U.S. Department of Homeland Security
Washington, DC 20472

FEMA

August 12, 2016

Mr. Gregory Cooke
Associate Chief, Policy & Licensing Division
Public Safety & Homeland Security Bureau
Federal Communications Commission

Re: IPAWS timeliness metrics to support Earthquake Early Warning development

Dear Mr. Cooke,

In an effort to support ongoing Earthquake Early Warning research, development, and regulatory activities, IPAWS is providing Wireless Emergency Alert (WEA) and Emergency Alert System (EAS) timeliness metrics collected from the IPAWS-OPEN system (aka Federal Alert Gateway). In order to obtain the most faithful processing times, the production IPAWS-OPEN system was used. The test IPAWS-OPEN system is not built to the same capacity, load, or performance parameters as is the production system. What follows is the resulting performance metrics, data collection methodology, caveats, and supplemental raw data. Any questions should be directed to the IPAWS Program Management Office.

Performance Metrics:

	Average (s)	Min (s)	Max (s)
Round Trip Transmission from Alert Originator to IPAWS-OPEN, Plus IPAWS-OPEN Processing to getACK request, Verify Authenticity, and Generate a Response	0.141	0.095	0.384
IPAWS Processing Time	1.667	0.691	28.533

Figure 1

Data Collection Methodology:
The goal of this effort is to obtain alert timeliness metrics; how long does it take to send an alert to the public. This time measurement is influenced by a multitude of factors: The incident, alert originator process and procedures, alerting software user interface, alerting software architecture, instantaneous internet latency, IPAWS-OPEN processing time, and CMSP processing time.

A general description of these items, and their timeliness considerations are as follows:

1. Incident – Some incident types are immediate action (e.g. explosion) whereas others are slowly evolving (e.g. hurricane approaching). The nature of the incident influences the time it takes for the alert originator to identify it as a threat requiring public alerting.

2. Alert Originator Process and Procedures – The time it takes for the public safety official to exercise their incident management processes and procedures, decide to send an alert, and then take action
3. Alerting Software User Interface – The time it takes to input alert information into the alerting software. Some user interfaces are streamlined and require minimal input, whereas others require all fields to be entered manually.
4. Alerting Software Architecture – Some alerting software performs queuing, pre-validation, or other actions that increase the time between the user "hitting send" and IPAWS-OPEN receiving the alert
5. Transmission Time 1 – The time it takes for the alert to travel from the alert origination software through the public internet to reach IPAWS-OPEN
6. IPAWS-OPEN Processing Time – The time it takes for IPAWS to verify authenticity of the alert, validate the alert structure, and queue the alert for transmission to the CMSP Gateways. More complex alerts require more processing time.
7. Transmission Time 2 – The time it takes for the alert to travel from IPAWS-OPEN through the public internet (via VPN connection) to reach the CMSP Gateway.
8. CMSP Processing Time – This is thought to include CMSP gateway and CMSP network processing and distribution time

The IPAWS Program Office only has insight into processes occurring within the IPAWS-OPEN system. Approximations can be made for latency involving transmission to/from the alert origination software, and transmission to/from the CMSP Gateway. As such, only items numbered 5-7 above can be addressed here (Figure 2). The metrics collected and represented here were collected as follows:

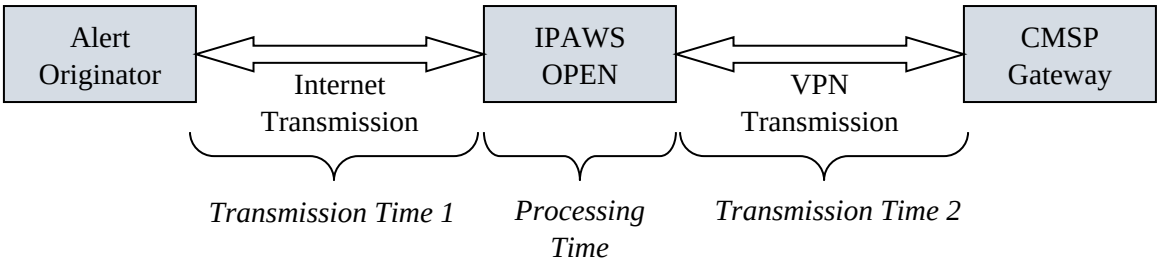

Figure 2

Transmission Time 1
The most accurate method to measure the time between Alert Originator sending an alert and IPAWS-OPEN receiving the alert is to synchronize clocks, issue the alert, and measure the delta. This is not easily accomplished, so an approximation was obtained. Using a SoapUI host as the Alert Originator, a getAck was sent. The host compared the sent time and receive time. This metric includes the round-trip internet travel and the time IPAWS-OPEN takes to process the getAck request, verify authenticity, and generate a response.

IPAWS-OPEN Processing Time

The time it takes for IPAWS to process a message is complex. Each alert is evaluated for several criteria (CAP, IPAWS Profile, WEA, EAS, NWEM, Public Feed, audio attachment, update or cancel reference, etc). Other factors influencing processing time are update and cancel messages for which the original alert referenced must be obtained in order to fully process the message. The "ideal" alert for EEW would not be evaluated for these criteria. The metrics collected for this effort include "non-ideal" alerts. Because we are concerned with WEA latency, the processing time was calculated as the time delta between IPAWS-OPEN identifying the alert as being valid for WEA (600 code) and the time the alert was received (200 code)

Note that there were some outliers in the collected metrics. For illustrative purposes, the histogram of processing times is shown here to emphasize that outliers were quite far from the average (Figure 3). Also, collected data indicates that 2.0 seconds corresponds to 95% percentile for the IPAWS-OPEN processing delay.

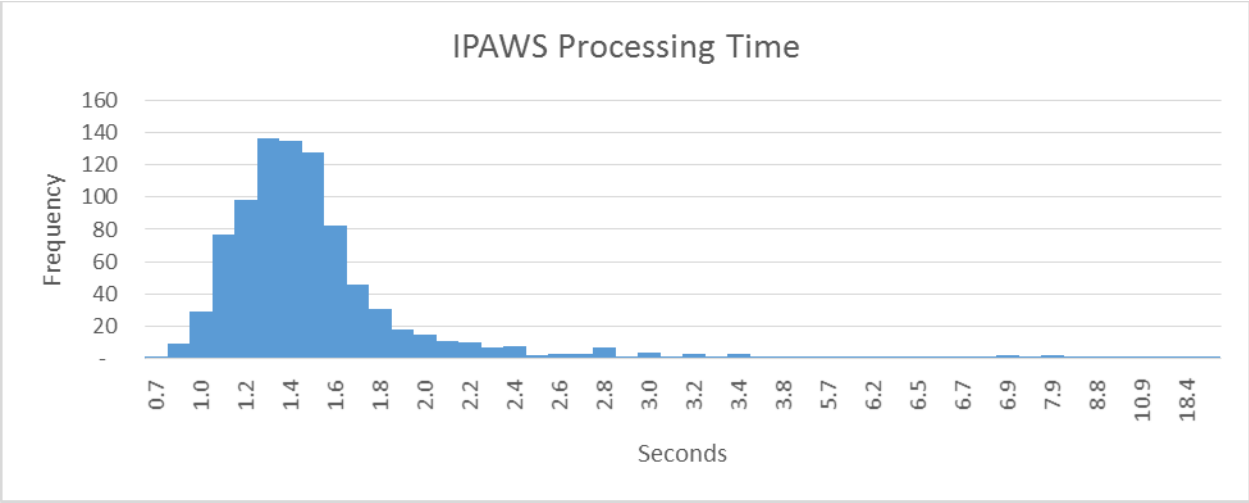

Figure 3

Caveats:

- Live testing is prohibited, therefore historical alert metrics were collected to obtain IPAWS processing time
- One-way Internet "transmission" latency between Alert Originator and IPAWS is not measured within IPAWS, so an approximation was used based on round trip timings.
- The alert complexity influences the processing time (e.g. intended for EAS, WEA, NWEM, includes polygons, includes mp3 audio, includes multiple FIPS codes).
- If EEW were to be included as a requirement for IPAWS, several performance enhancements would be made to reduce the processing latency. Essentially, a stripped down EEW alert would not require EAS validation, references to current or expired alerts, or mp3 audio attachments, therefore these functions would be omitted for this alert type.

Supplemental Raw Data:
Supplemental Raw Data can be provided by requesting from the IPAWS Program Management Office.

Respectfully,

MARK A LUCERO

Digitally signed by MARK A LUCERO
DN: c=US, o=U.S. Government, ou=Department of Homeland Security, ou=FEMA, ou=People, cn=MARK A LUCERO, 0.9.2342.19200300.100.1.1=0623735800.FEMA
Date: 2016.08.17 14:12:29 -04'00'

Mark Lucero
IPAWS Chief Engineer
National Continuity Programs
FEMA