December 2022

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII

REPORT ON WEA PERFORMANCE REPORTING

DRAFTED BY
WORKING GROUP 6: WEA APPLICATION PROGRAMMING INTERFACE

Table of Contents

1 Executive Summary

The Wireless Emergency Alerts (WEA) system is an essential part of America's emergency preparedness. Since its launch in 2012, the WEA system has been used more than 70,000 times[1] to warn the public about dangerous weather, missing children, and other critical situations – all through alerts on compatible cell phones and other compatible cellular mobile devices. WEA is a public safety system that allows customers who own compatible cellular mobile devices to receive geographically targeted, text-like messages alerting them of imminent threats to safety in their area. However, many authorized Alert Originators (AOs) do not currently utilize WEA. Some authorized Alert Originators report that they lack the awareness and confidence needed to use WEA in otherwise-appropriate circumstances due to concerns regarding reliability, latency, and accuracy, leading to a proposal for automated reporting of data related to performance metrics.

In addition, some Alert Originators actively using WEA have stated that having additional insights into WEA's performance may assist future alert planning, and that analysis of the performance data may allow stakeholders to identify areas of improvement for future alerts which will more effectively utilize WEA, EAS, and other alerting systems for public benefit. Improvements may also have the potential to increase public confidence in WEA.

The currently available State/Local WEA Test was designed to allow Alert Originators to certify operations, and to verify the abilities of WEA in their jurisdiction. Performance reporting from the State/Local WEA Test requires manual measurement and collection of data, so its scale is a function of resource (e.g., people, devices, etc.) availability.

This report analyses proposals intended to increase the size of the data sample and provide data at more regular intervals. Starting with what is available today for Alert Originators to review WEA performance through the existing State/Local WEA Test. In addition, the report discusses, at a high level, two automated performance reporting proposals, one based on opted-in consumer devices and one based on dedicated staged devices, as well as estimated timelines to change policies where required, study and design new functionality, develop standards, development and deployment of new WEA functionality where required, and implement changes to both devices and WEA architecture including cellular infrastructure.

CSRIC VIII recommends that the FCC consider all findings in this report.

2 Introduction

CSRIC VIII appreciates the focus on maximizing the success of WEA. As demonstrated over the past 10 years, WEA is a successful, voluntary emergency alert transmission system. Over the 10 years since WEA has been in service, the partnership between all WEA stakeholders have identified improvements to WEA for which solutions have been standardized both in ATIS and

[1] Federal Communications Commission, *Wireless Emergency Alerts (WEA)*, https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea (last visited Nov. 30, 2022).

3GPP. One such notable improvement was the introduction of Device-Based Geo-Fencing (DBGF) in WEA 3.0 devices that improves the geotargeting accuracy of WEA.

Available data demonstrates that WEAs are highly effective in reaching their destinations during an emergency; the FCC's report[2] found a 90% success rate for message transmission during the 2021 Nationwide WEA Test. Nonetheless, media reporting of recent disasters has demonstrated a comprehension gap and lack of awareness about the WEA system among some emergency management agencies.

2.1 CSRIC Structure

CSRIC VIII was established at the direction of the Chairperson of the Federal Communications Commission (FCC) in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VIII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VIII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VIII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairperson of the FCC.

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII					
CSRIC VIII Working Groups					
Working Group 1: 5G Signaling Protocols Security	Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment	Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks	Working Group 4: 911 Service Over Wi-Fi	Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure	Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts
Co-chairs: Brian Daly, AT&T & Travis Russell, Oracle	Co-chairs: Mike Barnes, Mavenir & George Woodward, RWA	Co-chairs: Micaela Giuhat, Microsoft & John Roese, Dell	Co-chairs: Mary Boyd, Intrado & Mark Reddish, APCO	Co-chairs: Todd Gibson, T-Mobile and Padma Sudarsan, VMware	Co-chairs: Farrokh Khatibi, Qualcomm & Francisco Sanchez, SBA
FCC Liaison: Ahmed Lahjouji	FCC Liaison: Zenji Nakazawa	FCC Liaison: Jeff Goldthorp	FCC Liaison: Rasoul Safavian	FCC Liaison: Saswat Misra	FCC Liaisons: James Wiley Tara Shostek

Table 1 - Working Group Structure

2.2 Working Group 6 Team Members

Working Group 6 consists of the members listed below.

Name	Company
Farrokh Khatibi (Co-Chair)	Qualcomm
Francisco Sanchez (Co-Chair)	U.S. Small Business Administration (SBA)

[2] Public Safety and Homeland Security Bureau, Report: August 11, 2021 Nationwide WEA Test Report (PSHSB, Dec. 2021), https://docs.fcc.gov/public/attachments/DOC-378907A1.pdf.

Mark Annas	City of Riverside Fire Department, OEM
Rebecca Baudendistel	NYC Emergency Management
Terri Brooks (Report Editor)	T-Mobile USA
Wade Buckner	International Association of Fire Chiefs
Kirk Burroughs	Apple
Brian K. Daly	AT&T, Inc.
Harold Feld	Public Knowledge
Craig Fugate	America's Public Television Stations
Michael Gerber	National Weather Service/NOAA
Dana Golub	Public Broadcasting Service
Stephen Guiwits	US Geological Survey
Mark Hess	Comcast Corporation
Antwane Johnson	FEMA
Robert Kubik	Samsung Electronics America
Jennifer Lazo	City of Los Angeles Emergency Management
John Marinho	CTIA
Susan Miller	ATIS
Krisztina Pusok	American Consumer Institute
Matthew Straeb	Global Security Systems, LLC
Peter Tomczak	FirstNet Authority
Dara Ung	Comtech Telecommunications Corp.
Larry Walke	National Association of Broadcasters
Steve Watkins	Cox Communications
Chia-Kaung (Jack) Yu	Google LLC

Table 2 - List of Working Group Members

Alternates for members are listed below.

Name	Company
Tim Dunn	T-Mobile USA
Nicholas Garcia	Public Knowledge
Kevin Green	FirstNet Authority
Al Kenyon	FEMA
Nathanael Scherer	American Consumer Institute
Charles (Peter) Musgrove	ATIS
Peter Scott	PBS

Table 3 - List of Working Group Alternates

3 Objective, Scope, and Methodology

3.1 Objective

While WEA is a one-way broadcast service that is not designed to enable the collection of performance data, there is belief that having additional insights into WEA's reliability, latency[3]

[3] A national latency testing exercise was done in September 2022, with public results from T-Mobile, Verizon and AT&T published by the FCC. See Wireless Emergency Alert Performance Testing, Wireless Emergency Alerts, Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System, *Order*, PS Docket Nos. 22-160, 15-91, 15-94 (PSHSB August 30, 2022), https://docs.fcc.gov/public/attachments/DA-22-901A1.pdf.
Verizon's Data: https://www.fcc.gov/ecfs/document/1001215579176/1
AT&T Data: https://www.fcc.gov/ecfs/document/10930171316553/1 and

and accuracy, as indicators of how WEAs propagate in communities, may assist Alert Originators in planning alerts and build public confidence in receiving the relevant alert expeditiously.

Many authorized Alert Originators report that they lack the confidence needed to use WEA in otherwise-appropriate circumstances because they lack information about, and confidence in, how WEA works in practice.

Analysis of the performance data may allow stakeholders to identify areas of improvement for future alerts which will more effectively utilize WEA, EAS, and other alerting systems for public benefit. However, it is not evident to the Cellular Industry that collecting and reporting performance data would meaningfully increase the effectiveness of WEA or increase participation among Alert Originators, who may have various reasons for declining to participate as an authorized Alert Originator or use WEAs in a given circumstance.

With regard to Alert Originators not currently participating in WEA, it should also be noted that while performance reporting may provide data related to general performance for WEA, no Alert Originator will know the specifics for their jurisdiction without engaging in the system.

CSRIC VIII has been charged to consider and present recommendations for enabling stakeholders in the ecosystem to report data which can be manipulated to assess WEA's reliability, latency, and accuracy, including the increased use of the currently available State/Local WEA Test capability, and to present recommendations following an analysis of proposals, automated and otherwise, for logging and collecting of performance data from consumer mobile devices, or staged devices, about the receipt and presentation of WEA.

3.2 Methodology

This report documents the following:

1) High-level descriptions of various proposed methods for performance data collection based on definitions of the metrics of reliability, latency, and accuracy,
2) The data elements which may be available in relation to the metrics of reliability, latency and accuracy, including limitations for the collection of that data,
3) Specific examples of how the data could be leveraged to lead to improvements in Alert Originator and other WEA stakeholder handling,
4) The development and/or design changes required to support proposed automated reporting and data collection, as the cell broadcast system currently is not designed to support such reporting,
5) The risks and challenges associated with automated reporting.

4 Background

https://www.fcc.gov/ecfs/document/10930171316553/2
T-Mobile Data: https://www.fcc.gov/ecfs/document/10010549603122/1

The IPAWS Modernization Act, enacted in 2016, requires FEMA, in consultation and coordination with FCC, to enhance and test the capabilities of the Integrated Public Alert & Warning System (IPAWS) and increase its adoption among state and local public safety agencies. In February 2020, The GAO published a report[4] to Congress citing the "*FCC has not developed goals and performance measures for these efforts. Doing so would help FCC more clearly assess whether the WEA improvements are working as intended. Furthermore, having specific performance information could increase alerting authorities' confidence in and use of IPAWS.*"

Effective emergency alerting is vital to helping save lives and property during natural disasters and other threats to public safety, highlighting the importance of WEA to disseminate critical information. As a result, the GAO recommended the following:

"*The Chairman of [sic] FCC should develop specific, measurable goals and performance measures for its efforts to monitor the performance of new WEA capabilities, such as enhanced geo-targeting and expanded alert message length. (Recommendation 1)*"

The first-ever 2021 Nationwide WEA Test was a "significant step in measuring WEA's performance" that gave reliable data regarding rate of receipt, transmission length, and message presentation. All WEA stakeholders can build on this success by conducting additional testing that improves on the methodologies of the initial Nationwide Test. The goal should be to seek to engender broad stakeholder participation in future tests, as each player in the WEA ecosystem has a different, critical role to play in testing the WEA system.

While the FCC collects EAS test data to assess how well EAS tests are received and retransmitted, a similar mechanism is desired for the WEA pathway. The EAS reporting, via the FCC's EAS Test Reporting System (ETRS), recognizes that EAS is a broadcast service, and collects data on the ability to receive and process the EAS message from IPAWS as well as the geographic coverage of the broadcast transmitters during tests of the EAS system. Since EAS is also a broadcast service, reporting on reception of the EAS is not subject to end device reporting but relies on members of the public and interested stakeholder organizations that are able to observe test results in their communities and provide useful feedback on the test, including any problems observed or any complications in the delivery of the EAS message during the test. Since WEA is also a broadcast service, this same methodology should apply.

[4] Government Accountability Office, Emergency Alerting: Agencies Need to Address Pending Applications and Monitor Industry Progress on System Improvements at 25-27 (2020), https://www.gao.gov/assets/gao-20-294.pdf.

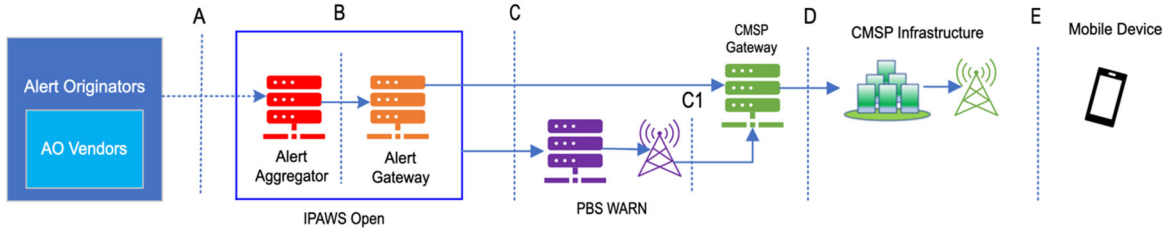

Figure 1 - Wireless Emergency Alert System

As shown in Figure 1, authorized national, state, tribal, or local government authorities may send alerts via IPAWS to the Participating Cellular Mobile Service Providers (CMSPs). The CMSPs then broadcast the alerts in the affected area which may be received by capable cellular mobile devices. All capable cellular mobile devices in the broadcast area will generally receive the alert;[5] however, mobile device users may opt out of having any type of alert presented, with the exception of the National Alert. Some alerts carry information which enables Device-Based Geo-Fencing (DBGF). In this case, DBGF-capable mobile devices will perform a location comparison as part of the alert processing when determining whether the alert should be presented.

In Figure 1, the vertical dotted lines between pairs of major responsible entities, referred to as "stakeholders" throughout this document, are labeled with the quick-reference names representing the specification requirements between any two stakeholders—A, B, C, C1, D, and E.

4.1 Definitions and Acronyms

4.1.1 Definitions

Performance Metrics:

Accuracy	Number of devices inside the Alert Area which[6] (including within 0.1 miles of the Alert Area boundary) presented the WEA divided by the total number of devices that presented the WEA.
Latency	Time between when the Alert Originator sends the WEA and the time that the WEA is presented on a device.
Reliability	Proportion of devices within the Alert Area (including within 0.1 miles of the Alert Area boundary) that received and appropriately processed (e.g., presented if appropriate based on user's setting, location, etc.) the

[5] WEA reception is highly dependent on RF coverage and propagation.
[6] Note that the FCC Requirements allow presentation up to 0.1 miles outside the boundary of an Alert Area defined by coordinates.

	alert.

Additional Definitions:

Alert Area	Geographic area associated with the geometric shape defined by coordinates provided by the Alert Originator.
Broadcast Area	Geographic area selected for the broadcast.
Cellular Industry	Collective of the CMSPs, mobile device manufacturers, and OS providers.
Civic Address	The street name and number designated by a Local Municipality. This generally takes the form of 123 Main Street, Anywhere, US 00000, however, other forms such as street intersection may also be presented.
Ground Truth	Information that is known to be real or true, provided by direct observation and measurement (i.e., empirical evidence) as opposed to information provided by inference.[7] Specifically, this would be performance information observed at the Test Participant's location that is known to be real or true, provide by direct observation and measurement. For example, location could be the Latitude/Longitude or a Civic Address; latency is the observed time of display of the WEA on the device.
Latitude/Longitude	Taken together in a given coordinate system (in the case of the US, generally specified by WGS-84) a means by which the position or location of any point on Earth's surface can be described.[8]
Type Allocation Code (TAC)	TAC is the initial eight-digit portion of the 15-digit International Mobile Equipment Identifier (IMEI) and 16-digit IMEI Software Version (IMEISV) codes used to uniquely identify wireless devices. The TAC identifies a particular model (and often revision) of wireless device for use on a 3GPP wireless network.
Overshoot	WEA broadcast propagating beyond the boundaries of the Alert Area resulting in presentation of the WEA beyond the Alert Area boundaries.
Undershoot	WEA broadcast propagating short of the boundaries of the Alert Area resulting in the lack of presentation of a WEA within the Alert Area.
WEA Stakeholder	Any entity with an ongoing vested interest in WEA, as a provider, vendor or user of some portion or the entirety of the service.

4.1.2 Acronyms and Abbreviations

AO	Alert Originator
CMSP	Commercial Mobile Service Provider
DBGF	Device-Based Geo-Fencing
EAS	Emergency Alert System
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency

[7] https://en.wikipedia.org/wiki/Ground_truth
[8] https://gisgeography.com/latitude-longitude-coordinates/

IMEI	International Mobile Equipment Identity
IMEISV	IMEI Software Version
IPAWS	Integrated Public Alert & Warning System
Lat/Long	Latitude/Longitude
PBS	Public Broadcast System
TAC	Type Allocation Code
WEA	Wireless Emergency Alert

4.2 Problem Statement

4.2.1 Identified Needs as Provided by the Alert Originators

Successful public alerting requires public safety officials to deliver emergency information to the people who need it, when they need it, and in a form they understand. Likewise, WEA performance reporting may help further understand the extent to which wireless alerts are received by the people who need them, when they need them, per U.S. regulatory requirements and industry standards.

Public safety has relied mostly on the collection of anecdotal information, and on objective information from the State/Local WEA Test, by the public safety community. Objective information may help public safety officials understand how they can best use the tools at their disposal to warn the general public of hazards, save lives, and protect property. It may also help the public safety community and wireless industry better understand where opportunities for improvement may exist, so that both parties can best work together to maximize the life-saving potential of WEA.

Usage and actions as a result of performance metrics will vary by the type of emergency and type of alert originator.

- Emergency Managers often deal with long duration emergencies, such as wildfires and law enforcement related emergencies that may go on for days or weeks. Throughout the course of the emergency (i.e., preparation, occurrence of the hazard, and ongoing emergency conditions), emergency managers are actively working to refine their life-saving alert messaging and public response. Thus, additional WEA performance metrics are useful to emergency managers throughout the course of the emergency. During long duration events, critical infrastructure may be impacted by the event, and thus CMSPs and other stakeholders work closely with the emergency management and first responder teams as they develop their response.

- NOAA's National Weather Service (NWS) most often activates WEA in bursts for multiple concurrent short fused and short duration events such as tornadoes and flash floods. Thus, NWS usage of WEA performance metrics is often, but not always, going to be during the NWS storm and service assessment phase which typically occurs within a day or two following the event. During this phase, the overall effectiveness of all methods of alerting,

including WEA, in getting the appropriate message to the public is analyzed with the goal of learning how to more effectively use WEA and other alerting tools for future emergencies.

Actions that result from analysis of WEA performance metrics may include:

- Determining optimal use of public warning including WEA, EAS, social media, etc.
- Refinement of the alert message to more effectively generate the needed public response
- Allocation and distribution of emergency response resources

WEA performance metric collection as related to the technical performance of the WEA delivery are intended to focus on factors within CMSP control. Technical performance trends for WEA delivery are helpful for refinement and future improvements to WEA delivery.

The desired information Alert Originators are specifically looking at receiving includes the following:

Accuracy, defined as the number of devices inside the Alert Area[9] which (including within 0.1 miles of the Alert Area boundary) presented the WEA divided by the total number of devices that presented the WEA, could also be characterized with information to include:

The distance outside the alert area where the WEA was presented

a. Average distance outside the alert area
b. Median distance outside the alert area
c. Maximum distance outside the alert area
d. Minimum distance outside the alert area

Latency, defined as the time between when the Alert Originator sends the WEA and the time that the WEA is presented on a device, may also include intermediary timestamp information which includes:

1. the time CAP alert is originated by an alert originator,
2. the time the CAP alert is received at FEMA IPAWS,
3. the time FEMA IPAWS delivers the WEA alert to each Participating CMSP,
4. the time FEMA IPAWS delivers the WEA alert to PBS,
5. the time that each Participating CMSP receives the alert at their CMSP Gateway,
6. the times that each Participating CMSP starts broadcasting the WEA,[10]
7. the time that PBS begins broadcasting the WEA,
8. the time that the WEA is received at the mobile device, and
9. the time that the WEA is presented to the user.

Reliability, defined as the proportion of devices within the Alert Area (including within 0.1 miles of the Alert Area boundary) that received and appropriately processed (e.g., presented if appropriate based on user's setting, location, etc.) the alert, may also include information such as:

[9] Note that the FCC Requirements allow presentation up to 0.1 miles outside the boundary of an Alert Area defined by coordinates.
[10] During any the standardization process the definition of "start of broadcasting" would need to be defined.

1. The number of mobile devices that received the alert and presented it successfully.
2. The number of mobile devices that received the alert but did not present it due to being outside the Alert Area.
3. The number of mobile devices that received the alert, presented the alert by default due to location being unavailable (e.g., location services turned off).
4. The number of mobile devices that received the alert but did not present due to the user's mobile device settings (e.g., opted out of AMBER alerts).
5. The number of all mobile devices that should have received the alert.

WEA performance metrics have the potential to provide actionable situational awareness information. Actions taken in response to WEA performance metrics will vary depending on the given scenario. The examples below illustrate some of the ways public safety officials would use WEA performance metrics to identify where and how limited public safety resources should be used to best save lives.

Reliability:

- During earthquakes and other emergencies, knowing the number of devices that received the WEA versus the number of devices in the alert area provides an estimate of how many people may need help and assists in resource and public safety response management.

- Assists in after action assessments and planning where identification of what's working and what's not working well helps public safety officials to better prepare for and better perform during the next event.

- Reliability information provides insight into how other forms of public communication (e.g., broadcasters, electronic media, social media, PA systems, sirens, door-to-door notification, air-asset alerting, etc.) should be leveraged, geotargeted, and the content of alert messages be refined to best convey the alert message in ways that saves lives.

- Provides the data needed to identify the needed focus and geographic targeting of follow up alerts, public outreach, education, and local strategic mitigation planning.

Latency:

- Knowing latency through the system can provide valuable life-saving seconds for the public and infrastructure in providing time to drop, cover, hold on and turn on/off critical infrastructure devices and medical procedures.

Accuracy:

The August 25, 2022 Placer, Yolo and Sacramento WEA tests are examples that illustrate the need for a greater understanding of actual WEA geographic targeting performance. During the test, cell phones at the Sacramento Emergency Operations Center presented WEA for all three

tests.

- If overshoot occurs and a number of devices present the alert outside of the alert area, then public safety officials who initiated the alert as well as those in neighboring jurisdictions would need to determine where and how best to reach out reach out the public using WEA and other forms of public communication (e.g., broadcasters, electronic media, social media, PA systems, sirens, door-to-door notification, air-asset alerting, etc.) in order to clarify the information.

- During a wildfire, life-saving instructions for a single fire can range from shelter in place to evacuate. Given that there are limited ways to escape or stay out of harm's way, specific geographically targeted life-saving instructions are needed and WEA overshoot could cause public confusion. When multiple adjacent wildfires are occurring, overshoot could cause more extensive public confusion. Geotargeting accuracy information will help alerting authorities to best craft the message for follow up alerts using WEA and other forms of public communication to ensure life-saving alert information is conveyed to the right people at the right time.

4.2.2 Concerns of Cellular Industry with Identified Needs

The Cellular Industry has expressed concerns on anticipated actionable results that may be expected with the collection of WEA accuracy, latency, and reliability performance data. With the improvements in WEA over the past decade, issues with mobile devices receiving WEAs outside the alert area have been addressed. Latency has been optimized in the CMSP infrastructure. And the National Tests have demonstrated the reliability of WEA.

One concern expressed by Alert Originators is the anecdotal nature of the data currently available, however, automated data collection in an ever-changing and adjusting field environment will always, to some extent, be anecdotal due to anomalies that come and go without visibility in the data collected.

Accuracy in WEA 1.0 and 2.0 will result in mobile devices receiving WEAs outside the alert area. However, with WEA 3.0 devices and the DBGF capability, accuracy will be very high as the device will not present the WEA unless it is within the Alert Area. There will be legitimate WEA 3.0 devices that present a WEA outside the Alert Area; for example, if the user has turned off location services or the mobile device cannot determine its location, or if the AO uses a geocode instead of a polygon or sets the DBGF bypass. Providing accuracy performance data that include these devices will not provide any actionable data; that is, there is no action to be taken if a WEA 3.0 device presents the WEA outside the Alert Area based on these legitimate cases.

Latency has also been addressed in the WEA ecosystem and further measurements will not provide actionable results. CMSPs in particular have optimized their networks for both initial broadcast of the WEA, as well as rebroadcast intervals throughout the time the alert is active. This rebroadcast is necessary in a mobile environment to maximize the probability of devices receiving the WEA in a complex RF environment. Mobile devices that receive the WEA on one

of the rebroadcast cycles may appear to have increased delay, but this in fact is not a delay but a characteristic of a mobile environment. Thus, "latency" will show devices that receive the WEA during any of the rebroadcast cycles; an "average" of these measurements will provide a false high latency metric, yet there is no action that can be taken by several WEA stakeholders.

The Automated Reporting from Opted-In Consumer Devices proposal has the potential for divulging consumer sensitive information, such as location of the mobile device before, during, and after the alert period. Customer choice to provide (opt-in) performance data must be a priority. Privacy implications of the automatic reporting of WEA performance information from WEA-capable mobile devices must be a consideration, as the collection of this information may be in conflict with Participating CMSP, mobile device vendor, and/or OS provider privacy policies. The Cellular Industry has stated that their privacy policies will prevent providing location information, or any information from which location could be derived, of their subscribers/consumers as part of any automated WEA performance reporting of consumer devices, even considering consumer opt-in, as no method for anonymizing data at the source (mobile device) has been identified. Privacy concerns and trust in WEA by mobile device customers may also increase the number of users that choose to opt-out of WEA due to the lack of confidence in the protection and use of their personal information.

4.3 Existing Tools

The FCC, FEMA, CMSPs, and state and local public safety agencies have carried out nationwide and localized alert tests since 2016, producing reports on capabilities and effectiveness of WEA. These existing tools should be the first consideration for conducting additional targeted testing to assess WEA efficacy.

The existing tool, which offers capabilities that can be, and have been, applied toward measuring reliability, latency, and accuracy, is the State/Local WEA Test.[11] This test involves having the Alert Originator place users in the field with one or more devices and having those users report specific data points following the broadcast of the alert. By developing goals and performance measures for State/Local WEA Tests, stakeholders would have clearer direction for what they plan to achieve and more specific means to assess the performance of the capabilities.

Alert Originators are well-positioned to specify areas where they believe WEA performance has been inconsistent, and have a critical role to play in verifying the success of the message delivery given that they control the content, intended geographic scope, duration, and special features of alerts. CMSPs can provide information about when alerts reach their gateway, ensuring the networks are functional, confirm that the alert is broadcast from all cell sites in the Broadcast Area, measure the time from message arrival in CMSP gateway to broadcast and confirm the number of times the alert was rebroadcast. Handset manufacturers and operating system developers are in the best position to collect data on alert

[11] Wireless Emergency Alerts, Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System, Report and Order and Further Notice of Proposed Rulemaking, PS Docket Nos. 15-91, 15-94, FCC 16-127 (September 29, 2016) (4th Report and Order and FNPRM), https://docs.fcc.gov/public/attachments/FCC-16-127A1.pdf, based upon CSRIC IV Testing Subgroup report https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-2_Testing-Rprt_061814.pdf.

accuracy, receipt, and relevant device settings. By conducting testing that leverages the unique positions and capabilities of the various WEA stakeholders, it is possible to gather more comprehensive data about WEA efficacy and use this information to develop policies that will help to ensure WEA is as successful and widely used as possible.

The State/Local WEA Test is required to be supported by CMSPs in the FCC's 4th Report and Order, released in September 2016. After standardization and development, this capability has been in operation since the deployment of WEA 2.0/3.0 by FEMA and the CMSPs in December 2019. One of the key backgrounds stated by the Commission in the 4th Report and Order was to "…encourage emergency management agencies to engage in proficiency training exercises…where appropriate…" and that "…emergency managers may also use State/Local WEA Tests to voluntarily collect and share information about geo-targeting, alert delivery latency, and other vital performance metrics. We encourage emergency managers and related entities to engage in extensive outreach to their respective communities in order to socialize the benefits of public participation in State/Local WEA Tests, and otherwise to raise public awareness about the benefits of receiving WEA messages, including through the use of PSAs."[12]

Ultimately, the stated goals of the State/Local WEA Test mandated by the Commission are to provide "…a solid testing and training platform…" which enables "…regular readiness testing and proficiency training…critical to maintaining WEA alert origination competency because '[i]f you don't use it you lose it.'"[13]

Additionally, other methods should be explored that could potentially allow CMSPs to support the needs of Alert Originators specified in Section 4.2.1 which avoid the extensive changes that would be required to support WEA automated performance reporting. These other methods should be considered on an event-by-event basis utilizing non-WEA tools, with Alert Originators, Emergency Managers, and the CMSPs working together to address the event needs. These tools may provide more accurate, timely, and actionable information that can be used in the response effort. For example, to identify the number of devices within an evacuation zone after a WEA containing an evacuation order was issued, using WEA performance metrics will likely be very inaccurate or inconclusive; there are potentially other non-WEA methods available that may provide more accurate information for this use case, thus allowing for a better response. Historically, the Alert Origination/Emergency Management community has not approached the cellular industry to help identify other means to provide data for these use cases.

[12] 4th Report and Order and FNPRM at page 46.
[13] 4th Report and Order and FNPRM at page 45.

5 Analysis, Findings, and Recommendations

5.1 Analysis

This section of the report provides a high-level analysis followed by detailed findings for data collection to support the metrics of reliability, latency, and accuracy, defined in Section 4.1.1, and expectations as to how this data could be leveraged by all stakeholders. Expected impacts to stakeholders required to achieve automated data collection are described in detail. Recommendations are then presented.

Proposals analyzed:

- State/Local WEA Test. See Section 5.1.1.
- Automated Performance Reporting from Opted-In Consumer Devices. See Section 5.1.2.
- Automated Reporting from Staged Devices. See Section 5.1.3.

Performance Metrics:

Reliability, Latency and Accuracy are defined in Section 4.1.1. Additional information regarding those performance metrics is as follows:

> Reliability is a performance metric which is intended to ensure that the WEA is being broadcast, and that it is then received and presented, according to user settings, by devices inside the Alert Area and is not presented when the device's location is outside of the Alert Area (including consideration of the 0.1 mile allowance and user configuration for location device setting). Specific data points may depend on the method of data collection, design of the system, and various configuration parameters.
>
> While latency may be measured between any two points in a communications chain, the critical measure of latency for WEAs shall be measured as the difference between the time that the WEA is initiated by an authorized Alert Originator and the time the WEA is presented at a mobile device. The thinking is if it is determined that the latency metric is not "acceptable" then there is a belief that there is a need to determine where latency improvements can be addressed.
>
> Cell broadcast technology, which is the broadcast transport for WEA, rebroadcasts the WEA at periodic intervals to ensure that mobile devices moving from outside of the Alert Area to inside the Alert Area, being turned on for the first time during the alert period, or that may have been experiencing RF anomalies during the initial broadcast or subsequent rebroadcasts, will receive the alert. Mobile devices receiving any of the periodic rebroadcasts, rather than the initial broadcast, may impact the "latency" metric, making it appear falsely high. This does not reflect a delay or latency in WEA delivery, but is a necessary capability to handle the complex RF environment.[14]

[14] A national latency testing exercise was done in September 2022, with public results from T-Mobile, Verizon and AT&T published by the FCC.

Applicable definitions are:

Broadcast Area	Geographic area selected for the WEA broadcast.
Alert Area	Geographic area of the geometric shape defined by coordinates provided by the Alert Originator. This is the area to which the alert applies.

The Broadcast Area may or may not fully cover the Alert Area depending on whether the participating CMSP's network infrastructure is technically capable of matching the specified Alert Area (see 47 CFR §10.450). In addition, to achieve the requirement of 100% coverage of the Alert Area, a CMSP may need to include cell sites well outside the Alert Area to broadcast the WEA into the Alert Area (resulting in overshoot of the broadcast). As an example, in Figure 2 below, the pink area represents the Broadcast Area and the blue polygon represents the Alert Area which is defined by the Alert Originator using lat/long coordinates. Coverage of 100% of the Alert Area requires broadcasting the WEA in all the cells/sectors shown with pink shading, as each one provides sufficient coverage to some portion of the Alert Area. Cells 1, 2, and 3 are sectored cells and the broadcast will go active on only the sectors that overlap some portion of the Alert Area, which is why no shading is shown in sector 1A. Cell 4 is an omnicell that will also be included in the broadcast given the partial overlap with the Alert Area. To ensure that the alert broadcast covers the entire Alert Area (which is a requirement on the CMSP by the FCC rules), overshoot (alert broadcast propagating beyond the boundaries of the Alert Area) will occur. Note that the actual broadcast area coverage will be different for each Participating CMSP as the cell site topology is unique (and proprietary) for each CMSP network.

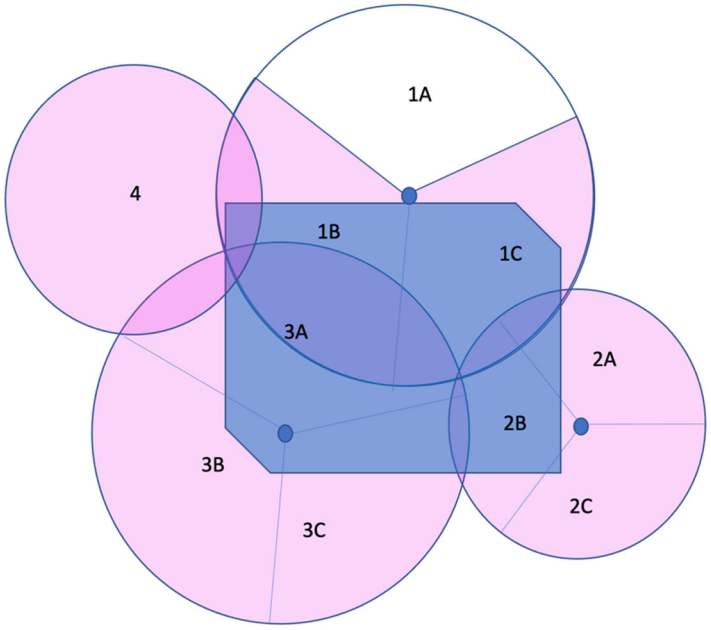

Figure 2 - Illustration of Broadcast Area versus Alert Area

5.1.1 State/Local WEA Test

The State/Local WEA Test capability allows for controlled testing done by the Alert Originators, with a known group of Test Participants at specified dates/times to enable reliable testing and analysis. This would allow for testing and building confidence of the end-to-end flow by the Alert Originator.[15]

Utilizing Test Participants who would be working hand in hand with the Alert Originators would ensure no privacy concerns. Many Alert Originator agencies have relationships with community groups[16] that can assist as ground truth observers in the State/Local WEA Test. Surveys may be sent out to solicit the public's input for the State/Local WEA Test.

Alert Originators should ensure proper exercise design and that their Test Participants have a State/Local WEA Test capable device and that the device has the State/Local WEA Test enabled. Choosing the number of Test Participants to provide a sample which represents part of the target population in the desired area will provide results within a given margin of error and confidence level.[17]

The processing of the State/Local WEA Test, from the time it leaves the Alert Originator's premises until it reaches the mobile device, is the same as every other alert class (with the exception of the National Alert class). The only difference in handling at the device is based on the opt-in/opt-out settings available per alert class that determine the final step of presentation. This means that testing with the State/Local WEA Test provides data that is fully representative of the operational success of WEA.[18]

5.1.1.1 Data Collection Details

Between the AO's, the CMSP and the Test Participants, relevant data to measure reliability, latency and accuracy need to be collected, and are listed below.

5.1.1.1.1 Reliability

Reported by the Test Participant:

1) Presentation of the alert based upon location of device/Test Participants for Ground Truth verification
2) Service provider
3) Device settings (S/L test on/off, Location on/off)
4) Device Manufacturer, Model, and OS version (a TAC of the Handset would be ideal).

[15] CSRIC IV Testing Subgroup report, page 24.
[16] For example, Amateur Radio Emergency Services teams, CERT teams, SKYWARN spotters.
[17] An example of a sample size calculator is available at https://www.surveymonkey.com/mp/sample-size-calculator/
[18] ATIS-0700037.v003, Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification.

5.1.1.1.2 Latency

Reported by the Test Participant:

1) Time of presentation on the handset
2) Pertinent details if presentation was later than expected, such as surroundings (e.g., in an elevator) that may have influenced reception

Reported by the Alert Originator

1) Time the alert was initiated

Reported by FEMA

1) Time the alert was received
2) Time the alert was sent to the CMSPs

Reported by the CMSP

1) Time the alert was received
2) Time the alert was first broadcast

5.1.1.1.3 Accuracy

Reported by the Test Participant:

1) Location at time of presentation (e.g., lat/long, civic address)
2) Manufacturer/model/OS version (to determine DBGF capabilities)
3) Device settings (S/L test on/off, Location on/off)

Reported by the Alert Originator

1) Alert Polygon Generated

5.1.1.2 Leveraging Data Analysis Results to Produce Improvements

As described in the CSRIC IV Testing Subgroup report,[19] the goal for State and Local WEA Testing was to provide a method for Alert Originators with a known set of Test Participants to build confidence in the WEA end to end flow. The development of this testing in CSRIC IV was done after conducting a formal survey of what Alert Originators thought they needed in a test environment. In addition, the concept of having known participants and known locations at known dates and times provides for reliable and repeatable testing which could be used by Alert Originators in various certification processes for their Public Safety agencies.

Data from routine State and local testing could be used as follows:

1. To have Alert Originators become more comfortable with the WEA Process, in general.
2. To have Alert Originators understand the compatible handsets that support State and Local testing and validate that DBGF on those devices indeed performs as intended.
3. To develop an understanding of what happens in an alert scenario when the device settings for location use are switched off, DBGF isn't available for the device and alerts are presented outside the Alert Area.
4. To provide for an additional outreach opportunity to the local community to participate in the testing so their community could better understand WEA presentation on the device.

[19] CSRIC IV Testing Subgroup Report (May 2014) at page 24, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-2_Testing-Rprt_061814.pdf.

5. To enable an understanding by Alert Originators, test participants and the local community on the timing of alert delivery and an estimate of how long it takes between the local Alert Originator initiating the alert on their origination software and receipt of the WEA on the device.

5.1.1.3 Development and Design Impacts

State and Local WEA Testing has been available since December 2019. It can immediately be used to conduct performance testing. Various alert originators use State and Local WEA Testing today on a routine basis. [20] This testing is consistent with the testing methodology for EAS.

5.1.1.4 Risks and Challenges

None Identified.

5.1.2 Automated Performance Reporting from Opted-In Consumer Devices

New automated reporting about WEA's performance by WEA stakeholders may have the potential to provide additional insights, which may increase the confidence in the use of WEA. Reporting of WEA's reliability, latency, and accuracy (as defined in Section 4.2.1) is proposed through the following steps:

1. **Consumer opt-in**: Enabling device users to opt-in to the collection and sharing of WEA data, specifically for the purpose of determining metrics, with the understanding that this data will be anonymized at the collection point,
2. **Performance Metric Data Collection**: WEA stakeholders collect message receipt and presentation and other performance-related data,
3. **Reporting the Performance Data**: WEA stakeholder(s) sends the relevant parameters to a single data collection point for metric calculations, and
4. **Performance Data Availability:** Enabling all stakeholder(s) (e.g., CMSPs, FEMA, Alert Originators) to have controlled access to this data.

For automated performance reporting, the highest volume of the performance data would be collected and reported from consumer devices for which the consumer has opted-in to collecting and sharing of the data with the WEA Performance Application Server (WEA-PAS). The Cellular Industry would not have visibility into this data, and have expressed concerns over consumer privacy.

The performance data collection and reporting of each relevant node in the WEA path is proposed through the development of necessary software to allow for appropriate data capture and sharing, consistent with user preferences, CMSP and mobile device/OS provider privacy policies, and any Federal/State/Local regulatory requirements.

[20] FEMA IPAWS Guidance, Conducting Wireless Emergency Alert Tests, https://www.fema.gov/sites/default/files/documents/fema_ipaws-guidance-conducting-wea-tests.pdf.

It is assumed that any future devices that support automated performance reporting would also support WEA 3.0 (i.e., DBGF-supporting devices). Neither WEA 1.0 devices nor WEA 2.0 devices would support automated performance reporting.

5.1.2.1 Data Collection Details

Automated performance reporting would require additional capabilities in the WEA architecture. For the purposes of this report, a new element referred to as the WEA Performance Application Server, or WEA-PAS, is proposed to collect the WEA performance data from WEA stakeholders. WEA-PAS receives the performance information, anonymizes the data, collates the data, and generates reports for reliability, latency, and accuracy. PBS WARN, in conjunction with FEMA, may be a good candidate for administering and hosting the WEA-PAS as PBS WARN currently maintains a history of WEAs, and IPAWS maintains credentials for authorized AOs and Participating CMSPs.

The WEA-PAS also allows stakeholders to view reports for WEAs they originated or broadcast. The WEA-PAS must have security and access protocols that protect the data, and limit access to only authorized users. At no time will customer or CMSP proprietary data be shared with or stored on the WEA-PAS.

Note that the reporting path from the CMSP infrastructure and mobile devices to the WEA-PAS may be through the CMSP infrastructure, however it is a separate data path and does not follow the cell broadcast route used to broadcast the WEA. Cell broadcast does not provide a reverse channel for any type of reporting.

A Reporting Mobile Device would be defined as a WEA-capable mobile devices meeting all three of the following conditions:

1) Is located within the Broadcast Area during the WEA's active period and received the WEA; and
2) User has opted in allowing the mobile device sharing of WEA performance metrics with the corresponding WEA Performance Application Server.

Correlation of the reported performance data from each node in the WEA path with the associated WEA also needs to be addressed. This would require substantial end to end architectural design discussions in an entity like ATIS and 3GPP, followed by an extensive standardization effort.

5.1.2.1.1 Reliability

Reliability is defined as the proportion of devices within the Alert Area that received and appropriately processed (e.g., presented if appropriate based on user's setting, location, etc.) the alert. Further, AOs have also asked for the following metrics related to reliability:

1. The number of mobile devices that received the alert and presented it successfully.

2. The number of mobile devices that received the alert but did not present it due to being outside the Alert Area.
3. The number of mobile devices that received the alert, presented the alert by default due to location being unavailable (e.g., location services turned off).
4. The number of mobile devices that received the alert but did not present due to the user's mobile device settings (e.g., opted out of AMBER alerts).
5. The number of all mobile devices that should have received the alert.

This proportion requires knowing the total number of devices in the Alert Area for the denominator, which is an unknown quantity and cannot be obtained without a complete redesign of existing cellular technology and changes to the privacy policies within the cellular ecosystem. Since WEA is an unacknowledged broadcast service, determination of the total number of WEA capable devices in the Alert Area that should have received and presented the alert cannot be obtained. CMSPs do not track the location of mobile devices, as tracking them poses significant privacy considerations, and thus do not know the total number of WEA capable devices in any given Alert Area. Also, Mobile devices by their very nature are mobile – they will be moving into and out of the Alert Area while the WEA is active. Users may be turning their mobile devices off or on, changing the number of devices within the Alert Area. Thus, the total number of WEA capable devices in the Alert Area is a dynamic number throughout the WEA alert lifetime, making it impossible to obtain any accurate count. Mobile devices cannot be relied on to report that they are within the Alert Area but did not receive and present the WEA, since they are unaware of the WEA being issued and do not know the coordinates of the Alert Area.

It may be possible to estimate the denominator by using census/population statistics for the number of potential recipients within the Alert Area, however this would be a rough estimate and would not give an accurate number of mobile devices that potentially could have received the WEA. This would not provide estimates for devices that may be roaming into the area. It may, however, help give the alert originators a very rough estimate as to the penetration of the WEA to the population in the Alert Area.

While the denominator of the metric is not known, for the numerator it may be feasible that capable Reporting Mobile Devices could report if they received and presented the WEA while within the Alert Area. To determine if the mobile device is within the Alert Area when the WEA broadcast is received and presented, the mobile device must compare its location to the Alert Area. To do this, it must have received the coordinates of the Alert Area in the WEA broadcast and be able to determine its location. If these location parameters are not available (e.g., the user has disabled location), then the mobile device cannot determine if it was in the Alert Area when the WEA was received and presented. These devices would be a contributing factor in a metric that is inaccurate and not meaningful or actionable.

In addition, given Figure 1 and the fact that mobile devices are "mobile", several cases add complexity to this proposed metric and need consideration:

- **Mobile Device is within both the Broadcast Area and Alert Area**: Capable Reporting Mobile Devices indicate receipt and presentation of the WEA broadcast while within the Alert Area. These Reporting Mobile Devices would be included in the WEA reliability performance metric.

- **Mobile Device is within the Broadcast Area but not the Alert Area**: Capable Reporting Mobile Devices that are within the Broadcast Area but outside the Alert Area (and do not move into the Alert Area while the WEA is active) would not be included in the WEA reliability performance metric.
- **Mobile Device is outside the Alert Area but moves into the Alert Area while the WEA is active**: Capable Reporting Mobile Devices that are outside the Alert Area and at some point, while the WEA is still active, moves into the Alert Area, indicate the mobile device received and presented the WEA while within the Alert Area. These Capable Reporting Mobile Devices would be included in the WEA reliability performance metric.
- **Mobile Device is outside both the Broadcast Area and the Alert Area and does not move into the Alert Area**: Capable Reporting Mobile Devices that are outside both the Broadcast Area and the Alert Area (and do not move into the Alert Area) are not included in the WEA reliability performance metric because such devices never receive the alert.

In summary, WEA Reliability calculations have the following challenges and limitations:

1) Reliability calculations as defined in Section 4.1.1 cannot require a proportion to the *total* number of mobile devices in the Alert Area, because this is unknown, dynamic, and cannot be obtained.
2) The number of devices for which users have opted into allowing performance reporting and are in the Alert Area will also not be known, and any given device may not receive and present the alert (e.g., radio anomaly, inside an elevator), and would subsequently not report it received the alert. This also will make the reliability metric unreliable.

5.1.2.1.2 Latency

Latency is defined as the time between when the Alert Originator sends the WEA and the time that the WEA is presented on a device. Latency metrics can also be obtained at various points in the WEA distribution chain as follows:

1. the time the CAP alert is originated by an alert originator,
2. the time the CAP alert is received at FEMA IPAWS,
3. the time FEMA IPAWS delivers the WEA alert to each Participating CMSP,
4. the time FEMA IPAWS delivers the WEA alert to PBS,
5. the time that each Participating CMSP receives the alert at their CMSP Gateway,
6. the times that each Participating CMSP starts broadcasting the WEA,[21]
7. the time that PBS begins broadcasting the WEA,
8. the time that the WEA is received at the mobile device, and
9. the time that the WEA is presented to the user.

WEA delivery has been optimized throughout the ecosystem. For example, the latency from the time FEMA IPAWS delivers the WEA the Participating CMSP Gateway to the time the WEA is broadcast by the CMSP infrastructure has been optimized and will vary little from WEA to

[21] During any standardization process the definition of "start of broadcasting" would need to be defined.

WEA. These minor variances are primarily due to the complexity of the polygon and determination of the cell sites/sectors that are needed to broadcast the WEA.

Due to the rebroadcast mechanism, Latency metrics in a cell broadcast environment will not provide conclusive or actionable information on the WEA delivery system.

Cell broadcast technology, which is the broadcast transport for WEA, rebroadcasts the WEA at periodic intervals to maximize the number of mobile devices that receive the WEA, and will make the proposed "latency" metric appear falsely high. The cell broadcast rebroadcast function is important because mobile devices may be moving into the Alert Area while the WEA is active, users may turn on devices for the first time while the WEA is active, mobile devices may be temporarily out of coverage and come back in coverage, etc. This does not reflect a delay or latency in WEA delivery, but is a necessary capability to handle the complex RF environment.

The proposed latency metric seems to assume that mobile devices receive the WEA on the very first broadcast, and any "delay" in receiving beyond that initial broadcast represents a latency problem. This is not accurate – devices may receive the WEA on any one of the rebroadcasts, and while may appear as a "delay" in receipt as each rebroadcast increases the time between when the WEA was originated to the time it was presented, the mobile device will actually be seeing the WEA for the first time on the rebroadcast and from the perspective of that mobile device, there is no "delay" or latency issue. Mobile devices do not know if they are receiving the first WEA broadcast or the "Nth" WEA broadcast.

In summary, the rebroadcast mechanism as part of the delivery of WEA will appear as an increase in the observed latency metric. But this is a false high reading that is not very meaningful nor actionable.

If the time of presentation of the WEA is deemed to be a collectable metric, Reporting Mobile Devices that receive a WEA could report the date/timestamp of when the WEA broadcast was presented, regardless of its location when it is presented. And given Figure 1 and the fact that mobile devices are "mobile", several cases add complexity to this proposed metric and need consideration:

- **Mobile Device is within both the Broadcast Area and Alert Area**: Capable Reporting Mobile Devices could report the date/timestamp upon the presentation of the WEA broadcast. Data from these capable Reporting Mobile Devices would be included in the WEA latency metric. The mobile device may receive the WEA on any one of the rebroadcasts while the alert is active, so this latency metric may be artificially false high.
- **Mobile Device is within the Broadcast Area but not the Alert Area**: Since the Capable Reporting Mobile Device does not move into the Alert Area, it does not present the WEA and thus does not report the presentation time. These capable Reporting Mobile Devices would not be included in the WEA latency metric.
- **Mobile Device is outside the Alert Area but moves into the Alert Area while the WEA is active**: Capable Reporting Mobile Devices that are outside the Alert Area but moves into the Alert Area while the WEA is active reports the date/timestamp upon the presentation of the WEA. These capable Reporting Mobile Devices would be included in the WEA latency metric, and since it would only report when it moves into the Alert

Area (and will present when it first receives the WEA during any of the rebroadcast cycles), there is again the potential of an artificially false high latency metric.

- **Mobile Device is outside both the Broadcast Area and the Alert Area and does not move into the Alert Area**: Capable Reporting Mobile Devices that are outside both the Broadcast Area and the Alert Area (and do not move into the Alert Area) do not present the WEA and are not included in the WEA latency metric. These capable Reporting Mobile Devices would not be included in the WEA latency metric.

Additional timestamps in the WEA delivery chain could be available for further analysis (such as the time the WEA was sent by FEMA IPAWS to the CMSP Gateway or the time the CMSP infrastructure began broadcasting the WEA), but these timestamps do not contribute to the latency metric as defined in this report, and do not vary significantly as there is no dependence on field conditions.

Performance Data options for the Latency Metric:

From the Alert Originator:

1. Date/timestamp of the origination of the WEA

From FEMA IPAWS:

1. Date/Timestamp when the CAP message was received from the AO
2. Date/Timestamp when the WEA message was delivered to each Participating CMSP
3. Date/Timestamp when the WEA message was delivered to PBS

From PBS:

1. Date/Timestamp when the WEA message was received from FEMA IPAWS
2. Date/Timestamp when the WEA was broadcast by the PBS broadcast network

From each Participating CMSP:

1. Date/Timestamp when the WEA was received from FEMA IPAWS or PBS
2. Date/Timestamp when the WEA was first broadcast from the CMSP infrastructure

From the Mobile Device:

1. Date/Timestamp of the receipt of the WEA
2. Date/Timestamp of the presentation of the WEA, if presented

5.1.2.1.3 Accuracy

Accuracy is defined as the number of devices inside the Alert Area[22] (including within 0.1 miles of the Alert Area boundary) which presented the WEA divided by the total number of devices

[22] Note that the FCC Requirements allow presentation up to 0.1 miles outside the boundary of an Alert Area defined by coordinates. See 47 CFR §10.450 (a).

that presented the WEA. In addition, AOs desire the distance outside the Alert Area where the WEA was presented:

a. Average distance outside the Alert Area
b. Median distance outside the Alert Area
c. Maximum distance outside the Alert Area
d. Minimum distance outside the Alert Area

Each distance measurement requires location of the mobile device, which raises privacy concerns even if the data is anonymized at the WEA-PAS. Customer location information is never reported.

WEA accuracy only applies to when the WEA alert is *presented* as there is intentional overshoot in order to cover 100% of the alert area, and a WEA-capable mobile device may *receive* a WEA broadcast outside the Alert Area but not *present* it to the mobile device user as part of DBGF, the accuracy is expected to be very high even with the Broadcast Area being greater than the Alert Area.

However, there are valid cases when DBGF-capable devices will present the WEA while the mobile device is outside the Alert Area. While there are a few reasons for this, they all involve the device not knowing or calculating its location, so as such would have no distance to report.

The primary cases for Overshoot are when the mobile device is within the Broadcast Area (Figure 2) but:

1) is unable to determine its location,
2) the user has location turned off, or
3) the alert originator specifies DBGF Bypass[23] due to the time sensitive nature of the WEA.

In each of these cases, the WEA may be presented to the user outside the Alert Area, resulting in Overshoot. These cases where the WEA is presented outside the Alert Area are legitimate cases for presentation and will result in an accuracy metric that will not provide meaningful or actionable data; that is, the presentation outside the Alert Area was a legitimate use case.

For the Accuracy metric, Reporting Mobile Devices that receive and present a WEA could report whether the mobile device was inside or outside the Alert Area when the WEA was presented. Note for consumer privacy considerations, the actual location of the mobile device will never be reported.

Any accuracy metric will only give a percentage for reporting devices, not all devices, meaning that the Reliability metric, as defined, cannot be met.

Performance Data options for accuracy:

[23] The FCC has approved acceptance of DBGF Bypass from USGS at this time.

From the Mobile Device:

1. An indication that the WEA was presented inside or outside the Alert Area

5.1.2.2 Leveraging Data Analysis Results to Produce Improvements

Due to the inconclusive nature of the metrics, it is not clear how collecting performance data would contribute to the success of WEA. It is unclear that information regarding the reliability, latency, and accuracy of WEA would be of practical utility for any enhancements to the WEA delivery system given the invisible factors (e.g., radio frequency effects) which constantly vary in the field. Evidence suggests that lack of Alert Originator adoption appears to be due at least in part to a determination that it is unnecessary, insufficient awareness, resources, and training regarding the availability and use of WEA—issues that performance data will not address.

5.1.2.3 Development and Design Impacts to Produce Automated Reporting

5.1.2.3.1 Alert Originators

None identified.

5.1.2.3.2 Alert Originator Vendors

Development of software to report the performance information to the WEA Performance Application Server (WEA-PAS).

The following is a summary of the Alert Originator performance data that would be needed to support automated performance reporting. Examples include:

- Parameter that uniquely identifies the WEA that is sent
- Date/timestamp of the origination of the WEA. Used for WEA latency report.

5.1.2.3.3 FEMA

The following are examples of the FEMA IPAWS performance data that would be needed to support automated performance reporting:

- Parameter that uniquely identifies the WEA that is sent
- Date/Timestamp when the CAP message was received by FEMA IPAWS
- Date/Timestamp when the CMAC message was initiated to each Participating CMSP Gateway and PBS

5.1.2.3.4 CMSP Network

The following are examples of the CMSP Network performance data that would be needed to support automated performance reporting:

- Parameter that uniquely identifies the WEA that is sent
- Date/Timestamp when the CMAC message was received by the CMSP Gateway
- Date/Timestamp when the CMSP began the WEA broadcast

Analysis and planning for handling increased capacity due to data reporting must be performed.

5.1.2.3.5 PBS

The following are examples of the PBS Network performance data that would be needed to support automated performance reporting:

- Parameter that uniquely identifies the WEA that is sent
- Date/Timestamp when the CMAC message was received by the CMSP Gateway
- Date/Timestamp when PBS began the WEA broadcast

5.1.2.3.6 Mobile Device

Development of user interfaces to manage opt-in/out of performance reporting, ability to capture presentation date/time of WEA alerts, ability to determine location inside or outside the Alert Area when a WEA is presented, development of software to report the performance information to the WEA Performance Application Server (WEA-PAS).

The following are examples of the mobile device performance data that would be needed to support automated performance reporting:

- Parameter that uniquely identifies the WEA that is received and presented
- Date/Timestamp when the mobile device received the WEA.
- Indication if the mobile device was inside or outside of the Alert Area upon receipt of the WEA.
- Date/Timestamp when the mobile device presented the WEA. Used for WEA latency report.
- Indication if the mobile device was inside or outside of the Alert Area upon presentation of the WEA. Used for WEA reliability and accuracy reports.
- Indication if the mobile device received the alert, presented the alert by default due to location being unavailable (e.g., location services turned off, or DBGF bypass is enabled by AOs)

Indication that the mobile device received the alert but did not present due to the user's mobile device settings (e.g., opted out of AMBER alerts).

5.1.2.4 WEA Performance Application Server

Development of a new WEA Performance Application Server (WEA-PAS) to receive WEA performance data from all reporting mobile devices from all Participating CMSPs, develop a security profile to allow the secure transfer of data from mobile devices to the WEA-PAS, anonymize the received WEA performance data, collate each received WEA performance report

with the appropriate WEA alert, and provide secure APIs for each stakeholder to generate WEA performance reports.

Industry agreement on what entity could be trusted with such sensitive data will need to occur.

5.1.2.5 Risks and Challenges

5.1.2.5.1 Public Education Campaign

A public education campaign will be required to ensure that consumers fully understand that the user must take specific steps to opt-in to the automated reporting, hopefully minimizing the number of consumers that may misunderstand and opt-out of WEA due to privacy concerns. Announcing to the WEA consumer base that new functionality will exist on mobile devices that will allow their device to automatically upload information at some point in time following the receipt of a WEA, even accompanied by the explanation that they have to manually opt-in, could be a significant detriment to the goal of increasing the number of consumers receiving alerts. Consumers may also turn location services off to avoid tracking as part of any WEA performance data collection, negating the intended benefits of DBGF.

5.1.2.5.2 Alert Originator Education

An educational campaign would be required to educate Alert Originators on what this data is and what it is not, including identified gaps in the data and limitations on what it can tell us about WEA performance. Alert Originators should also be aware that data will not be available from all users (e.g., those that opt out, devices not capable of reporting, devices that did not receive the WEA).

5.1.2.5.3 Service Risks

While reporting from the mobile devices should not produce impacts to the cell broadcast system capacity, it has the potential to impact CMSP traffic capacity. Traffic capacity following any alert requiring user action, such as contacting emergency services or family members or searching the web for more information, has a strong potential to increase the traffic on the network. The additional traffic from reporting of performance data could negatively impact the ability of the CMSP's network to fully support the needs of the consumers during that time. Even delayed automated reporting, triggered at a later time, carries that possibility of localized congestion during the reporting period. An example would be performance reporting from a large city, where potentially millions of devices would have to provide performance reports, nearly simultaneously, on top of the existing network traffic.

5.1.2.5.4 Additional Challenges

As described above, automated performance reporting will be based on a very narrow set of data, limiting the range of metrics that can be calculated with any certainty.

With regard to presentation based on location accuracy, the only location data to be obtained during automated data reporting will only be available from the mobile device with no corroboration from any additional source.

Although the device may indicate whether the alert was presented or not based on user settings, analysis of presentation aspects would require a consistent set of user settings on the device to

enable data capture and processing, putting the data collection and analysis out of formal control. Currently device menus (e.g., options) vary.

5.1.2.5.5 Privacy Concerns

Compliance with customer privacy, based upon Federal, State and Local regulatory requirements, CMSP privacy considerations, and mobile device/OS provider considerations, is a significant consideration and privacy concerns may result in more users opting-out of WEA.

Any attempt to collect the users' location data would have to be collected in an anonymized form, no standards exist for conveying location anonymously and non-anonymized location would be a huge privacy concern.

5.1.2.5.6 Estimated Study, Standardization, Development & Deployment Considerations

Implementing the proposal for automatic performance reporting from opted-in consumer devices would potentially require a substantial reworking of the existing WEA system, including the network architecture, software managing the system, alert originators' systems, FEMA gateway, and other components. In addition, new mobile devices may be required to implement the changes— leading to a lengthy period of time for new devices to be developed, produced, bought by consumers, and deployed into the wireless networks.

While actual timelines are dependent on the FCC R&O and solutions developed through the study and standards process, a very rough high-level estimate is as follows:

- Standards study phase: 6-8 months
- Standardization Phase: 12-24 months dependent on extent of 3GPP involvement
- AO software, FEMA IPAWS, PBS Development: 12-18 months
- WEA-PAS RFP/Development/Implementation/Testing: 24-36 months
- CMSP Infrastructure Development: 12-18 months
- CMSP Infrastructure Deployment and testing: 6-8 months
- Mobile Device Development: 12-24 months
- Mobile Device Upgrade: 12-24 months post development

Note that some of the software development (i.e., post design and standardization) steps may be done in parallel. However, the whole program is expected to take between 6-8 years.

5.1.3 Automated Reporting from Staged Devices

This proposal describes a variation of automated reporting from mobile devices which would specifically employ staged devices. Similar to the proposal of reporting from opted-in consumer devices, this proposal would involve the design of a new device capability that would trigger reporting of various data from the staged devices, as well as the need to establish a data collection entity. The staged devices would be stationary with a known location, access to power, and a data connection.

The reasoning behind using staged devices is primarily anchored in the intent to alleviate technical concerns with the quality of the data. Having a known set of devices, along with their locations, settings, make/model, etc., eliminates unknown variables, making any calculations or trends drawn from the data more reliable than data reporting from opted-in consumer devices.

There is a significant added benefit of having no policy or privacy concerns, as opted-in consumer devices are not involved, reducing the implementation challenges. This, in turn, removes the risk of having users opt-out of WEA due to automated data reporting. A major purpose of this CSRIC study is to promote the use of WEA. Risking the possibly of having users opt-out of WEA is at direct odds with that goal.

It is assumed that future new devices that support WEA 3.0 (i.e., DBGF-supporting devices) will support automated performance reporting. Neither WEA 1.0 devices nor WEA 2.0 devices will support automated performance reporting.

5.1.3.1 Data Collection Details

The known device data, to be used in one or more metrics, is as follows:

1) Location of device
2) Service provider
3) Device settings
    a. Location on/off
    b. User WEA Opt-in/Opt-out settings
    c. Language settings
4) Device Manufacturer/Model/OS Version (determines capabilities, such as DBGF)

The following sections indicate the data that would be reported via specific stakeholder and by the device, preferably using some type of algorithm for staggering the load on the network, although this proposal minimizes the amount of data needed to be signaled over the network due to the amount of known data.

5.1.3.1.1 Reliability

Reported by Alert Originators:

1) Alert Area definition (geocode, and geometric coordinates if applicable)
2) Languages provided (English 90, English 360, Spanish 90, Spanish 360)

Reported by all Stakeholders: (pertains to all metrics)

1) Correlation data (Specifics TBD)

5.1.3.1.2 Latency

Reported by Device:

1) Time of reception
2) Time of presentation

Reported by FEMA:

1) Time the alert was received
2) Time the alert was sent to the CMSPs

Reported by CMSP:

1) Time the alert was received
2) Time the alert was broadcast

NOTE: Rather than having FEMA and the CMSPs report each time, a series of State/Local WEA Tests could be performed to determine an expected average. This timing does not vary significantly.

5.1.3.1.3 Accuracy

Known device data as well as reported data listed above for Reliability would meet requirements. No additional data needed.

5.1.3.1.4 Additional Considerations

None identified.

5.1.3.2 Leveraging Data Analysis Results to Produce Improvements

General scenarios have been supplied in Section 4.2, but no specific application of this data to modifications of processing or handling of the alert have been identified.

5.1.3.3 Development and Design Impacts to Produce Automated Reporting

Data correlation design will apply to all stakeholders.

5.1.3.3.1 Alert Originators

Planning and placement of devices to achieve desired test data would be required.

5.1.3.3.2 Alert Originator Vendors

Development of software to report the performance data would be required.

5.1.3.3.3 FEMA

Development of software to report FEMA IPAWS performance related data points would be required.

5.1.3.3.4 CMSP Network

Development of software to report CMSP Network performance related data points would be required.

Analysis and planning for handling increased capacity due to data reporting must be performed.

5.1.3.3.5 PBS

Development of software to report PBS performance related data points would be required.

5.1.3.3.6 Mobile Device

Development of software to log and report receipt and/or presentation of the WEA and related timing of events would be required. All static data (Make, model, OS version, user settings, location) is known.

5.1.3.4 Risks and Challenges

While reporting from the staged devices should not produce impacts to the cell broadcast system capacity, it will impact CMSP traffic capacity. Traffic following any alert requiring user action, such as contacting emergency services or family members, has a strong potential to increase. The additional traffic from reporting of performance data could negatively impact the ability of the CMSP's network to fully support the needs of the consumers during that time; although this proposal minimizes the amount of data needed to be signaled over the network due to the amount of known data. Even delayed automated reporting, triggered at a later time, carries that possibility.

5.2 Recommendations

CSRIC VIII recommends that the FCC consider all findings in this report.

CSRIC VIII recommends that the FCC consider a requirement for an automated email to convey WEA performance reporting information from CMSPs and from PBS to an AO, or a centralized reporting location, for each sent WEA. Details for the generation procedures and content of the email automated performance report are encouraged to be worked out between AOs and CMSPs/PBS in a new ATIS WEA standard to support WEA automated performance reporting via email.

5.2.1 Alert Originator Perspectives on WEA Automated Performance Reporting

Alert Originator (AO) members of Working Group 6 disagree with some items in the report being presented as fact at the urging of Commercial Mobile Service Providers (CMSPs). Statements declaring or suggesting that automated WEA performance reporting will be of little or no use were based on statements by CMSPs and device manufacturers that device location data is unknown and any measures will be imperfect or misleading. However, public safety officials must often make decisions during emergencies that are based on imperfect information. Furthermore, CMSP Responses to the FCC Data Privacy Probe[24] released by the FCC on August 25, 2022, includes statements such as the following which suggest device location data is known.

> [C]ollect device location data provided by mobile device operating systems...determined using information from the device's Global Positioning System ("GPS") antenna, Wi-Fi access point(s), and mobile network and sensor location data available to the operating system provider...may be as specific as device telephone number and latitude/longitude coordinates...used in connection with our Business and Marketing Insights program...develop insights to help estimate...how many customers go to a retail store...total number of customers that were at a stadium at a given time.[25]
>
> [E]mbedded in the firmware of Android devices by original equipment

[24] https://www.fcc.gov/document/rosenworcel-shares-mobile-carrier-responses-data-privacy-probe
[25] Verizon Response https://www.fcc.gov/document/response-verizon

> manufacturers ("OEMs")...collects device diagnostic and location data on a passive basis (e.g., when a device powers on or contacts a new cell tower), including latitude/longitude information...collects the location of a person's device to direct a cell tower to provide telecommunications...In addition to first-party marketing...customers can choose to participate in Relevant Advertising ("RA"), which is an opt-out advertising program, and Enhanced Relevant Advertising ("ERA"), which is an opt-in advertising program.[26]
>
> Like all wireless providers...we collect information about a customer's location when they place or receive cell phone calls or text messages, or when they have an active data session...location data that (1) relates to an identified or reasonably identifiable person, (2) identifies an individual's location within 1,850 feet, which is the largest distance considered "sensitive" or "precise" under state laws...policy is not to collect or retain Geolocation Data for advertising purposes without affirmative customer consent may disclose Geolocation Data to our service providers...[27]

One company in the marketplace, CellInt[28] discusses how they work together with carriers to utilize network data to anonymously monitor for traffic, transportation, and smart city planning.

AOs greatly value the privacy of the general public and have expressed no interest in obtaining information about cellular customers. AOs are instead interested in information about distribution of mobile devices in and around the alert area that will improve situational awareness and help emergencies managers make decisions that best save lives and protect property. If necessary, AOs offer that privacy concerns could be further alleviated by a small blurring of location data, such as 50 to 250 feet. Concerns would be further limited with a customer opt-in providing affirmative consent to providing anonymized data.

5.2.2 Cellular Industry Perspectives

5.2.2.1 Findings

The WEA system has, both in 2021 and 2022, been the subject of close scrutiny, and has been tested through both a nationwide test using the State/Local WEA Test, which was standardized in WEA 2.0 and WEA 3.0 as a result of CSRIC IV recommendations[29] and FCC action[30], and through the use of the Public Safety alert category. These tests, organized and coordinated by the FCC in cooperation with the CMSPs and numerous alert agencies, verified the strong reliability and speed of the WEA system. In addition, the State/Local WEA Test offers a tool for any Alert Originator to check any number of system aspects within their own jurisdiction.[31]

---

[26] AT&T Services Response https://www.fcc.gov/document/response-att-services
[27] T-Mobile Response https://www.fcc.gov/document/response-t-mobile
[28] https://www.cellint.com/about-us/news-and-events/
[29] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0
[30] https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1119/FCC-15-154A1.pdf
[31] FEMA IPAWS Guidance to AO's on conducting State and Local WEA Tests:
https://www.fema.gov/sites/default/files/documents/fema_ipaws-guidance-conducting-wea-tests.pdf

It has been stated that Alert Originators may be able to adjust their approach to alerting in general, but to WEA more specifically, through having concrete, rather than anecdotal, data. This is one of the two drivers for this in-depth analysis of providing WEA performance metrics. There are many decision factors that play a part in the real-time decisions of the alerting agencies, and a better understanding of certain WEA performance metrics may improve the outcome of a given event, or provide learnings for future events.

This report has analyzed specific performance metrics related to WEA dissemination, and discussed, in detail, the nature of each metric. Specifically, this report explores the knowns, unknowns, and uncertainty about these metrics, especially with regard to the field variations in a complex radio environment that will have no visibility in any form of performance reporting, and which would weaken or skew, and in some cases invalidate, any conclusions drawn from the data. Due to these factors, any attempt at adjustment of the input data or processes for WEA may bring about unintended, and possibly negative, impacts. This data may supply input for the response of the limited public safety resources available and identify other dissemination sources (social media, sirens, etc.), though it is unclear as to what role any WEA performance metrics would play.

It is also noted that since WEA is a broadcast service, CMSPs have no insight into the mobile device reception or processing of WEAs; specifically, CMSPs cannot determine which mobile devices received the WEA broadcast, the devices' location when they receive the WEA, which devices presented the WEA and which did not, or what the customer device settings are related to WEA presentation or device location.

The other stated goal of this effort is to hopefully increase the number of authorized Alert Originators using WEA by boosting their confidence in the system. While data obtained in the widespread testing managed and coordinated by the FCC, has verified the performance of WEA, confidence would be better built through direct engagement with WEA because that performance would directly relate to any WEA which an individual AO may send in their jurisdiction. The State/Local WEA Test not only verifies the performance of the WEA system but allows AOs to verify their own operations and understanding of this complex, multi-stakeholder system, including specific WEA options which may be more suitable for a given AO or jurisdiction.

All of these factors bring into question the ability of a WEA performance reporting system to achieve the stated goals. Nonetheless, the technical aspects of supporting performance reporting have been explored at length. Three performance reporting proposals are described in detail in the report and are summarized in Table 4 which lists data points as related to performance metrics defined in this report, along with an indication under each proposal as to whether the data can be obtained. The proposals in this report have not considered near-instantaneous analysis and reporting, as these scenarios surfaced late in the process of creating this report. This type of immediate processing has not been analyzed at all and no findings or conclusions are presented.

Due to the inability of the proposal of Automated Performance Reporting from Opted-In Consumer Devices to meet the basic data needs, coupled with both the associated strong privacy concerns described throughout this report and the risks of user opt-out, this path is not

recommended for either of the goals stated in relation to this task. Further details with regard to data reliability for this proposal can be found in Section 5.2.2.2.

It is also noted that there may be other means to achieve the stated objectives of the AOs using non-WEA methods to obtain data; these other methods should be considered on an event-by-event basis utilizing appropriate non-WEA tools, with Alert Originators, Emergency Managers, and the CMSPs working together to address the event needs. Historically, the Alert Origination/Emergency Management community has not approached the cellular industry to help identify either their needs or other means to provide data for these use cases.

The State/Local WEA Test was designed to meet the needs of verifying operations and performance within the AOs' jurisdictions. This evaluation method is currently available, used by a small number of AO's (demonstrating an under-utilized method), has low complexity, and no traffic capacity impacts. Given all these factors, the State/Local WEA Test represents the best path forward for bringing Alert Originators on board for scenarios best met by WEA. Alert Originators must engage in the system to know its potential for their jurisdiction, and to verify their own operations, training, and best practices. Following this engagement, those AOs would be in the best position to gauge the effectiveness of WEA and its best use in conjunction with any other avenues of alert dissemination available to them.

It is possible that the Automated Performance Reporting with Staged Devices could supply additional decision-making support to the Alert Originators for adjustments to alerts or to their actions during ongoing events, however, the relationships between this data and any possible actions have not been explored or defined clearly enough to determine whether this would be advisable. In addition, there has been no evidence that the larger quantity of data that would be supplied by this system, as compared to the State/Local WEA Test, would be expected to identify any additional information or data trends.

5.2.2.2 Reliability of Data

Section 5.2.1 in this report references collection of data, specifically citing loose, non-recorded estimates related to marketing and crowd movement. The text implies that the incomplete data identified in Section 5.1.2 Automated Reporting from Opted-In Consumer Devices could be improved. The type of data collection referenced in Section 5.1.2, if feasible to collect, would, in fact, further degrade the data quality beyond the original findings in this report.[32]

WEA utilizes the Cellular Broadcast System to push information outward to the devices in the fastest and most reliable way possible in the cellular network. Unlike the call setup process, there is no return signaling from the device back to the network. With this restriction being understood, Section 5.2.1 focuses on location estimates from uplink traffic signals. These are random, unpredictable, and not stored. During an active alert, it is possible that some portion of

[32] One of the aspects in Section 4.2.2 of this report is the Privacy implications of the automatic reporting of WEA performance information from WEA-capable mobile devices. Collection of this highly sensitive CPNI may be in conflict with Participating CMSP, mobile device vendor, and/or OS provider privacy policies. If theses Privacy concerns are not properly addressed, it may lead to an increase of mobile device customers that choose to opt-out of WEA due to the lack of confidence in the protection and use of their personal information.

Reporting Mobile Devices (RMDs) may engage the uplink traffic channel. The CMSP's network would have no knowledge as to which devices have opted-in for WEA analytics, therefore it would only be able to report aggregate data. The AOs would have no method by which to correlate the automated reports from the RMDs with specific portions of the aggregate data from the CMSPs.

For example, say there are initially 100 devices in the Alert Area when the alert starts, and 10 of these devices have opted in for reporting, and the alert is active for 30 minutes. The CMSP may report 800 device engagements in uplink traffic over those 30 minutes. Many of these engagements may be repeated engagements from the original devices, new devices that moved into the Alert Area during the alert, and some devices that started in the Alert Area, moved out, then moved back in. If the AOs have 8 of the 10 RMDs report in, there will be no numbers to which to compare that result. They will not know that only 8 RMDs reported the alert. Assuming that a database containing all opted-in devices could be created and instantaneously updated as new devices opt-in or opt-out, aggregate data from the CMSP (no association with Personally Identifiable Information) supplies no method to determine the fact that 10 devices should have received the alert and reported, and provides no way of knowing whether the total of 800 uplink engagements came from a few devices or many. There are no calculations that can be drawn from this data.

The Alert Originators have repeatedly stated that anecdotal data is not good enough. The information, or more specifically the lack of information, produced by this type of reporting would not even qualify as anecdotal.

5.2.2.3 Privacy of Data

Additionally, Section 5.2.1 makes specific reference to responses to FCC Chairwoman Rosenworcel following her request for information about their data retention and data privacy policies and practices; one in particular is the response from AT&T.[33] As AT&T states, "(w)e welcome the opportunity to highlight the robust privacy protections, safeguards, and choices that our customers enjoy when it comes to their personal information." AT&T's global privacy program is based on four simple principles which will carry over to any WEA performance reporting:

- Transparency. We're open and honest about how we use your data.
- Choices and control. We give you choices about how we use your data.
- Security. We use strong safeguards to keep your data confidential and secure.
- Integrity. We do what we say.

There is specific mention of IQI software, developed and owned by AT&T, which is embedded in the firmware of Android devices by original equipment manufacturers ("OEMs"). IQI collects device diagnostic and location data on a passive basis (e.g., when a device powers on or contacts a new cell tower), including latitude/longitude information. AT&T Mobility uses IQI software to improve network performance and for customer service purposes. For example, AT&T Mobility uses data derived from IQI software to identify areas where it needs to enhance network coverage.

[33] https://www.fcc.gov/document/response-att-services

It should be explicitly noted that "AT&T Mobility does not share IQI data except where legally required, nor do we use it for advertising purposes." Also, this software is only available in Android devices, which represent <~50% of the market share of devices.[34] Thus, this data is not available from all devices and any attempt to use this method would provide incomplete data.

AT&T's "commitment to customers' privacy and the security of their personal information—including location information—is unwavering." AT&T explicitly states in the customer Privacy Policy that they use information collected from customers, including location data, together with the information from testing and running their network, to power their services and to improve customers' experiences. Each AT&T Mobility customer receives the AT&T Privacy Policy, which informs the customer of the criteria used to determine their practices governing retention and data destruction. As stated, "(w)e require a search warrant based on the probable cause standard for all law enforcement demands for real-time or historical location information, except for exigent requests, such as emergency requests related to kidnappings, missing person cases, and attempted suicides." AT&T does not share location data with location aggregators and location-based service providers and would not share such data with other third parties without the customer's consent.

Similar Privacy Policies are enforced by all stakeholders in the Cellular Industry.

[34] https://hypebeast.com/2022/9/apple-iphone-overtakes-androids-us-market-share a

6 Conclusions

The federal government, Cellular Industry, Alert Originators, and other WEA partners have collaborated through CSRIC over the past 10 years to make recommendations that improve WEA. As a result, the value of WEA has increased and WEA has been activated over 70,000 times to save lives and protect property. Opportunity exists to enhance WEA in ways that not only improve the conveyance of emergency information to the general public, but also to provide feedback to alert originators that will increase public safety planning and response.

Technical hurdles to enhancing WEA can be challenging. However, value remains in exploring new capabilities and enhancements to WEA that improve public safety.

It is understood that all the proposals in this report will have security considerations; due to time limitation an evaluation of security aspects of these proposals was not considered in this report.

The following table summarizes the proposals as evaluated by the Cellular Industry, listing the aspirational data desired from the AOs and an indication of whether the metric is available from the proposal:

Table 4 - Summary of the proposals presented in the report

	State/Local WEA Test	Automated Performance Reporting from Opted-in Consumer Devices	Automated Reporting from Staged Devices
With respect to accuracy:			
Number of devices inside the Alert Area which presented the WEA	**Yes**	**No**[35]	**Yes**
Total number of devices that presented the WEA	**Yes**	**No**[35]	**Yes**
Average distance outside the alert area	**Yes**	**No**[36]	**Yes**
Median distance outside the alert area	**Yes**	**No**	**Yes**
Maximum distance outside the alert area	**Yes**	**No**	**Yes**
Minimum distance outside the alert area	**Yes**	**No**	**Yes**
With respect to latency:			
The time CAP alert is originated by an alert originator.	**Yes**	**Yes**	**Yes**
The time the CAP alert is received at FEMA IPAWS	**Yes**	**Yes**	**Yes**

[35] Devices not opted-in to automated reporting may have presented.
[36] Location may not be provided with this proposal.

The time FEMA IPAWS delivers the WEA alert to each Participating CMSP	**Yes**	**Yes**	**Yes**
The time FEMA IPAWS delivers the WEA alert to PBS	**Yes**	**Yes**	**Yes**
The time that each Participating CMSP receives the alert at their CMSP Gateway	**Yes**	**Yes**	**Yes**
The time that each Participating CMSP starts broadcasting the WEA	**Yes**	**Yes**	**Yes**
The time PBS begins broadcasting the WEA	**Yes**	**Yes**	**Yes**
The time that the WEA is received at the mobile device	**No**	**Yes (if at least one device reports)**	**Yes**
The time that the WEA is presented (if presented) to the user	**Yes**	**Yes (if at least one device reports)**	**Yes**
With respect to reliability:			
The number of mobile devices that received the alert and presented it successfully	**Yes**	**No**[35]	**Yes**
The number of mobile devices that received the alert but did not present it due to being outside the Alert Area	**No**	**No**[35]	**Yes**
The number of mobile devices that received the alert, presented the alert by default due to location being unavailable (e.g., location services turned off).	**Yes**	**No**[35]	**Yes**
The number of mobile devices that received the alert but did not present due to the user's mobile device settings (e.g., opted out of AMBER alerts).	**Yes**	**No**[35]	**Yes**
The number of all mobile devices that should have received the alert.	**Yes**	**No**[35]	**Yes**
Deployment Timeline Estimate	**Available now**	**X years** (see 5.1.2.5.6)	**Z years** (similar to 5.1.2.5.6)

A. Appendix A – Additional Enhancements Discussed

A.1 Potential "Enhanced State/Local WEA Test"

A potential enhancement to the State/Local WEA Test is to include a new indicator that determines whether or not WEA Automated Performance Reporting (per the procedures in Section 5.1.2) is to be triggered upon receipt of the message in the network and at devices that have opted-in to the State/Local WEA Test. This indicator could apply to any WEA message (not just the State/Local WEA Test) and could be set by the AO on a per-alert basis.

This new triggering indicator would require new standards procedures and protocol to be developed, as this indicator does not currently exist in the State/Local WEA Test message or in any other WEA message. Such development would be over-and-above the development associated with the WEA Automated Performance Reporting capabilities described in Section 5.1.2.

A.2 Potential AO-settable Indicator to Trigger WEA Automated Performance Reporting

It is possible for an AO-settable indication to be sent with each WEA message generated by an AO which determines whether or not WEA Automated Performance Reporting is to be triggered in the network and in devices for the associated WEA message.

If WEA Automated Performance Reporting is to be initiated for each and every WEA message for all future time, then an AO-settable indication to trigger such procedures is not needed. However, to allow the AO flexibility to receive WEA Automated Performance Reporting data for only select WEA messages now and in the future, an AO-settable trigger could be developed to allow such flexibility.

The WEA Automated Performance Reporting capability as described in Section 5.1.2 would apply to all future WEA messages with no ability of the AO, the wireless operators, or the devices to stop data reporting for received WEA messages in the network and at devices unless such an AO-settable trigger indication is designed into the system as automated reporting is being developed.

Section A.1 describes the use of this trigger with the State/Local WEA Test message to create an "Enhanced State/Local WEA Test" but the trigger need not be limited to a single WEA message type and can apply to all WEA messages generated by an AO.