U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

May 15, 2017

TO: Members, Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Hearing entitled "Future of Emergency Alerting."

I. INTRODUCTION

On Wednesday, May 17, 2017, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Communications and Technology will hold a hearing entitled "Future of Emergency Alerting."

II. WITNESSES

One panel of witnesses will testify.

- Sam Matheny, Chief Technology Officer, National Association of Broadcasters;
- Christopher Guttman-McCabe, Chief Executive Office, CGM Advisors, LLC; and
- Dr. Farrokh Khatibi, Director of Engineering, Qualcomm Technology.

III. DISCUSSION

As the quality of our nation's communications networks improves, so too does the ability of public safety communications to incorporate the robust capabilities of digital technologies. Earlier this year, FirstNet established a public-private partnership for the deployment of a nationwide wireless broadband network for the Nation's First Responders and steady progress is being made in the deployment of next generation 911 networks.[1] This hearing will examine the third prong of public safety communications – emergency alerting – including its current state and its future against the backdrop of these and other evolving technologies.

Today, emergency alerting consists of three general delivery mechanisms: (1) Emergency Alert System (EAS), a broadcast-based national public warning system for the delivery of alerts to warn the public of impending emergencies; (2) Wireless Emergency Alerts (WEA), a system for the delivery of emergency alerts to mobile services; and (2) social media platforms like Facebook and Twitter have been integrated into emergency preparedness, response and recovery

[1] *See* 2016 National 911 Progress Report at 3, *available at* https://www.911.gov/pdf/National-911-Program-2016-ProfileDatabaseProgressReport-120516.pdf.

activities of federal authorities and local and state authorities. Taken together, these mechanisms enable the dissemination of life-saving information at the most critical of times.

EAS

The Emergency Alert System is the nation's primary alerting system to warn the public of impending emergencies. Tracing its roots to the CONELRAD (Control of Electromagnet Radiation) system established by President Harry S. Truman in 1951, the system currently requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, and direct broadcast satellite (DBS) providers to provide communications capability to allow the President of the United States to address the American public during a national emergency.[2] In its more familiar form, EAS is used to distribute emergency alerts issued by state and local governments and weather alerts issued by the National Weather Service (NWS). The Federal Emergency Management Administration (FEMA) in partnership with the Federal Communications Commission (FCC) and National Oceanic and Atmospheric Administration (NOAA), is responsible for operating and maintaining EAS at the federal level.

As explained by the FCC, EAS is

> [A] broadcast-based, hierarchical alert message distribution system through which an alert message originator at the local, state, or federal level encodes (or arranges to have coded) a message in either the EAS Protocol or Common Alerting Protocol (CAP). If an alert originator, such as the NWS, initiates an alert using the EAS Protocol, it is transmitted from one EAS Participant to another in process that is often referred as the "daisy chain.[3]

The capabilities of internet connectivity were introduced into EAS in 2012.[4] Since then, authorized emergency alert authorities are able to distribute alerts over the internet to EAS participants by formatting those alerts in CAP, and delivering those alerts through the FEMA-administered Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (IPAWS-OPEN). [5] CAP is an open, interoperable standard. CAP

---

[2] Originally conceived at a time "when over-the-air broadcasting was the best-available technology for widely disseminating emergency alerts[.]," the inclusion of cable services, digital radio and DBS reflect upgrades in response to changing consumer consumption patterns and innovations in technology. *See Emergency Alerting, Capabilities Have Improved, but Additional Guidance and Testing Are Needed*, United States Government Accountability Office, GAO-13-375, April 2013, *available at* https://www.gao.gov/assets/660/654136.pdf.

[3] *See* In the Matters of Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System Wireless Emergency Alerts, PS Docket No. 15-94, PS Docket No. 15-91 Notice of Proposed Rulemaking,(*EAS NPRM*) (rel. Jan. 29, 2016) paras 6-8, *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-5A1.pdf.

[4] *Id*. at para 7.

[5] FEMA initiated IPAWS in 2004 to integrate EAS and other public alerting systems into a comprehensive alerting system. In 2006, Executive Order No. 13407 entitled "Public Alert and Warning System" was issued adopting a policy that the United States have a comprehensive, integrated alerting system. Pursuant to that policy, the Secretary of Homeland Security was directed to transition existing capabilities into a coordinated and integrated system. IPAWS is that system.

formatted alerts can include audio, video, or data files; images; multilingual translations of alerts; and weblinks providing additional information which EAS Participants (television and radio broadcasters, cable systems, DBS) can broadcast to the public.[6]

On September 28, 2016, FEMA, in coordination with its partner agencies, conducted the second nationwide test of EAS to assess the reliability and effectiveness of the IPAWS distribution architecture and improvements to EAS following the first nationwide test of the system in 2011. In its report analyzing the test, the FCC's Public Safety and Homeland Security Bureau (Bureau) concluded that "a range of operational and technical issues still remain" that affect EAS performance.[7] Among those identified was the observation that "[a]lmost half of test participants received the test over-the-air rather than from IPAWS, and these participants were unable to deliver the CAP-formatted digital audio, Spanish, and text files as a result."[8] In response to these observations, the Bureau recommended, among other things, that the FCC should facilitate and encourage the use of IPAWS as the primary source of alerts nationwide and "examine how to improve and expand the content included in IPAWS alerts to bridge the gap between today's alerting systems and future next generation alerting."[9]

As the FCC and its partners consider these recommendations and next steps, television broadcasters have proposed to move the industry to its next generation broadcast platform also known as ATSC 3.0.[10] ATSC 3.0 is an Internet Protocol-based system and according to its proponents, merges the capabilities of over-the-air broadcasting with the broadband viewing and information delivery methods of the Internet. Proponents also tout the new standards' potential to allow broadcasters to offer innovative technologies and services to consumers, improved over-the-air reception on televisions and mobile devices, IP-based transport streams, enhanced mobile capability, more localized content, better accessibility options, and, importantly, advanced emergency alerting.[11] ATSC 3.0 could enable advancements in emergency alerting that include geo-targeting of emergency alerts to tailor information for particular communities and the capability to "wake up" receivers to alert consumers to emergencies and disasters.[12] Proponents of ASTC-3 deployment have joined to develop and deploy the Advanced Warning and Response Network (AWARN) around these and other capabilities to "enhance emergency preparedness and surpass the current EAS system."[13] The FCC recently sought comment on rules that will

---

[6] CAP provides each alert with a unique identifier and supports authentication through the provision of a digital signature and an encryption fields that enables greater protection of the message.
[7] *See Report: September 28, 2016 Nationwide EAS Test*, Federal Communications Commission, April 2017 (*EAS Test Report*) *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-344518A1.pdf.
8 *EAS Test Report* at 3
[9] *Id*.. The FCC released a Notice of Proposed Rulemaking in January of 2016 seeking comment on among other things, ensuring that alerting mechanisms are able to leverage advancements in technology, including IP-based technologies. *See EAS NPRM*.
[10] *See* Joint Petition for Rulemaking of America's Public Television Stations, the AWARN Alliance, the Consumer Technology Association, and the National Association of Broadcasters, GN Docket No. 16-142 (*ATSC 3.0 Joint Petition*) (filed Apr. 13, 2016), *available at* https://www.fcc.gov/ecfs/filing/60001667342/document/60001701021.
[11] *Id.*
[12] *Id* at 5.
[13] *See* https://www.thebroadcastbridge.com/content/entry/2812/awarn-seeks-to-become-the-nationals-premiere-emergency-warning-system.

allow broadcasters the flexibility to deploy ATSC 3.0 with the release of a notice of proposed rulemaking in February.[14]

Wireless Emergency Alerts

In 2006, in recognition of the public's increasing reliance on wireless services and devices to communicate, Congress provided for the expansion of emergency alerting to mobile services with the enactment of the Warning, Alert and Response Network (WARN) Act.[15] The WARN Act required the FCC to adopt "relevant technical standards, protocols, procedures, and other technical requirements . . . necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts," which it did in 2008 with the establishment of Wireless Emergency Alerts (WEA).[16] WEA permitted federal, state, and local government entities to geographically target 90-character Presidential, Imminent Threat, and AMBER Alerts to the WEA-capable mobile devices of Participating CMS Providers' subscribers.

Like EAS, a WEA Alert Message is sent using CAP. The message is relayed to the FEMA-operated alert aggregator via a secure, internet-based interface where it is authenticated, validated, and subsequently delivered to FEMA's alert gateway. At the FEMA alert gateway, the message is prepared for delivery to a participating wireless provider. The message is then sent across a secure internet-based connection to the participating provider for distribution to mobile subscribers.[17]

In 2016, the FCC took steps to "take advantage of the significant technological changes and improvements experienced by the mobile wireless industry" since 2008 and improve WEA.[18] Among other things, the FCC increased the maximum alert message length from 90 to 360 characters for 4G-LTE and future networks; created a new alert message classification for "Public Safety Messages," defined as "an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property;" required participating providers to support embedded references (*i.e.*, URLs and phone numbers) included in alert messages; required participating providers to support transmission of Spanish-language alert messages; and,

---

[14] *See Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard*, GN Docket No. 16-142, Notice of Proposed Rulemaking, (Rel. Feb. 24, 2017*) available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-13A1.pdf.

[15] Title VI of the Security and Accountability For Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (2006).

[16] WEA was formerly known as the Commercial Mobile Alert System or CMAS. The FCC changed the name "Commercial Mobile Alert System" to "Wireless Emergency Alert" in 2013.

[17] Wireless subscribers may opt out of receiving alerts but may not opt out of receiving presidential alerts.

[18] *In the Matter of Wireless Emergency Alerts, Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-91, PS Docket No. 15-94, Notice of Proposed Order and Further Notice of Proposed Rulemaking, (*WEA Order*) (rel. Sept. 29) *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-127A1.pdf.

required participating providers to narrow their geographic targeting (geo-targeting) of alert messages to areas that best approximate alert areas specified by the alert originator.[19]

In addition to adopting these upgrades, the FCC also sought comment on the feasibility and costs of additional measures to upgrade WEA. These include requiring support for certain multi-media content, including thumbnail-sized images and hazard signals in alert message and expanding the language capabilities of WEA beyond English and Spanish.[20] The FCC also sought comment on more granular geo-targeting of alert messages such that providers match the target area specified by alert originators so that only devices in the geographic area affected by an event receive the alert, and no devices outside the impacted area would receive.[21]

Social Media

In addition to EAS and WEA, social media platforms such as Twitter and Facebook have emerged as mechanisms for emergency communications.[22] The rise of these platforms as alerting tools coincides with the emergence and proliferation of mobile services. Although not regulated, social media has been integrated into emergency preparedness, response, and recovery activities at the federal, local, and state levels augmenting EAS and WEA.[23]

While it is broadly recognized that social media tools may offer benefits to public safety authorities, *e.g.*, social media tools allow emergency managers to disseminate information, monitor social media networks for better situational awareness, and improve collaboration for sharing information during an event,[24] it is also recognized that there are challenges with their use. It has been noted that "government entities seeking to assess the extent of and impacts from emergency situations are challenged by social media reports that are difficult to validate, can give a distorted view of the greatest community need, and are prone to spoofing and other malicious activity."[25] Extensive work has been undertaken and continues in both academia and public safety to ascertain the impact and use of social media in times of emergency and as an alerting tool.

Emergency alerting continues to evolve, improving incrementally with advancements in communications technologies. These advancements and future possibilities will be examined.

IV. STAFF CONTACTS

[19] "Geo-targeting" alerts refers to the ability of the WEA architecture to direct an alert to a geographic area that matches that desired by the alert originator.
[20] *WEA Order* at paras 126-137.
[21] *Id*. at paras 138-145.
[22] *See e.g.*, *EAS NPRM* at para 11.
[23] *See Alerts and Warnings Using Social Media Project Fact Sheet*, Department of Homeland Security, *available at* https://www.dhs.gov/publication/alerts-and-warnings-using-social-media-project.
[24] *See e.g.*, 5 ways to use social media for better emergency response, GCN, (2010) *available at* https://gcn.com/articles/2010/09/06/social-media-emergency-management.aspx.
[25] *See EAS NPRM* at para 11.

If you have any questions regarding this hearing, please contact Kelsey Guyselman or Gene Fullano of the Committee staff at (202) 225-2927.