

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of )  
 )  
Impact of Unauthorized EAS Alerts ) PS Docket No. 14-200

**COMMENTS OF  
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association<sup>1</sup> (NCTA) hereby submits its comments in response to the Public Safety and Homeland Security Bureau's request for comment on the impact of unauthorized Emergency Alert system (EAS) messages on EAS Participants and public safety. The Bureau opened this inquiry into the technical, operational and policy implications of unauthorized EAS alerts in response to an October 24, 2014 incident involving the transmission of an erroneous Emergency Action Notification (EAN) event code by a syndicated radio broadcast show in several states. In the Public Notice, the Bureau seeks input on ways EAS Participants and EAS equipment can improve message authentication to prevent such occurrences in the future.

**Background**

In response to the October 24<sup>th</sup> incident, NCTA issued an advisory to our member companies as soon as we became aware of the unauthorized EAN transmission by the syndicated radio broadcast that may have been retained in EAS equipment. We understand that EAS vendors also notified their customers and provided detailed instructions on how to cancel

---

<sup>1</sup> NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over \$210 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 27 million customers.

unauthorized national EANs from the alert queue in their EAS encoder/decoder equipment. Depending on the type of equipment and system configuration, the spurious alert was cached in some cable systems pending automatic transmission on November 9th, the date stamp in the event code. Those companies affected immediately responded to the advisories in coordination with their vendor to remove the EAN. Based on NCTA's follow-up with our member companies, no cable system inadvertently retransmitted the unauthorized EAN on November 9, 2014.

### **Impact to EAS Participants**

Cable systems disseminate EAS messages at the state and local level by retransmitting emergency information on an automated basis as it is received from a local primary broadcast station(s) or directly from an EAS originating source, such as the National Weather Service. Most cable systems monitor one or two local primary ("LP") stations and disseminate the EAS messages received from the stations to their customers.

In general, unauthorized EAS alerts, including EANs, are a rare occurrence in the EAS ecosystem. During the October 24<sup>th</sup> incident, in some limited cases cable EAS equipment instantly forwarded the EAN message, and in other cases equipment cached it for release on the date and time set in the header code (November 9<sup>th</sup>). The difference in the way different types of EAS Participant's equipment responded related more to the equipment vendor and equipment configuration than to the type of participant (e.g. broadcast, cable, others). As noted above, once notified of the incident, cable operators followed the instructions provided by their EAS vendor to eliminate the erroneous EAN.

The Bureau also asks how EAS equipment handles the absence of an End of Message (EOM) code. In the case of typical, non-EAN alerts, EAS equipment times out after two minutes

and normal programming resumes if an EOM is not received. If an EOM is not received for an EAN alert, most equipment requires that the operator manually reset the equipment in order for normal programming to resume.

### **Message Authentication**

In activating an EAS alert, cable operators follow the four-part message protocol set forth in the Commission's rules.<sup>2</sup> The "header code" element contains basic information about the alert, including the identity of the message originator, the type of event, the geographic location for the alert, the valid time period for the message, the date and time of release of the message by its originator, and the identity of the entity transmitting the message. This information is important to the proper handling and routing of all incoming EAS messages. The required elements of an EAS message also provide a level of security to the system, making it less susceptible to security threats and discrepancies in dissemination of alerts. However, the EAS protocol was not designed nor does it possess the means to *authenticate* the source of the message.

The Bureau asks whether EAS Participants have implemented "strict time" filters on EAS equipment, as recommended by the Federal Emergency Management Agency (FEMA) as a short-term fix.<sup>3</sup> In previous NCTA comments in the EAS docket, we recommended that message originators properly encode the "time of release" element of the header protocol to reflect the time that the message is actually released to ensure that EAS messages are transmitted securely and routed accurately.<sup>4</sup> But we appreciate the Commission's assertion in its recent Notice of

---

<sup>2</sup> 47 C.F.R. § 11.31 (the four parts are: preamble and header codes; audio attention signal; message; and preamble and End of Message codes).

<sup>3</sup> Public Notice at 3.

<sup>4</sup> See NCTA Comments, EB Docket No. 04-296 (filed Aug. 14, 2014); NCTA Comments, EB Docket No. 04-296 (filed Nov. 4, 2013).

Proposed Rulemaking on the technical and operational issues identified from the 2011 nationwide EAS test that EAS equipment should run the EAN immediately whether or not the date and time information of the message matches the actual release time.

The Bureau also asks what actions can be taken, either technically or operationally, to enhance EAS alert authentication. NCTA recommends that the government explore ways to verify the source of the message through implementation of the Integrated Public Alert and Warning System (IPAWS) Common Alerting Protocol (CAP). CAP uses advanced technology to permit emergency warnings to multiple information networks, public safety alerting systems, and personal communications devices through existing EAS infrastructure. Cable systems and other EAS participants deployed CAP pursuant to Commission rules adopted in 2007, and today are able to receive and disseminate CAP-formatted EAS alerts. According to FEMA, CAP technology may permit further enhancements to EAS to ensure that messages are issued from a trusted source:

FEMA IPAWS is furnishing the message authentication and message aggregation pieces for CAP/EAS. Alerting officials can compose a CAP message using any of a number of authoring tools, the message originator's credentials will then be checked and the message posted to the aggregator. Properly constructed messages will then be available for retrieval by CAP enabled EAS devices for broadcast and cable operators . . . [t]he IPAWS Aggregator confirms that the source of an alert is an authorized IPAWS user.<sup>5</sup>

In the years since CAP deployment, state and local emergency management agencies generally have not deployed the transmission equipment to create CAP alerts. On the national level, we understand that FEMA has chosen not to use CAP messaging for national Presidential alerts because of the difficulty in supporting audio streaming. Audio streaming is necessary to permit the unlimited alert duration required of a national alert under 47 CFR section 11.33(a)(9).

---

<sup>5</sup> [https://www.fema.gov/pdf/emergency/ipaws/cap\\_ipaws\\_faq.pdf](https://www.fema.gov/pdf/emergency/ipaws/cap_ipaws_faq.pdf).

Despite these obstacles, CAP may be an avenue for improved authentication once the technology is fully utilized at the federal and state level.

In the meantime, as the Notice points out, the Bureau's inquiry builds on the recommendations contained in the Communications Security, Reliability and Interoperability Council (CSRIC) June 2014 report on EAS security and reliability.<sup>6</sup> The EAS Security Best Practices developed by the EAS working group and adopted by the Commission recommend, among other things, that EAS Participants follow certain protocols to minimize any security vulnerabilities in EAS. For example, EAS participants should always use a firewall between EAS equipment and the public Internet to reduce unknown external actors from compromising the system. Best practices related to passwords, user accounts, user restrictions, and vendor software patches and security notifications are also covered. The report further recommends that "EAS devices should be configured to validate digital signatures on CAP messages if the source of the CAP message requires this feature. This will prevent spoofed or otherwise altered alerts from being aired."<sup>7</sup> The cable industry supports these recommendations and follows basic network security protocols for EAS as for any other functions and services on their broadband networks.

---

<sup>6</sup> *Initial Report, CSRIC WG3 EAS Security Subcommittee Report:*  
[http://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG-3\\_Initial\\_Report\\_061814.pdf](http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial_Report_061814.pdf).

<sup>7</sup> Report at p. 12.

In providing consistently dependable networks, cable operators continuously work to assess, deter, and neutralize network security vulnerabilities and threats as a central part of their enterprise risk management strategy. To achieve the next level of security for EAS, we recommend that the Commission explore methods to build on the existing EAS infrastructure to improve message authentication.

Respectfully submitted,

**/s/ Rick Chessen**

Andy Scott  
Vice President of Engineering

Rick Chessen  
Loretta Polk  
National Cable & Telecommunications  
Association  
25 Massachusetts Avenue, N.W. – Suite 100  
Washington, D.C. 20001-1431  
(202) 222-2445

December 5, 2014