1</sup> FIPS county codes are five-digit codes that uniquely identify counties and county equivalents in the United States and certain U.S. possessions.

from CAP to CMAC (Commercial Mobile Alert Reference Point C) format and forwards (or pushes) the message to the various CMSPs' Gateways<sup>2</sup>.

One potential source of unexpected and random processing time is potential queuing at the IPAWS Gateway due to simultaneous arrival of more than one WEA alert message at the gateway. Currently, the IPAWS Gateway is required to transmit Presidential Alerts immediately upon receipt. Presidential Alerts preempt all other Alert Messages. Further, Imminent Threat Alerts and AMBER Alerts are treated based on a "First In, First Out" (FIFO) queuing mechanism. If EEWs are defined as Imminent Threats, it is possible that an EEW may arrive while there are other alert messages to be processed, and get queued for an indeterminate time as a result.

In the *EEW Public Notice*, the Bureau sought comments on the IPAWS Aggregator and Gateway processing time.<sup>3</sup> Data provided by FEMA indicates that the average processing time incurred within IPAWS is 1.667 seconds, the best case processing time is 0.691 seconds,<sup>4</sup> and the processing time in 95% of all cases is less than two seconds.<sup>5</sup> Notwithstanding that CTIA asserts that the processing time associated with IPAWS "greatly exceed[s] three seconds,"<sup>6</sup> we use FEMA's data-supported average and values for 95% of instances for our analyses.

---

<sup>2</sup> This is performed over the C-interface for WEA.

<sup>3</sup> *EEW Public Notice*, 31 FCC Rcd at 3462.

<sup>4</sup> FEMA Comments at 1.

<sup>5</sup> *Id.* at 3.

<sup>6</sup> CTIA Comments at 5.



## APPENDIX D

### Functions and Latencies in Wireless Emergency Alerts

The Commission does not mandate a particular technology for the delivery of WEA.<sup>1</sup> However, the primary technology used for the distribution of WEA is cell broadcasting, a point-to-multipoint technology that allows geo-targeted alerts to be delivered to all compliant handsets in an emergency area in a way that does not use or depend on point-to-point architecture used for voice calls and text messages. The cell broadcasting standards that apply to WEA, and which we will be using as the basis for our analysis in this white paper, are premised on 3G/UMTS and 4G/LTE technologies.<sup>2</sup>

The earthquake alert message from the IPAWS OPEN will be delivered to the Participating CMS Provider's Alert Gateway (CMSP Gateway). The alert message will then be transferred through several nodes as depicted in Figure D1 below—to the Cell Broadcast Center (CBC), the Radio Network Controller (RNC)/Mobility Management Entity (MME), NodeB (NB)/eNodeB (eNB), and ultimately delivered and displayed on the user's device.<sup>3</sup> While some of the elements in this architecture may be physically collocated and experience no added transfer time (e.g. CBE and CBC), sources of added processing time can be observed throughout this architecture.

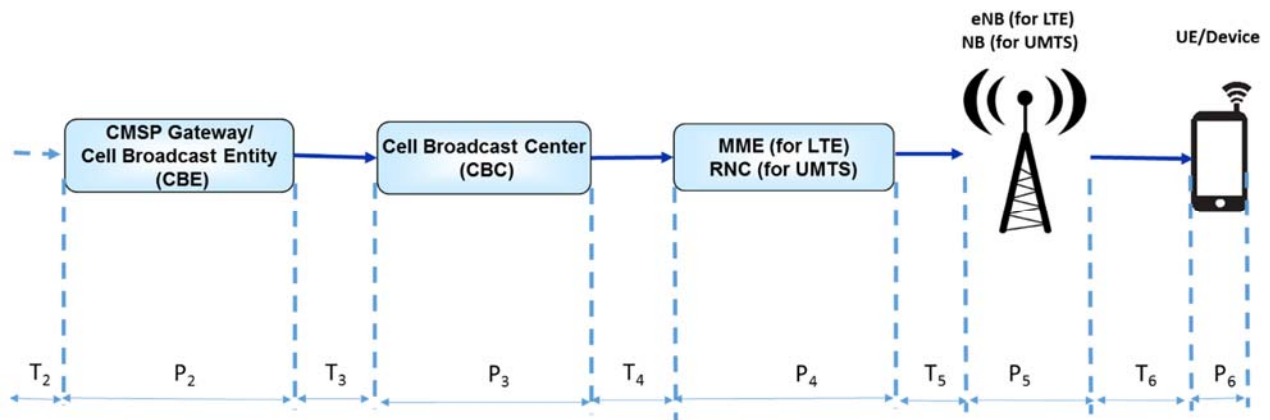


Figure D1 – WEA Message Delivery - Network Architecture

(“T” stands for the Transmission time and “P” for the Processing time)

Currently, there are three Classes of Alerts in WEA: Presidential, Imminent Threat, and AMBER. CAP alert messages provides a field for each event type (“Event Code”). The event code for the Presidential and AMBER Alerts are EAN and CAE, respectively. Imminent Threat Alerts are based on the CAP

<sup>1</sup> See 3GPP TS 23.041; 3GPP TS 22.268, 3GPP TS 29.168, 3GPP TS 36.413, 3GPP TS 36.331, 3GPP TS 23.401, ATIS-TIA J-STD-101, and ATIS-TIA J-STD-101.

<sup>2</sup> 2G/GSM and cdma2000 (1xRTT/EVDO) networks will not be considered in this white paper as the technical bars to a three second alert over these networks is significant, and they will be retired in the near future. See AT&T *ex parte* at 1.

<sup>3</sup> The network architectures for the WEA and the ETWS are specified by the 3GPP. 3GPP TS 23.041. The interfaces between MME and eNB (S1-MME), RNC and NB (Iub), CBC and MME (SBc) and CBC and RNC (IuBc) are defined in the 3GPP Standards and have certain latency requirements.

elements of Urgency, Severity, and Certainty and may use various event codes.<sup>4</sup> Currently, the Earthquake Alert is defined as part of the Imminent Threat Alert messaging and has the event code “EQW.” While presently under consideration for expansion to 360 characters, current WEA rules limit alert message length is limited to 90 characters and alert messages are delivered only when the WEA-capable user device is turned on and is in the idle mode (not in the middle of a voice call and/or a data session).<sup>5</sup>

### **EEW Alert Transmission from IPAWS to WEA:**

After the IPAWS Gateway prepares the WEA alert message for delivery to the Participating CMS Provider by converting to the Commercial Mobile Alert for C-Interface (CMAC) format, the WEA alert message is then disseminated across a secure Internet-based interface (the C-Interface) to the CMSP Gateway for distribution to mobile customers over cell broadcast (CMSP Infrastructure).<sup>6</sup>

For the WEA, IPAWS Gateway forwards (“pushes”) the CMAC to the CMSP Gateway via the C-interface. The data transmission between IPAWS Gateways and the CMSP Gateways are typically via secure VPN connections. The connection setup is typically done once and prior to the transmission of the actual EEW alert message, therefore the connection setup time will be ignored. Depending on the distance and the specific type of the transmission medium, the maximum transmission time would be typically less than 50 ms.<sup>7</sup>

### **Functions Performed in the CMSP Network:**

The CMSP Gateway receives alerts from the IPAWS via the C-interface processes them through various nodes, each of which contributes to the end-to-end transmission and processing time, until the alert is delivered and displayed at the device. Some of functions performed by the CMSP Gateway include authentication of connection to the IPAWS, validation of message integrity and determination of alerting parameters. The most notable function performed by the CBC is the mapping of the alert geo-target area to the set of corresponding broadcast cell sites in the CMS providers. RNC and MME manage the transmission of the alerts through the UMTS and LTE networks. The base stations (eNB/NB) are responsible for the scheduling of the alerts over the broadcast channels. To save battery life, the handheld

---

<sup>4</sup> 47 CFR § 10.400(b). 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). 47 CFR § 10.400(b)(1). 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). 47 CFR § 10.400(b)(2). 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). 47 CFR § 10.400(b)(3).

<sup>5</sup> See *Improving Wireless Emergency Alerts and Community-Initiated Alerting*, Notice of Proposed Rulemaking, 30 FCC Rcd 13781 (2015).

<sup>6</sup> Within the CMSP infrastructure, the WEA alert message is routed from the Participating CMS Provider’s (or TPP’s) Alert Gateway to the CMSP’s base stations (the D-Interface), which transmit the alert message to subscriber (and roaming) devices (the E-Interface). The WEA system currently deployed by FEMA and Participating CMS Providers is based on standards created by the Alliance for Telecommunications Industry Solutions (ATIS), the Telecommunications Industry Association (TIA) (jointly, ATIS/TIA), and the 3rd Generation Partnership Project (3GPP). See CSRIC IV, Working Group Two, Wireless Emergency Alerts, Geo-targeting, Message Content and Character Limitation Subcommittee, *Final Report*, at 7 (2014), [https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_CMAS\\_Geo-Target\\_Msg\\_Content\\_Msg\\_Len\\_Rpt\\_Final.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_CMAS_Geo-Target_Msg_Content_Msg_Len_Rpt_Final.pdf) (last visited Jun. 9, 2015) (CSRIC IV WEA Messaging Report).

<sup>7</sup> See Appendix C, note 8.

device operates in the Discontinuous Reception (DRX) mode composed of an “off” or sleep period followed by a short awake or “on” period. Since the earthquake alerts may arrive at any time, the device will be notified via the paging channel about the arrival of the alert, scheduled to occur during the “On” portion of the DRX cycle.

### **CMSP Gateway/CBE:**

The CMSP Gateway is interconnected to the Alert Gateway via the C-interface. In 3GPP architecture for Cell Broadcast, the Cell Broadcast Entity (CBE) could be the CMSP Gateway, a commercial service entity, or an entity which performs both functions. CMSP Gateway/CBE performs a number of functions including: Authentication of interactions with the Alert Gateway, provide security mechanisms such as firewall, keeps the interface connection alive, validate message integrity and alerting parameters and responding with an error message to the Alert Gateway if the validations fail, define the frequency and duration of the retransmissions of alert messages, support a mechanism to handle congestion, and provides the CBC with the geo-target information (e.g., geo-code, polygon, circle) associated with the alert message.

Currently, the CMSP Gateway processes the alert messages in a First In-First Out (FIFO) queuing method, except for a Presidential-level alert which is immediately moved to the top of the queue and processed before all other non-Presidential alerts. It is clear that in the unlikely event that several non-Presidential alert messages, including the Earthquake alert, arrive together simultaneously, the FIFO queuing mechanism would introduce a random amount of delay before the Earthquake alert message is processed.

The interface between CBE and CBC is specified by ATIS<sup>8</sup>. The CMSP Gateway/CBE forwards alert messages to the CBC for further processing and delivery to the end user WEA-capable devices.

### **Cell Broadcast Center (CBC):**

The Cell Broadcast Center (CBC), which is the information distribution center, is typically part of the CMSP core network and may be connected to several CBEs. The CBC performs several functions<sup>9</sup> including determining the set of cells to which a CBS message should be broadcast based on the geo-target area, the time at which an alert message should commence being broadcast, the time at which alert message should cease being broadcast, and the period at which broadcast of an alert message should be repeated. Additionally, the CBC has the capability to adjust the CBE-requested retransmission frequency and duration depending on network conditions or operator policy.

The CBC may be connected to several RNCs for the UMTS and MMEs for the LTE networks. The MME acts as a load balancer for the CBC, the function that is performed by RNC in the UMTS network, and reduces the processing time at the CBC.

The 3GPP has defined a mandatory protocol between the CBC and the RNC in 3GPP TS 25.419, and between the CBC and the MME in 3GPP TS 29.168.

---

<sup>8</sup> ATIS-0700008, *Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification*; March 2010.

<sup>9</sup> 3GPP TS 23.041

## Radio Network Controller (RNC)/Mobility Management Entity (MME) & NodeB (NB)/eNodeB (eNB):

The Radio Network Controller (RNC) interfaces to only one CBC, whereas the MME may interface to one CBC or multiple CBCs. The RNC and the MME are mainly responsible for interpretation of commands from the CBC, storages of messages from the CBC, providing to the CBC acknowledgement of successful execution of commands received from the CBC, reporting to the CBC failure when a command received from the CBC is not understood or cannot be executed, and routing of alert messages to the appropriate distribution area (NodeBs (NBs) for UMTS and eNodeBs (eNBs) or possibly eNBs in the indicated Tracking Areas for LTE).

For UMTS, WEA messages are received by CMPS gateway and are transmitted to target coverage areas using UMTS Cell Broadcast Service (CBS), without any modification to the 3GPP-defined CBS.

The message flow for WEA distribution in UMTS is shown in Figure D2 below. The end user is notified about the alert message via *Paging Message* and subsequent *System Information Change Message*. The actual alert is delivered via *CBS (Alert) Message*.

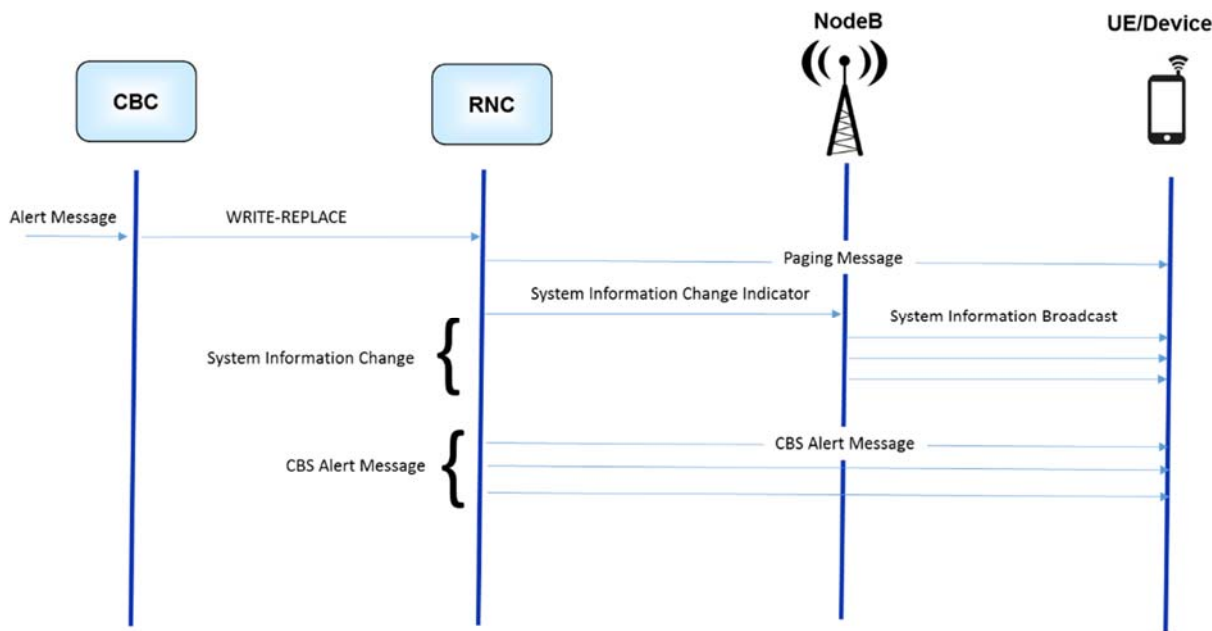


Figure D2 – WEA Message Distribution in UMTS

The message flow for WEA distribution in LTE is shown in Figure D3 below.<sup>10</sup> WEA notification can occur at any point in time. For LTE, the *Paging* message is used to inform WEA-capable UEs about presence of one or more WEA notifications. When the UE receives a *Paging* message including the *WEA-Indication*, it starts receiving the WEA notifications according to *SchedulingInfoList* contained in *SystemInfoBlockType1*. WEA notification is contained in the *SystemInformationBlockType12* (SIB-12).

<sup>10</sup> 3GPP TS 36.331 V13.1.0 (2016-03)

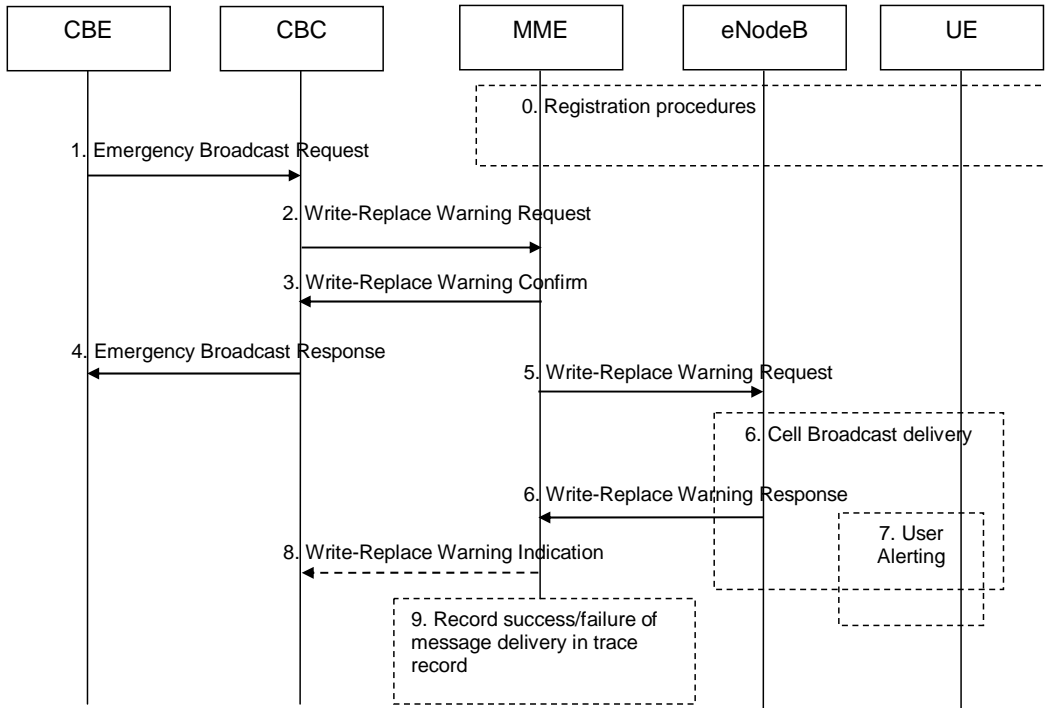


Figure. D3 – WEA Message Distribution in LTE

**Mobile Device/UE:**

Following are some of the alert related functions that the UE/Device performs:<sup>11</sup> Detecting duplicate messages, discarding alerts not in a suitable data coding scheme, entering Discontinues Reception (DRX) mode based upon received Schedule Message, providing user ability to activate/deactivate alerts through Man-Machine Interface (MMI), and providing test capabilities.

The requirements for the mobile device behavior upon the receipt of WEA alert message is defined in the J-STD-100.<sup>12</sup> The mobile device monitors associated channel or channels for alerts. Distribution of the alert messages to the CMSP’s subscribers is unidirectional from the CMSP network to the mobile device of the subscriber, without any acknowledgement from the mobile device.

While the 3G UMTS technology allows alert delivery only during the *Idle* mode, the LTE cell broadcast technologies provide alert message delivery capability during both the idle mode and the connected mode. Currently, per the FCC requirements, WEA-capable mobile devices will be receiving the alert messages *only* in the idle mode (when the mobile device is on and not on an active voice call or in a data session). And currently, WEA messages are limited to 90 characters (one Message Page).

<sup>11</sup> 3GPP TS 23.041

<sup>12</sup> Joint ATIS/TIA CMAS Mobile Device Behavior Specification (ATIS-TIA-J-STD-100)

## Processing Time Associated With Transmitting an EEW Alert via WEA:

As depicted in Figure D1, the total alert delay from the arrival of the alert message at the CMSP-GW to the alert delivery on the device, is composed of the following delay components: P<sub>2</sub>, T<sub>3</sub>, P<sub>3</sub>, T<sub>4</sub>, P<sub>4</sub>, T<sub>5</sub>, P<sub>5</sub>, T<sub>6</sub> and P<sub>6</sub>. Typically CMSP-GW/CBE and CBC are collocated, and the main source of delay comes from the CBC performing the mapping of the geo-target area into the corresponding broadcast cell sites. It is desired to keep the geo-target area as precisely defined as possible to avoid over alerting stress, while not under-delivering alerts. The processing delay incurred in the mapping will be directly related to how the geo-target area is specified and the accuracy of this mapping. Currently, per the FCC, the minimum requirement for specifying the geo-target area is at the county-level resolution by using the FIPs codes. Given that for each CMS provider, the set of cell sites in a given county can be determined *a priori* and saved in the database, the mapping (i.e., the database lookup) can typically be performed very quickly, contributing negligible delay.

We recommend that for EEW, the alert originator specify the geo-target area in a FIPS code, and when advanced mapping products that can deliver more precise geo-targeting with very low processing delays for mapping become commercially available, use the more precise geo-targeting products. We note that Comtech/TCS currently provides mapping products that performs geo-target area to RF coverage area matching. Its current product provides 100 ms per 10,000 cell site mapping delay performance<sup>13</sup>. Given that earthquake coverage area is *not* nationwide and is usually within a given area or state such as California or Oregon, it suffices to consider the given area or state for the purpose of geo-target mapping process<sup>14</sup>. Conservatively, we budget 100 ms of delay for the geotarget area to cell site mapping purpose.

The interfaces between MME and eNB (S1-MME), RNC and NB (Iub), CBC and MME (SBc) and CBC and RNC (IuBc) are defined in the 3GPP Standards and have certain latency requirements.<sup>15</sup> For instance, the S1-MME delay is required to be less than 50 ms. The connections between CMSP-GW/CBE and CBC, CBC and MME/RNC, and MME/RNC and NB/eNB are typically SLA-based managed *private* IP connections with low delays and low delay tolerances, which enable *rapid delivery*.<sup>16</sup> Accordingly, we observe that conservatively one can consider a 250 ms delay budget for the above collective delays, excluding the delays in the eNB/NB (T<sub>6</sub>) and device/UE (P<sub>6</sub>).<sup>17</sup>

One potential source of unexpected and *random* delay is the potential queuing delay at the CMSP-GW due to simultaneous arrival of more than one WEA alert message at the gateway. Currently, a participating CMSP is required to transmit Presidential Alerts immediately upon receipt. Presidential Alerts preempt all other Alert Messages. A Participating CMS Provider is required to transmit Imminent Threat Alerts and AMBER Alerts on a First In-First Out (FIFO) basis.

---

<sup>13</sup> See Comtech/TCS *ex parte* filing, PS Docket 16-32.

<sup>14</sup> We observe that in the USGS Study, “Magnitude vs Intensity: Northridge earthquake of January 17, 1994 with the magnitude of 6.7M”, by Lisa Wald & Wendy Shindel, July 2004, the area with “intensity of V or higher” damage was approximately 6,000 square miles.

<sup>15</sup> See 3GPP TR 25.913.

<sup>16</sup> Verizon *ex parte* filing, July 11, 2016, PS Docket 16-32

<sup>17</sup> [http://www.verizonenterprise.com/external/service\\_guide/reg/cp\\_pip\\_plus\\_sla.pdf](http://www.verizonenterprise.com/external/service_guide/reg/cp_pip_plus_sla.pdf), and FCC documents “Measuring Broadband America” Report and “Measuring Latency Discussion” ....

Prioritizing EEW alerts at the CMSP-GW potentially could eliminate this random queuing delay for time critical EEW alerts.<sup>18</sup> This is technically feasible since WEA currently allows the prioritization of the Presidential Alerts. ATIS agrees that the alert prioritization is technically feasible and states that "... it should be technically possible to prioritize these alerts (similar to the prioritization of Presidential Alerts ...)"<sup>19</sup>. Additionally, we believe that the mechanism by which the Presidential alerts are prioritized can also be used to prioritize the Earthquake alerts. We believe that Earthquake alerts should have the highest priority among all WEA alerts, including all Imminent Threat Alerts and Amber Alerts, except the Presidential Alerts. We further recommend to implement the prioritization of EEW alerts through WEA by using the existing "event code" ("EQW") for the earthquake.

The significant delays through the CMSP alert delivery chain occur at the eNB/NB ( $T_6$ ) and in the UE/device ( $P_6$ ).

### **LTE eNodeB Transmission Delay<sup>20</sup>:**

For LTE, the alert message to be broadcast is delivered via MMEs to the appropriate eNBs and the corresponding cells in the specified geo-targeted area. The eNBs are responsible for *scheduling* of the broadcast of the alert message and the repetitions in each cell.

WEA notification can occur at any point in time. For LTE, the *Paging* message is used to inform WEA-capable UEs about presence of one or more WEA notifications. When the UE receives a Paging Messaging including the WEA-Indication, it starts receiving the WEA notifications according to *SchedulingInfoList* contained in *SystemInfoBlockType1*. The actual WEA message is contained in the *SystemInformationBlockType12* (SIB-12). SIB-12 can carry multiple (up to 64) message segments, and each segment can carry certain number of bits.

A short Earthquake alert message (less than 90 characters) would minimize delay, as it requires only one SIB-12 message segment. Per the 3GPP TS 36.331, the maximum number of bits allowed by the physical layer that can be carried inside one segment of SIB-12, depending on the various Downlink Control Information (DCI) formats, maximum number of bits is at least 1736 bits, or 217 bytes, or 248 7-bit characters.

In LTE, the SIB-12 messages are transmitted with a CMSP defined periodicity (pre-configured at the eNB) which can take any of the following values: 80 ms, 160 ms, 320 ms, 640 ms, 1.28 s, 2.56 s and 5.12 s. Per ATIS report,<sup>21</sup> this figure is typically set at 320 ms. Therefore, with the typical CMSP setting, the SIB-12 related transmission delay is 320 ms.

Given the unknown and unpredictable RF channel conditions, it is possible that on rare occasions SIB-12 message may not be received successfully by the UE. In those situations, the UE will receive the SIB-12 in its next repetition, during the repetition period. This would introduce an additional delay of 320 ms. Thus  $T_6$ , in Figure D1, would normally be 320 ms, and with additional delay, 640 ms.

---

<sup>18</sup> Our recommendation is in line with queuing prioritization recommended by the Homeland Security Science & Technology in its Report "*Wireless Emergency Alerts – System Enhancement Recommendations*," July 2013.

<sup>19</sup> ATIS ex parte filing, PS Docket 16-32, July 19, 2016

<sup>20</sup> WEA messages for LTE networks are carried on SIB-12, on the "Control Plane". QCI are part of "User Plane".

<sup>21</sup> ATIS Feasibility Study For LTE WEA Message Length, ATIS-0700023.

We recommend that SIB-12 frequency can be set at the minimum setting value of 80 ms, which would minimize the  $T_6$  delay. If allowing one extra SIB-12 period to cover bad channel conditions, the corresponding total delay,  $T_6$ , would be 160 ms.

### **UMTS Transmission Delay:**

For the UMTS, the mobile device in the alert geo-targeted area will be notified about the WEA alert via the Paging message. Device will also receive the *System Information Change* message and the actual alert message will be delivered on the CTCH (Common Traffic Channel) logical channel. The minimum period with which a CBS message (the Secondary notification) may be broadcast over the air interface is a period of 1 second<sup>22</sup>. In case of poor RF channel condition, the CBS message may be received in the next broadcast period. This would add an additional delay of 1 second, and the corresponding total delay,  $T_6$ , would be 2 seconds.

### **Device Delay:**

For LTE, once the WEA alert arrives at the UE, assuming that the UE is in the *Idle* mode, the UE will be in the *Paging DRX Cycle*, in order to save battery power. DRX Cycle is composed of a short “on” period, where the device wakes up to check to see if it is paged during its specific Paging Frame and Paging Occasion. If it is not paged, then will go through another paging DRX cycle. But if it is paged, then it checks for System Information Change Message and if there are any alerts, it would be directed to SIB-12. The UE will decode and receive the WEA alert.

The paging DRX cycle setting is a tradeoff between saving battery power and latency.<sup>23</sup> Since WEA notification may arrive anytime, possibly during the “off” period of the paging DRX cycle, the device will not become aware of the WEA notification until the next “on” period. This would introduce, for the worst case, a delay amount equal to the paging DRX cycle time, and on the average, half of that time<sup>24</sup>. The Paging DRX Cycle can be configured to be 320 ms, 640 ms, 1.28 s and 2.56 s, and is typically set at 1.28 s<sup>25</sup>. Since the device processing time is typically very small, in the order of 10s of ms, therefore, the total worst case delay incurred in the UE,  $P_6$ , based on the typical settings, would be around 1.28 s, and on the average around 640 ms.

For UMTS, the UE up on receipt of the Paging Message, will receive the System Information Change message and the actual alert (CBS message) on the CTCH logical channel. The expected delay here would be for the worst case, the Paging DRX cycle time, and on the average, half of this time. Assuming typical DRX cycle period of 1.28 s<sup>26</sup>, the worst case delay introduced would be 1.28 s, and on the average 640 ms.

---

<sup>22</sup> See 3GPP TS 23.041 V13.2.0 (2015-12)

<sup>23</sup> Paging DRX Cycle can be set at the UE (Device) and by the network. In operation, the minimum of the two values is used.

<sup>24</sup> It is a well-known statistical fact that the mean (average) of a uniform random variable is its middle point. More specifically, if the uniform random quantity takes on a value between  $a$  and  $b$ , its mean value will be  $(a+b)/2$ , and its variance will be  $(b-a)^2/12$ .

<sup>25</sup> Based on our discussion with UE vendors. Also, see “*Impact of SIB Scheduling on the Standby Battery Life of Mobile Devices in UMTS*,” A. Catovic *et. al.*

<sup>26</sup> *Id*



**Total WEA end-to-end processing and transmission time:**

The transmission and processing times for WEA are summarized in Tables D1 and Table D2 below for various scenarios. In these scenarios a number of parameter values are common across all scenarios and do not change. These values are 50 ms for T<sub>1</sub>, 50 ms for T<sub>2</sub>, and 250 ms for the total of P<sub>2</sub>, T<sub>3</sub>, P<sub>3</sub>, T<sub>4</sub>, P<sub>4</sub>, T<sub>5</sub>, and P<sub>5</sub>.

**The Conservative Case for WEA** refers to the case in which the processing time for IPAWS (P1) is a conservative value of 2 seconds (95 percentile value), the Paging DRX cycle values is 1.28 seconds, eNB transmission time for LTE is 640 ms (320 ms, with one additional retransmission), and NB transmission time for UMTS is 2 seconds (1 second with one additional retransmission).

**The Average Case for WEA** refers to the case in which the processing time for IPAWS (P1) is the current average value of 1.667 seconds, the Paging DRX cycle values is 640 ms (half of 1.28 seconds), eNB transmission time for LTE is 640 ms (320 ms, with one additional retransmission), and NB transmission time for UMTS is 2 seconds (1 second with one additional retransmission).

While the scenarios above are based on data provided by FEMA and various other sources, in addition to the optimization ideas mentioned throughout the white paper, we recommended optimizing the processing time in IPAWS to 900 ms, and the SIB-12 transmission time to 80 ms. The corresponding new scenarios are created as follows.

**The Conservative Case improved by WEA optimizations**, refers to the case in which the processing time for IPAWS (P1) is the improved value of 900 ms, the Paging DRX cycle values is 1.28 second, eNB transmission time for LTE is 160 ms (80 ms with one additional retransmission), and NB transmission time for UMTS is 2 seconds (1 second, with one additional retransmission).

**The Average Case improved by WEA optimizations** refers to the case in which the processing time for IPAWS (P1) is the improved value of 750 ms, the Paging DRX cycle values is 640 ms (half of 1.28 seconds), eNB transmission time for LTE is 160 ms (80 ms with one additional retransmission), and NB transmission time for UMTS is 2 seconds (1 second, with one additional retransmission).

These scenarios with corresponding parameter values are summarized in Table D1 below.

**Table D1 – Summary of transmission and processing time for different scenarios (in ms)**

	Conservative	Average	Conservative with optimizations	Average with optimizations
<b>P1 (IPAWS)</b>	2000	1667	900	750
<b>P6 (DRX)</b>	1280	640	1280	640
<b>T6 (eNB TX) for LTE</b>	640	640	160	160
<b>T6 (NB TX) for UMTS</b>	2000	2000	2000	2000

**Table D2 – WEA End-to-End Transmission and Processing Time Summary (in ms)**

<b>Technology</b>	<b>Conservative</b>	<b>Average</b>	<b>Conservative with optimizations</b>	<b>Average with optimizations</b>
<b>LTE</b>	4270	3297	2690	1900
<b>UMTS</b>	5630	4657	4530	3740

In summary, our analysis indicates that for LTE, currently WEA allows EEW to be delivered with an end-to-end transmission and processing time, including processing time introduced by IPAWS processes, of 3.30 second to 4.27 seconds. Currently, WEA for LTE provides CMSP-related (*i.e.*, CMSP Gateway to device) transmission and processing times of 1.53 seconds to 2.17 seconds. For UMTS, WEA currently allows EEW to be delivered with an end-to-end transmission and processing time, including processing time introduced by IPAWS, of 4.66 second to 5.63 seconds.

## APPENDIX E

### Earthquake and Tsunami Warning System (ETWS)

Earthquake and Tsunami Warning System (ETWS) is a 3GPP Standard based warning system, originally initiated by Japan. The original ETWS technical specification was for UMTS and part of the 3GPP Release-8. Subsequently, ETWS technical specifications for LTE was released. ETWS is designed to accommodate two basic types of Earthquake and Tsunami related alert messages: 1) The primary notification, which contains minimum, most urgently required information such as “An Earthquake Occurred”; and 2) the secondary notification, including supplementary information not contained in the Primary notification, such as seismic intensity, epicenter, etc. The original ETWS has the basic requirement that the Primary notification be delivered within 4 seconds to the UE in the notification area where the warning notification is expected to be distributed even under congestion situation<sup>1</sup>.

#### 1. Network Architecture

The ETWS platform, along with WEA, is designed based on the Cell Broadcast Service (CBS) and has the same CMSP network architecture as WEA, depicted in Figures D1, D2 and D3. Currently, ETWS is deployed in Japan and directly connects the alert originator JMA (Japan Metrological Agency) to the CMSP Gateway, without passing through an entity similar to the IPAWS OPEN. For the U.S., the ETWS can potentially be deployed similar to WEA, with the appropriate modifications (discussed below).

#### 2. How Does ETWS Work

For LTE, the alert message to be broadcast is delivered to the CMSP Gateway/CBE and traverses through the CBC and the MME to reach to the appropriate eNBs and the corresponding cells in the specified geo-targeted area. The eNBs are responsible for *scheduling* of the broadcast of the alert message and the repetitions in each cell.

ETWS notification can occur at any point in time. For LTE, the *Paging* message is used to inform ETWS-capable UEs about presence of ETWS notifications. The *SystemInfoBlockType10* (SIB-10) is used to carry the Primary notification, which only carries the Warning Type (i.e., Earthquake, Tsunami, or Earthquake-Tsunami, etc.) The Secondary notification, if present, is carried via *SystemInfoBlockType11* (SIB-11) and carries the supplemental message. SIB 10 and SIB 11 have similar Periodicity and Reputation frequency as SIB-12, discussed earlier for the WEA.

For UMTS, similarly, the alert message to be broadcast is delivered to the CMSP Gateway/CBE and traverses through the CBC and the RNC to reach to the appropriate BTS. The mobile device in the alert geo-targeted area will be notified about the ETWS alert via the *Paging* message. The *Paging* message also carries the Primary notification (i.e., the Warning Type). The mobile device will also receive the *System Information Change* message and the actual Secondary notification, if present, on the CTCH (Common Traffic Channel) logical channel.

---

<sup>1</sup> See 3GPP TS 22.168 V8.1.0 (2008-06).

### 3. ETWS Delay Analysis

Given the similar architecture for the alert delivery up to the eNB/NB for the ETWS and WEA, the corresponding delay analysis would apply and provide the same delay budget. More specifically, as discussed in the WEA delay section above, the total delay between the CMSP-GW/CBE and the NB/eNB is expected to be around 250 ms.

For LTE, since the ETWS notification can occur at any point in time, the *Paging* message is used to inform ETWS-capable UEs about the presence of ETWS notifications. When the UE receives a Paging Messaging including the ETWS-Indication, it starts receiving the ETWS notifications according to *SchedulingInfoList* contained in *SystemInfoBlockType1*. The ETWS Primary notification is contained in the SIB-10, and the Secondary notification, if present, in the SIB-11.

Similar to the SIB-12 for WEA, the SIB-10 and SIB-11 messages are transmitted with a CMSP defined periodicity (pre-configured at the eNB) which can take any of the following values: 80 ms, 160 ms, 320 ms, 640 ms, 1.28 s, 2.56 s and 5.12 s.

The delay analysis for WEA using SIB-12 would similarly apply for the ETWS using SIB-10 and SIB-11. For example, setting the SIB-10 and SIB-11 frequency at the minimum setting value of 80 ms would minimize the  $T_6$  delay for the ETWS. If allowing one extra SIB-10/11 period to cover bad channel conditions, the corresponding total delay,  $T_6$ , would be 160 ms.

For LTE, once the ETWS alert arrives at the UE, assuming that the UE is in the *Idle* mode, the UE will be in the *Paging DRX Cycle*, in order to save battery power. If it is paged, then it checks for *System Information Change* Message and if there are any alerts, it would be directed to SIB-10/11. The UE will decode and receive the ETWS Primary, and the Secondary notification, if present. The Paging DRX Cycle can be configured to be 320 ms, 640 ms, 1.28 seconds and 2.56 seconds, and is typically set at the value of 1.28 seconds<sup>2</sup>. Since the device processing time is typically very small, in the order of 10s of ms, the total worst case delay incurred in the UE,  $P_6$ , based on the typical settings, would be around 1.28 s, and on the average around 640 ms.

For UMTS, the mobile device in the alert geo-targeted area will be notified about the ETWS alert via the Paging message. The Primary notification, i.e., the Warning Type, is part of the Paging message. Device will also receive the *System Information Change* message and the actual alert message, the Secondary notification, if present, will be delivered on the CTCH (Common Traffic Channel) logical channel. The Primary notification is guaranteed to be delivered to the device within 4 seconds from the time of delivery to the CMSP gateway. And, the minimum period with which a CBS message (the Secondary notification) may be broadcast over the air interface is a period of 1 second<sup>3</sup>. In case of poor RF channel condition, the CBS message may be received in the next broadcast period. This would add an additional delay of 1 second, and the corresponding total delay,  $T_6$ , would be 2 seconds.

For UMTS, by including the Warning Type in the paging message, the device up on receipt of the Paging message during the next DRX cycle “on” time, will pop up the stored appropriate alert message and generate the appropriate alert sound/cadence (based on the Warning Type). The expected delay here would be for the worst case, the Paging DRX cycle time, and on the average, half of this time. Assuming

---

<sup>2</sup> Based on our discussion with UE vendors. Also, see “*Impact of SIB Scheduling on the Standby Battery Life of Mobile Devices in UMTS*,” A. Catovic et. al.

<sup>3</sup> See 3GPP TS 23.041 V13.2.0 (2015-12)

typical DRX cycle period of 1.28 seconds<sup>4</sup>, the worst case delay introduced here would be 1.28 seconds, and on the average 640 ms.

#### 4. Summary of ETWS Delays

Based on the end-to-end Earthquake Alert delivery delay analysis performed above, the delays for ETWS are summarized in Tables E1 and Table E2 below for various scenarios. In these scenarios a number of parameter values are common across all scenarios and do not change. These values are 50 ms for T<sub>1</sub>, 50 ms for T<sub>2</sub>, and 250 ms for the total of P<sub>2</sub>, T<sub>3</sub>, P<sub>3</sub>, T<sub>4</sub>, P<sub>4</sub>, T<sub>5</sub>, and P<sub>5</sub>.

For ETWS, the scenarios we consider here are only those we recommend based on the optimum standard configurations, since we are not informed about the operational values in the field.

**The Conservative Case with recommended values for ETWS**, refers to the case in which the processing delay for IPAWS (P1) is the improved value of 900 ms, the Paging DRX cycle values is 1.28 seconds, eNB transmission delay for LTE is 160 ms (80 ms with one additional retransmission), and NB transmission delay for UMTS is 0 second.

**The Average Case with recommended values for ETWS**, refers to the case in which the processing delay for IPAWS (P1) is the improved value of 750 ms, the Paging DRX cycle values is 640 ms (half of 1.28 seconds), eNB transmission delay for LTE is 160 ms (80 ms with one additional retransmission), and NB transmission delay for UMTS is 0 second.

These scenarios with corresponding parameter values are summarized in Table E1 below.

**Table E1 – Summary of parameter values for different scenarios (in ms)**

	Conservative with Improved Values	Average with Improved Values
<b>P1 (IPAWS Delay)</b>	900	750
<b>P6 (DRX Delay)</b>	1280	640
<b>T6 (eNB TX Delay) for LTE</b>	160	160
<b>T6 (NB TX Delay) for UMTS</b>	0	0

---

<sup>4</sup> *Id*

**Table E2 – ETWS End-to-End Delay Summary (in ms)**

<b>Technology</b>	<b>Conservative (with Recommended values)</b>	<b>Average (with Recommended values)</b>
<b>LTE</b>	2690	1900
<b>UMTS</b>	2530	1740

Given that ETWS for UMTS could provide end-to-end delay, including the delay caused by IPAWS, of 1.74 to 2.53 seconds, our recommendation is that if the WEA delays over UMTS are not acceptable, the ETWS “dual-stack” solution be deployed, where Earthquake Alerts are delivered via ETWS and other types of alerts are delivered through WEA.

**5. “Dual-Stack” (Patch) WEA and ETWS & Impact of IPAWS OPEN**

One possible solution to address potential delay issues for the Earthquake alert message delivery is to consider deploying a dual-stack solution, where Earthquake alert messages are delivered via ETWS and the other alert messages are delivered via WEA. To provide such capability the following changes need to be made.

Currently for WEA, the C-interface is defined between the IPAWS and the CMPS-GW to provide alerts to the CMSP-GW in CMAC format. ETWS alerts are delivered to the CMSP-GW, potentially, through a different interface defined by Japan. In using IPAWS to deliver the ETWS alerts, FEMA may need to introduce the proper software to convert Earthquake CAP alert to the format needed to be carried over this new interface and be delivered to the ETWS (port) of the CMSP-GW. It is also necessary that the CMSP-GW supports this new interface.

Furthermore, the network equipment (CMSP-GW, CBC, etc.) and the device have to be upgraded to support both WEA and ETWS. The devices, including the field devices, can be upgraded by “possible software update mechanisms to receive WEA and EWTS messages”<sup>5</sup>.

**APPENDIX F**

**Functions and Latencies in the Emergency Alert System (EAS)**

The EAS is a broadcast-based, hierarchical alert message distribution system in which an alert message originator at the local, state or national level encodes (or arranges to have encoded) a message in the EAS Protocol.<sup>117</sup> The alert is then broadcast from one or more EAS Participants, and subsequently relayed

<sup>5</sup> BlackBerry ex-parte filed in the PS Docket 16-32.

<sup>117</sup> The message provides very basic information about the emergency involved. See 47 CFR § 11.31. Under this protocol, an EAS alert uses a four-part message: (1) preamble and EAS header codes (which contain information regarding the identity of the sender, the type of emergency, its location, and the valid time period of the alert); (2) audio attention signal; (3) audio message, if included by the alert originator; and (4) preamble and “end of message” (EOM) codes. See *id.* § 11.31(a). Although the EAS Protocol specifies that the message can be audio, video, or text, in practice, only audio is sent.

from one station to another until all affected EAS Participants have received the alert and delivered it to the public.<sup>118</sup> This process of EAS alert distribution among EAS Participants is often referred as the “daisy chain” distribution architecture.<sup>119</sup> Because this EAS architecture has been in place since the inception of the EAS, it is often referred to as the “legacy EAS.” Since June 30, 2012, however, authorized emergency alert authorities also have been able to distribute EAS alerts over the Internet to EAS Participants (who in turn deliver the alert to the public) by formatting those alerts in CAP and delivering those alerts through IPAWS.<sup>120</sup> This CAP-based process for distributing alerts to EAS Participants represents the “IP-based EAS.”

Both the legacy and IP-based EAS architectures are designed so that EAS Participants deliver to the public the alert content they receive from the EAS sources they monitor. Further, the EAS architecture and equipment is designed to operate automatically, both to minimize the risk of operator error and to facilitate EAS operation at unattended stations.<sup>121</sup> In particular, the EAS header codes, End-of-Message code, and audio message (if included) that comprise any given EAS alert are determined by the entity that originates the alert (typically, the NWS or state and local emergency management authorities).<sup>122</sup> The EAS equipment of EAS Participants that receive the EAS alert convert the header codes into visual crawls<sup>123</sup> and broadcast the audio<sup>124</sup> – if the EAS Participant’s broadcasts are monitored by downstream stations, it will re-encode (regenerate) the alert so as to trigger EAS equipment in such monitoring

---

<sup>118</sup> The EAS Protocol is identical to the Specific Area Message Encoding (SAME) digital protocol utilized by NWS for weather alerts. See *Third Further Notice of Proposed Rulemaking*, 26 FCC Rcd 8154, para. 5 (citing NOAA Weather Radio SAME Info, <http://www.nws.noaa.gov/nwr/nwrsame.htm>; Specific Area Message Encoding (SAME), National Weather Service Instruction 10-1712 (Feb. 12, 2007), available at <http://www.nws.noaa.gov/directives/010/pd01017012b.pdf>).

<sup>119</sup> At the national level, EAS message distribution starts at Primary Entry Point (PEP) stations, which are a group of geographically diverse, high power radio stations designated and tasked by FEMA to transmit “Presidential Level” messages initiated by FEMA. See *Fifth Report and Order*, 27 FCC Rcd 642, 646-47, para. 7. At the state level, state governors and state and local emergency operations managers activate the EAS by utilizing state-designated EAS entry points – specifically, State Primary stations and “State Relay” stations. See 47 CFR § 11.20. State Relay stations relay both national and state emergency messages to local areas. See 47 CFR § 11.18(d).

<sup>120</sup> See 47 CFR § 11.56; see also *Fifth Report and Order*, 27 FCC Rcd 642, 644-45, para. 4.

<sup>121</sup> See Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System, *Report and Order and Further Notice of Proposed Rulemaking*, 10 FCC Rcd 1786, 1822-23, paras. 103-104 (1994) (subsequent history omitted) (*1994 Report and Order*).

<sup>122</sup> See 47 CFR § 11.31.

<sup>123</sup> See 47 CFR § 11.51(d), (g)(3), (h)(3), (j)(2).

<sup>124</sup> For state and local alerts, EAS Participants broadcast any accompanying audio message on a permissive basis, but are required to broadcast the Presidential audio associated with the federal Emergency Action Notification. See 47 CFR § 11.51(a), (b).

stations, thus perpetuating the daisy chain alert distribution cycle. All of these functions are typically done automatically. In terms of timing, state and local EAS alerts are required to be broadcast within 15 minutes of receipt, and the alert messages themselves are typically limited to a duration of two minutes.<sup>125</sup>

Although CAP and SAME both convey data, the two protocols function in entirely different ways.<sup>126</sup> CAP essentially represents an envelope into which data is packaged according to predetermined fields and packetized for transmission over various IP-based mediums, such as the Internet. The SAME protocol is designed to combine specific codes that identify alert data (e.g., type, origin, area affected) with an audio message and modulate those onto an RF signal.<sup>127</sup> Thus, for example, CAP conveys an alert's identifying data in separate fields from the audio or video message (which may be provided either as a file or a link to a URL); whereas in a SAME-formatted message, the audio portion of the message is already modulated onto the RF signal along with the EAS codes.<sup>128</sup> Accordingly, when the EAS decoder receives a SAME-formatted message, it also receives whatever audio may be associated with that message. On the other hand, when a CAP-enabled EAS decoder receives a CAP-formatted message, it may play back the audio file or retrieve streaming audio from another source.

Broadcast-based EAS Distribution Architecture. The original and still widely used method for distributing EAS alerts (also called the "EAS Daisy Chain") occurs outside the IPAWS architecture. This distribution system is a process whereby alert information is encoded (as audible tones) onto the fundamental broadcast transmission of an EAS Participant in conformance with the EAS Protocol, *see* 47 CFR § 11.31, and is received not only by that EAS Participant's local audience, but also by downstream EAS Participants monitoring that transmission, who have EAS equipment that in turn is activated to retransmit that EAS alert information to their local audiences and monitoring stations, and so on until all EAS participants have received the EAS alert.

---

<sup>125</sup> *See* 47 CFR §§ 11.51(n), 11.33(a)(9).

<sup>126</sup> Unlike CAP, SAME only provides information concerning the originator of the alert, the type of alert (or "event"), the areas affected, the duration of the alert, the time the alert was issued, and the call sign of the EAS Participant that is transmitting or retransmitting the alert. *See* 47 CFR § 11.31. Under the SAME/EAS Protocol, an EAS alert uses a four-part message: (1) preamble and EAS header codes (containing information regarding the identity of the sender, the type of emergency, its location, and valid time period of the alert); (2) audio attention signal; (3) message; and (4) preamble and EAS end of message codes. *See id.* § 11.31(a).

<sup>127</sup> As explained in the *Second Report and Order*, SAME was originally developed to be transmitted via broadcast radio for receipt by relatively simple devices. *See Second Report and Order*, 22 FCC Rcd 13275, 13284-85, para. 20 (*citations omitted*).

<sup>128</sup> Encoding a SAME-formatted message involves modulating the various codes associated with the SAME protocol and an audio message onto an RF signal using the audio frequency-shift keying (AFSK) modulation scheme to open an audio channel in the EAS decoder. Specifically, the EAS decoder is activated by receiving the SAME protocol preamble codes plus header codes, which are repeated three times consecutively at the start of an EAS message transmission. The EAS decoder uses bit-by-bit comparison for error detection to ensure that at least two of the three match. Depending upon the nature of the alert message, this three-time transmission (or "burst") is followed by a two-tone Attention Signal (currently, 8-25 seconds in duration), which functions as an audio alert to listeners and viewers that an emergency message follows. The Attention Signal may be followed by an audio message. At the end of this message, the preamble plus end of message code is transmitted three consecutive times to signal to the EAS decoder that the alert message is terminated and to return to regular programming. *See* 47 CFR § 11.31. When EAS Participants regenerate, or encode, the message they receive for the benefit of downstream monitoring stations, they are only encoding the EAS Codes as AFSK tones (and any embedded audio message).



As illustrated below, the EAS architecture is designed to cascade the alert through a pre-established hierarchy of broadcast, cable, and satellite systems:

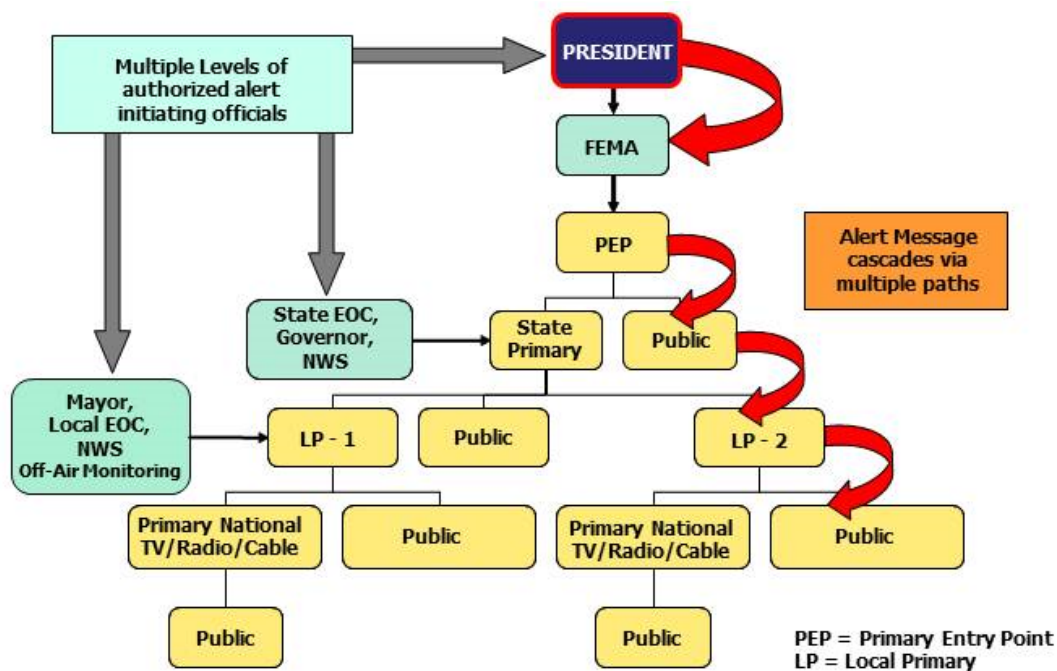


Figure F1: EAS "Daisy Chain" Alert Distribution Diagram

The time required to broadcast the EAS Header Codes delivered by the audible frequency-shift keying data tones alone is 7 seconds, and the underlying protocol requires those tones at the beginning of any EAS message. Thus, although the legacy EAS would have value for less time-sensitive aspects of earthquake-oriented alerts, it is infeasible in its current form for delivering an initial EEW

**IPAWS Internet-based EAS Distribution Architecture.** The primary method for distributing EAS alerts over IPAWS is direct transmission over the Internet of CAP-formatted EAS alerts from IPAWS to EAS Participants. There are essentially three discrete alert processing steps involved in disseminating CAP EAS alerts from IPAWS to the public. First, the CAP alert must be acquired from IPAWS by the EAS device. Specifically, IPAWS uses an Atom Syndication Format (ATOM) feed that EAS devices poll periodically to acquire new, relevant CAP alerts.<sup>129</sup> Second, the acquired CAP alert must then be processed within the EAS device to determine validity, extract relevant information and convert it into a Specific Area Message Encoding-compliant (SAME-compliant) alert.<sup>130</sup> Third, the SAME-compliant

<sup>129</sup> The Atom Syndication Format is an XML language used for web feeds. See *Atom Enabled*, <http://atomenabled.org/> (last visited Aug. 25, 2016).

<sup>130</sup> Specific Area Message Encoding (SAME) is a digital protocol that is identical to the EAS protocol and utilized by NWS for weather alerts. See *Review of the Emergency Alert System; Independent Spanish Broadcasters Association, The Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, Third Further Notice of Proposed Rulemaking, 26 FCC Rcd 8154, para. 5 (citing *NOAA Weather Radio SAME Info*, <http://www.nws.noaa.gov/nwr/nwrsame.htm>; Specific Area Message Encoding (SAME), National Weather Service Instruction 10-1712 (Feb. 12, 2007), <http://www.nws.noaa.gov/directives/010/pd01017012b.pdf>).

information is output to downstream equipment (which may include middleware) that actually broadcasts or otherwise overlays the EAS information onto the program stream viewed and/or listened to by the public on televisions, radios and other devices.

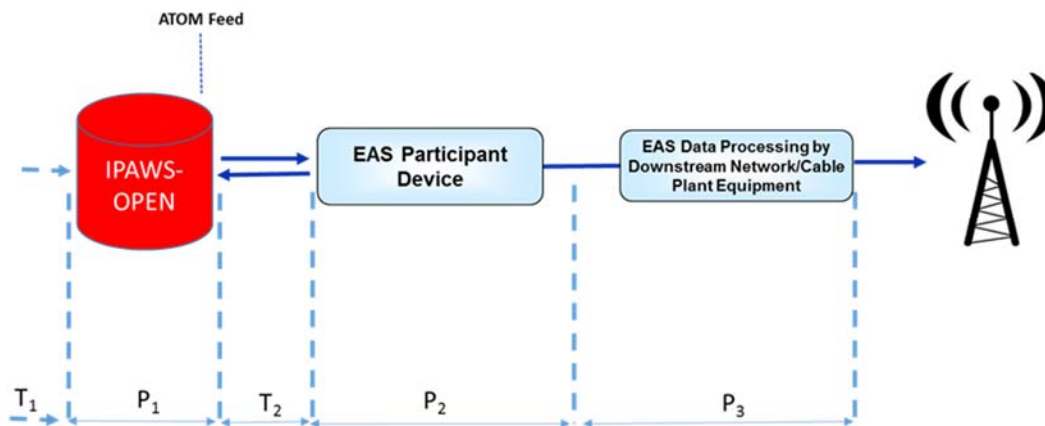


Figure F1: EAS CAP Alert Distribution Diagram

(“T” stands for the Transmission time and “P” for the Processing time)

### EEW Alert Transmission from IPAWS-OPEN to the EAS:

Under the current IPWS/EAS architecture, EAS Participants would receive EEWs from IPAWS by having EAS equipment at their facilities “poll” the IPAWS “Atom feed.” Polling the CAP EAS alert from the IPAWS Atom feed is a three-step process. First, the EAS device checks to see if anything new is posted. Second, if there is a new alert, the EAS device checks to see if it is relevant to them (*e.g.*, confirming the geographic area(s) specified in the alert applies to them). Third, if the alert is relevant, the EAS device retrieves the full CAP message. For an alert without audio, polling can contribute a maximum of 900 seconds to the alert distribution process.<sup>131</sup> For an alert with audio, this step can add another second.<sup>132</sup>

Added to the time associated with polling itself would be time associated with the intervals between EAS Equipment polling of the IPAWS Atom feed. IPAWS does not specify polling intervals, but has informally suggested intervals of 30 seconds. EAS device manufacturers indicate that the polling interval in EAS devices can be set by the end user based on the device user interface capability, participants ISP connection data rate, and recommendations by FEMA to maintain an acceptable load on the server. Device polling minimums range from approximately 1 second to 30 seconds with defaults of 30 or 60 seconds.<sup>133</sup> Individual participant settings depend on the Internet connection agreements they have with their ISP, with those who have broadband connections and few restrictions on the amount of data usage per month able to use faster polling rates. Based on these factors and FEMA recommendations, typical configurations in deployed EAS equipment set the polling rate between 30 and 60 seconds.<sup>134</sup>

Thus, the Atom feed alert distribution process adds significant time to the EEWS delivery process.

<sup>131</sup> Where device polling minimums are set as high as 60 seconds and at least one manufacturer has a maximum of 900 seconds. See Trilithic *ex parte* at 1; Sage *ex parte* at 2.

<sup>132</sup> Where a 960Kb CAP message downloaded over a 8Mbps DSL link takes approximately one second.

<sup>133</sup> See Trilithic *ex parte*, 13 June 2016, 1, (Trilithic *ex parte*); Sage *ex parte*, 16 June 2016, 2, (Sage *ex parte*).

<sup>134</sup> See Sage Comments at 5; Monroe Reply Comments at 7; Trilithic *Ex Parte* Letter at 1.

According to EAS device manufacturers, performance of the three steps themselves typically takes 250 ms to 4 seconds,<sup>135</sup> depending upon equipment, message size, connection, whether audio files need to be retrieved and is highly dependent on the participant's ISP network and Internet congestion between the participant and the IPAWS server. This gives a transmission time of approximately 250 ms to 4 seconds, where the new, relevant CAP alert is on the Atom feed when the device polls, an ideal Internet connection is used, and the alert is short with no streaming audio, plus whatever the polling interval is set at. Average behavior with current setting can be expected to run around 30 seconds.

The time to transmit an alert from IPAWS to the EAS contributes to the end-to-end timeline of the alert depends on when the alert is posted to the Atom feed. Assuming a polling interval of 30 seconds, if the alert is posted on the Atom feed 10 seconds after the EAS device's last poll, then on the EAS device's subsequent poll, that alert will be 20 seconds old, and the actual time contributed to the overall end-to-end processing time of the alert from the transmission to the EAS will be 20.25 to 24 seconds (comprised of the 250 ms to 4 seconds to acquire the alert plus the 20 seconds that alert was waiting on the Atom feed before that acquisition occurred at the start of the EAS device's subsequent poll). For another example, if the polling interval is set at one minute and the alert is posted on the Atom feed 59 seconds after the device's last poll, the transmission time is only one second plus the time it takes to complete the three-step alert acquisition process; but if the alert is posted to the Atom feed one second after the device's last poll, then the transmission time is 59 seconds plus the time it takes to complete the three-step alert acquisition process.

### **Processing of the EEW Alert by the EAS Device:**

The average EAS device internal processing time of CAP-formatted alerts is approximately two seconds.<sup>136</sup> The EAS Participant's EAS device must internally process the CAP alert. This includes authenticating the CAP message, which commenters indicate takes 100 ms or less; converting the CAP message to SAME; and generating any required text to speech. The EAS rules require that the EAS device convert the CAP alert into SAME-compliant data that can be rebroadcast consistent with the EAS Protocol.<sup>137</sup> This is a standardized process that is fairly straightforward; however, CAP provides several methods for conveying the audio portion of the EAS alert, which can significantly impact the overall processing time.<sup>138</sup> If the CAP message conveys audio by including a URL from which the audio must be retrieved before the alert is ready to be transmitted to downstream equipment, the EAS device internal processing time expenditure can last several seconds, depending upon the audio file size and any

---

<sup>135</sup> See Trilithic *ex parte*, 1; Sage *ex parte* 2.

<sup>136</sup> See *supra* note 59. As noted, the two-second figure for EAS device processing is a rough average of processing times reported by EAS device manufactures, based on a plain CAP message with little or no text, and no embedded audio or streaming audio, and could exceed two seconds in various instances. See *id.*

<sup>137</sup> See 47 CFR § 11.56.

<sup>138</sup> For example, audio can be conveyed in an EAS CAP alert via an embedded audio file, identification of a URL source for streaming audio, or, if neither of the foregoing applies, Text-to-Speech (if enabled in the EAS Participant's EAS device). See ECIG Guide, § 3.5. Moreover, there is device design variance among EAS equipment manufacturers that marginally impacts CAP-to-SAME alert conversion. For example, EAS equipment manufacturers indicate that the time period to process a typical CAP alert that includes embedded audio or, in the alternative, requires TTS, for output to downstream equipment that ultimately broadcasts or otherwise transmits the alert data that is viewed and/or heard is between 500 ms and 8 seconds. See Trilithic *Ex Parte* Letter at 2; Sage Comments at 4; Monroe Reply Comments at 7.

downloading latencies, such as the data transfer rate of the EAS Participant's IP service.<sup>139</sup>

Assuming an EEW alert sent over the EAS does not rely on streaming audio, and does not include embedded audio, but rather relies upon text-to-speech (TTS) to generate the audio (which would be produced based upon the EAS header codes and possibly some very brief text included in the CAP alert), it seems reasonable to estimate the average EAS device internal processing time of that CAP alert to be approximately two seconds.<sup>140</sup>

### **Processing of EAS Data by Downstream Equipment:**

There are any number of systemic and operational parameters associated with EAS Participant's system that may increase the time between when the EAS data is ready for output from the EAS device and when that data is actually overlaid onto the programming streams available to the public.<sup>141</sup> Sage observes, for example, that encoding/compression delay, profanity filters, and HF radio encoder, can add several seconds of processing time.<sup>142</sup> Similarly, Trilithic observes, "Due to different architectures and equipment used to support EAS, it can take anywhere from 5 to 120 seconds to present alert information to all subscribers."<sup>143</sup> Thus, EAS alert processing ultimately is not limited to just IPAWS and EAS equipment, but rather involves the entire panoply of studio, transmitter, headend, and other EAS Participant facility equipment, none of which is regulated under the EAS rules.

### **End-to-End Processing Times Associated With Transmitting an EEW Alert via EAS:**

The total end-to-end processing and transmission time of an EEW alert transmitted using EAS can be broken up into the five discrete time periods found in Figure F1 above. Because the EAS is comprised of many different services (TV broadcast, coax, fiber and wireless cable service, radio, etc.), each deployed over very different types of facilities, the resulting total end-to-end processing time of an EEW alert transmitted using EAS is a time range of 3.717 seconds for EAC-to-IPAWS transmission, and IPAWS and EAS device processing,<sup>144</sup> coupled with (a) the Atom feed transmission time, which for typical EAS device configurations can vary from 250 ms to 34 seconds,<sup>145</sup> and (b) the downstream equipment processing time, which can vary from 5 seconds to 120 seconds.<sup>146</sup> Because the function of the EAS Protocol requires all EAS alerts to commence with the modulated audio tones comprising the message preamble and header codes familiar to the public as the three squawks prior to the alert<sup>147</sup> – which by

---

<sup>139</sup> See, e.g., Monroe Reply Comments at 7; Sage Comments at 4.

<sup>140</sup> See *supra* note 59.

<sup>141</sup> Monroe observes, for example, that "[EAS] Participants may manually 'hold' such a message until they release it," and "[s]ome [EAS] [P]articipants may utilize scheduling software to 'fit' the EAS alert into a programming window within that allowable time period." Monroe Reply Comments at 7.

<sup>142</sup> Sage *Ex Parte* at 5.

<sup>143</sup> Trilithic *Ex Parte* at 2.

<sup>144</sup> See *supra* note 59.

<sup>145</sup> See Trilithic *ex parte*, 1, Sage *ex parte* 2.

<sup>146</sup> See, e.g., Trilithic *Ex Parte* at 2; Sage *Ex Parte* at 5; Monroe Reply Comments at 7.

<sup>147</sup> See 47 CFR § 11.31.

itself takes approximately seven seconds to complete<sup>148</sup> – the actual elapsed time before the audio message associated with an EAS alert message is actually heard by the public is the sum of the overall transmission and processing times, plus the seven seconds associated with broadcasting the EAS tones (and another eight seconds can be added to this total in the event that the Attention Signal is aired).

Under the current rules and technical structure, as described above, simply getting the alert from the alert originator through IPAWS and through the EAS device to the point where it is ready to be handed off to the downstream equipment in the EAS Participant's facility represents a time period of at least 3.717 seconds – and that time period is for a basic CAP EAS alert with little or no text, no streaming audio and one geographic location, and does not include the time between when the alert was posted on the IPAWS Atom feed and when the alert is polled, which may add a few seconds to a few minutes of transmission time.

---

<sup>148</sup> Sage *Ex Parte* at 4; The basic header tones take seven seconds as described in the CSRIC4 report. Each additional location code in the EAS message would add 276 ms to the header portion. (15.36 ms per character x 6 characters per location \* 3 headers).