WORKING GROUP 3
Emergency Alert System (EAS)

EAS Security Subcommittee
Final Report
March 2015

Table of Contents

1 Results in Brief 3
1.1 Executive Summary 3
2 Introduction 4
2.1 CSRIC Structure 4
2.2 Working Group 3 EAS Security Subcommittee Team Members 5
3 Objective, Scope, and Methodology 7
3.1 Objective 7
3.2 Scope 7
3.3 Methodology 7
4 Background 8
5 Recommendations 10
5.1 Outreach Pathways 11
5.1.1 Government 11
5.1.1.1 FCC 11
5.1.1.2 FEMA 12
5.1.2 Industry Stakeholders & Constituencies 12
5.2 Outreach Methods 13
6 Conclusions 15

1 Results in Brief

1.1 Executive Summary

The Federal Communications Commission (Commission or FCC) established the Communications Security, Reliability and Interoperability Council (CSRIC) "…to provide recommendations...to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety." To achieve that goal, CSRIC IV established and chartered ten "Working Groups" to examine the various issues of concern in these areas.

Working Group 3 (WG3) was formed to develop recommendations for the CSRIC's consideration regarding any actions the FCC should take to improve the Emergency Alert System (EAS). WG3 was divided into three subcommittees: one to review FCC rules and processes concerning state EAS Plans, one regarding EAS security, and one to address EAS Operational Issues and the Nationwide EAS Test. Each group worked with specific tasks and questions, as assigned by the Commission and the CSRIC.

This document was prepared by the CSRIC WG3 subcommittee on EAS security. It identifies the principal groups associated with EAS as: EAS Participants, emergency alert originators, EAS device manufacturers, the federal government, and local emergency managers. This document complements the Initial Report submitted to the CSRIC by this subcommittee in June 2014 (WG3 Initial Report) (available here). The WG3 Initial Report addressed the need for information assurance and security controls throughout the EAS ecosystem in the form of best practices guidelines for each of the relevant stakeholders.

This report seeks to provide recommendations on how the Commission can promote and facilitate both awareness and adoption of the "best practices" guidelines contained in the WG3 Initial Report.

2 Introduction

CSRIC IV Working Group 3 was established to develop recommendations for the CSRIC's consideration regarding any actions the FCC should take to improve the EAS.

To tackle the issues relevant to EAS, a diverse team of Subject Matter Experts was recruited to participate. The following areas of expertise are represented within the group.

- Message Originators: the Federal Emergency Management Agency (FEMA), the National Weather Service (NWS), State & Local Emergency Managers; State EAS Networks.
- EAS Participants: Radio; TV; Cable TV; Satellite TV; Satellite Radio.
- EAS Equipment Manufacturers.
- State Emergency Communications Committees, EAS Experts and Consultants.
- Public Interest, Persons with Disabilities.

CSRIC Working Group 3 is divided into three sub-groups:

- **State EAS Plans**. Recommend steps to improve the process for developing and submitting state EAS plans to the Commission. Consider the formation and role of State Emergency Communications Committees (SECCs), and processes for optimizing the EAS while minimizing burdens on EAS stakeholders. This subcommittee submitted its final report to the CSRIC in March 2014.
- **Nationwide EAS Test/Operational Issues**. Address and explore operational issues that arose during the nationwide EAS Test in November 2011. This subcommittee submitted its final report to the CSRIC in June 2014.
- **EAS Security**. Recommend actions to improve promote the security of the EAS. This subcommittee submitted its initial report to the CSRIC in June 2014.
    - As documented herein, CSRIC subsequently tasked WGs with addressing outreach and awareness regarding the recommendations contained in the WG3 Initial Report.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Working Group 1 Next Generation 911	Working Group 2 Wireless Emergency Alerts	Working Group 3 EAS	Working Group 4 Cybersecurity Best Practices Working	Working Group 5 Server-Based DDoS Attacks	Working Group 6 Long-Term Core Internet Protocol Improvements	Working Group 7 Legacy Best Practice Updates	Working Group 8 Submarine Cable Landing Sites	Working Group 9 Infrastructure Sharing During Emergencies	Working Group 10 CPE Powering

2.2 Working Group 3 EAS Security Subcommittee Team Members

Working Group 3 consists of the members listed below. The WG3 Security subcommittee for this Final Report consists of two Co-Chairs: Gary Smith and Larry Walke.

Name	Affiliation(s)
Adrienne Abbott	Nevada EAS Chair
John Archer	SiriusXM
John Benedict	CenturyLink
Ron Boyer	Boyer Broadband
Ted Buehner	Warning Coordination Meteorologist National Weather Service
Ben Brinitizer	Society of Broadcast Engineers
Lynn Claudy	National Association of Broadcasters
Roswell Clark	Cox Media Group
Kimberly Culp	Larimer Emergency Telephone Authority
Edward Czarnecki	Monroe Electronics
David Donovan	President, NY State Association of Broadcasters
Chris Fine	Goldman Sachs
Clay Freinwald (WG 3 co-chair)	Clay Freinwald Technical Services / Chair, Washington State SECC
Les Garrenton	LIN Media
Mike Gerber	NOAA
Suzanne Goucher	Maine Association of Broadcasters / Chair, Maine SECC
Neil Graves	SNR Systems (formerly FEMA IPAWS)
William Hickey	Premiere Radio Networks
Craig Hoden	NOAA
Chris Homer	Public Broadcasting Service
Steve Johnson	Johnson Telecom
Alfred Kenyon	FEMA IPAWS
Mark Lucero	FEMA
Wayne Luplow	LGE/Zenith Electronics
Bruce McFarlane	Fairfax County
Dan Mettler	Clear Channel Media + Entertainment / Chair Indiana SECC
David Munson	FCC Liaison
Brian Oliger	Hubbard Radio/WTOP
Darryl Parker	TFT, Inc.
Rich Parker	Vermont Public Radio /Chair, Vermont SECC
Jerry Parkins	Comcast Cable
Efraim Petel	AtHoc, Inc.
Richard Perlotto	Shadowserver Foundation
Joey Peters	MyStateUSA, Inc.
Peter Poulos	Citi
Harold Price	Sage Alerting Systems

Richard Rudman	Broadcast Warning Working Group / Vice Chair, California SECC
Francisco Sanchez, Jr.	Harris County (TX) Office of Homeland Security
Tim Schott	NOAA
Andy Scott	V.P. Engineering, NCTA
Bill Schully	DIRECTV
Gary Smith	Cherry Creek Radio, Arizona SECC
Matthew Straeb	Global Security Systems/ALERT FM
Gary Timm	Broadcast Chair, Wisconsin SECC
Leonardo Velazquez	AT&T U-Verse
Larry Walke (WG3 co-chair)	National Association of Broadcasters
Michael Watson	Gray Television Group
Kelly Williams	NAB
Reed Wilson	Belo Corp.

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

The charter for CSRIC IV calls on WG3 to "develop and provide recommendations on how the Commission can promote and facilitate both awareness and adoption of the "best practices" guidelines contained in the WG3 Initial Report. Particular focus should be placed on awareness and adoption by EAS Participants and, in particular, the smaller sized entities least likely to be aware of such guidelines, unsure of which guidelines would be applicable to their operational situations, uncertain as to how to implement those that do apply. Recommendations should also provide guidance to help such entities overcome the obstacles that similarly situated EAS participants face.

3.2 Scope

The EAS Security Subcommittee considered the following sectors of the EAS ecosystem regarding outreach and enhanced implementation of EAS security measures:

- EAS Participants.
- Emergency Alert Originators.
- EAS Device Manufacturers.
- U.S. Government.
- Industry Associations.

This document addresses the immediate need to permeate the EAS ecosystem with information and guidance regarding the security of EAS. Accordingly, we considered a host of methods for increasing the awareness of all EAS stakeholders, including:

- Government-issued notices and documents.
- Internet-based outreach (*e.g.*, webcasts, email, social media).
- Newsletters, trade publications.
- Education programs at conferences and conventions.
- Direct outreach to state-level EAS committees.

3.3 Methodology

The subcommittee used a collaborative, inclusive approach. Given the vast expertise of various members, it was important to provide an open forum through which participants could express their opinions and help shape this report. These discussions largely took place during a series of weekly conference calls moderated by the subcommittee co-chairs: Gary Smith of Cherry Creek Radio and Larry Walke of the National Association of Broadcasters.

4 Background

EAS is the primary national warning system that provides the President with the means to address the nation during a national crisis. State and local officials also use EAS to issue warning messages about imminent or ongoing hazards in specific regions. Three Federal agencies share responsibility for administering EAS: the FCC, FEMA, and the National Weather Service.

Functionally, EAS is a hierarchical alert message distribution system. Initiating an EAS message, whether at the national, state, or local level, requires the message initiator to deliver specially-encoded messages to a broadcast station-based transmission network that, in turn, delivers the messages to individual broadcasters, cable operators, and other EAS Participants. EAS Participants maintain special encoding and decoding equipment that can receive the message for retransmission to other EAS Participants and to end users (broadcast listeners and cable and other service subscribers).

The Integrated Public Alert and Warning System (IPAWS) is the Nation's next generation public alerting system. It is designed to improve public safety through the rapid dissemination of emergency messages to as many people as possible over as many communications devices as possible. IPAWS builds additional redundancy in EAS by establishing diverse dissemination paths including Internet Protocol networks. IPAWS accepts standards-based alert and warning messages generated by emergency managers using existing state, local, tribal, or territorial systems, or an IPAWS web interface. These common alerting protocol (CAP) formatted messages are then forwarded to the FEMA IPAWS aggregator, which disseminates the message through all distribution means.

Since its inception, EAS has had vulnerabilities that have resulted in both accidental and deliberate dissemination of unauthorized EAS alerts. Human error, the retransmission of outdated alerts and the intentional transmission of the EAS data bursts accompanied by the two-tone attention signal by unauthorized parties have been documented.

The addition of the common alerting protocol (CAP) adds another gateway for unwanted intrusion into the system through the public internet. CAP requires all EAS decoders to be able to decode and relay CAP-formatted EAS messages which are delivered over an Internet Protocol (IP) network from any of a number of government and private CAP aggregators. Cyber-intrusions and attacks, whether by viruses, malware, spyware, or other Information Technology (IT) security breaches – are on the rise in in both public and private enterprise. EAS Participants now face additional vulnerabilities as IP integration introduces a new gateway into the system. Unauthorized EAS breaches over the past two years have illustrated that operational security challenges range from those that could have been prevented by very

fundamental, common-sense measures, to those that may require proactive efforts by the EAS Participant to better secure their IT enterprise.

The first step towards minimizing security risks to EAS is the development of recommendations that are flexible and adaptable to various stakeholders in the EAS ecosystem. As mentioned, the WG3 Initial Report contains such "Best Practices."[1]

The next step requires education, increased awareness, and implementation of those recommendations among EAS participants and other critical components of the EAS system. It is vital that information and guidance is provided to all entities, including those in small and rural communities, given both the "daisy-chain" nature of traditional EAS and the IP nature and dependence of CAP-enabled EAS, as well as the confusion that can result from the broadcast of improper or unauthorized EAS messages. It is these smaller-sized entities that are most likely found at the end of the chain, and most vulnerable to digital disruptions of their EAS operations. EAS Participants must increase their awareness of the need to put basic policies, processes and products in place to protect both themselves and the integrity of the nation's public warning system.

Smaller-sized and rural broadcast entities often face particular challenges in maintaining awareness of current security measures, due to limited human, financial or technical resources. In the case of smaller and rural radio stations, for example, many do not employ a full-time engineering or operations staff, instead relying on independent technical consultants that may handle operations and engineering matters for multiple stations within a particular geographic region. While these consultants may possess a range of technical skills and expertise, cybersecurity may not be one of them. Moreover, the cost of needed upgrades, security issues and the time it takes to fix problems may pose additional financial and resource challenges for smaller and rural EAS Participants, compared to larger and better resourced operations. For the same reasons, these broadcast EAS Participants may find it more difficult to maintain awareness of FCC actions or recommendations regarding EAS security.

It is important that EAS Participants understand that neither the size of their operations, nor the particular type of their business, lessen the risk from vulnerabilities or a cyberattack. EAS Participants must appreciate that if they use the Internet – as required for CAP-enabled EAS, and increasingly for other routine functions – they are vulnerable. The goal of WG3 is to disseminate information about the best practices recommended by CSRIC, with the ultimate objective of encouraging EAS Participants to implement measures that reduce the risk of cyber breaches.

[1] The WG3 Initial Report recommends measures concerning password security, firewalls, equipment maintenance, secure physical and remote access to equipment, and awareness of equipment manufacturer notifications, among other steps. WG3 Initial Report at 11-13.

For these reasons, it is critical that consistent, tailored outreach methods be devised and implemented to successfully penetrate the awareness of the full range of EAS participants. WG3 considered this specific challenge in the development of the recommendations set forth below. We considered the various industry groups that represent EAS participants, equipment manufacturers that maintain communications with their customers for purposes of system software upgrades and other product opportunities, and government agencies like the FCC that license or authorize the operations of all EAS participants.

5 Recommendations

WG3 recommends that the Commission develop and implement a schedule of multi-faceted programs designed to educate the universe of EAS stakeholders regarding EAS security, with a particular focus on outreach to smaller-sized and rural EAS participants. An important component of these efforts centers on the content of such education. The WG3 Initial Report contains a comprehensive list of cybersecurity best practices for the various sectors of the EAS ecosystem, including EAS participants, EAS message originators and other government bodies, and equipment manufacturers. However, that document was designed for purposes of review by CSRIC members, most of whom have some expertise in security or network issues. Accordingly, that report has a somewhat complex format,[2] sets forth only general categories of recommendations, and lacks any detailed guidance on implementing the recommendations, thereby making it ill-suited for a public advisory item.

For purposes of enhancing cybersecurity awareness among all EAS participants, WG3 recommends that the Commission consider developing a series of cybersecurity best practices items. First, the Commission should prepare a user-friendly, manageable list of recommended best practices for mitigating security risks to the EAS system of relevance to the broad spectrum of EAS stakeholders.[3] In addition, the Commission should consider creating a set of best practices targeted to more narrow subsets of the EAS ecosystem, non-enterprise based networked facilities such as smaller and rural radio EAS participants, small cable systems, and large television groups, among others. This approach should improve the Commission's success in raising awareness of cybersecurity risks among all EAS participants, and more importantly, widespread implementation of measures designed to minimize those risks. Such a program would also best enable state EAS committees, industry associations and other organizations to support and extend the Commission's outreach efforts, as discussed below.

[2] The format of the WG3 Initial Report largely mirrors the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the National Institute of Standards and Technology (NIST) in February 2012 (available here).

[3] WG3 notes that the appendix to the FCC's Public Notice seeking comment on implementation of best practices contained in the WG3 Initial Report could serve as a model for such a document (available here).

The best practices should be prominently displayed and readily accessible on the FCC's website, and repeatedly flagged in relevant Commission documents and other venues. Below we offer a series of specific proposals for educating EAS participants on cybersecurity risks and mitigation measures.

5.1 Outreach Pathways

5.1.1 Government

5.1.1.1 FCC

FCC EAS Handbook. The EAS Operating Handbook summarizes the actions to be taken by personnel at EAS Participants' facilities upon receipt of an Emergency Alert Notification (EAN) or State and Local Area alert. The Handbook is issued by the FCC, and a copy of the Handbook must be located at normal duty positions or EAS equipment locations when an operator is required to be on duty and be immediately available to staff responsible for authenticating messages and initiating actions. 47 C.F.R. § 11.15. The FCC issues several Handbooks, tailored for different categories of users: (1) TV; (2) AM, FM and digital audio; (3) cable systems; (4) satellite; and (5) wireline video providers.

Given the duty to maintain the EAS Handbook on site, and the fact that it is particularized to various categories of EAS Participants, the handbook is an ideal resource for information on cybersecurity. WG3 thus recommends that the Commission modify each EAS Handbook to include recommended best practices for reducing cybersecurity risks, relevant to each group of EAS participants.

FCC Webinars & Webcasts. The Commission periodically conducts online webinars and webcasts on various policy issues, including security-related topics, such as Public Safety Answering Point architecture, text-to-911, and 911 certification. WG3 recommends that the Commission hold an interactive webcast aimed at educating EAS participants regarding cybersecurity. Such an event should be held in the near future following the close of CSRIC IV -- no later than during October in connection with National Cybersecurity Awareness month -- and thereafter annually in October, at a minimum.

Public Advisories and Notices. WG3 recommends that the Commission issue a Public Advisory to all EAS Participants reminding them of the digital vulnerabilities of EAS systems and equipment, and recommending a list of best practices for addressing those vulnerabilities. Such recommendations should also be noted in other EAS-related documents, including docketed proceedings and FCC staff speeches and remarks.

5.1.1.2 FEMA

FEMA's IPAWS Program Office has conducted several webinar series that have covered a number of relevant topics:

Alert Origination Service Provider Series.
This series showcased products from vendors that have a Memorandum of Agreement with IPAWS to demonstrate connectivity and validation of alerts sent to the IPAWS Lab at the Joint Interoperability Test Command (JITC) in Maryland (*e.g.*, WEA, EAS, NWEM) and user interfaces with the consumer (*e.g.*, geotargeting, selection criteria).

Unique Alert Services.
This event showcased products from vendors that are designed to monitor the IPAWS All-Hazards Information Feed (IPAWS Public Feed) and redistribute them through various channels (*e.g.*, internet, subscriptions, digital signs).

Alerting Best Practices Webinar Series.
IPAWS is currently offering webinars of a wide range of topics that pertain to Alerting Authorities, Law Enforcement, the General Public, and a variety of information related to the Integrated Public Alert and Warning System and its components

- The IPAWS program was also were featured on the International Association of Emergency Managers' audience, as well as the National Crime Prevention Council's audience.
- The most recent webinar, held on January 21, 2015, showcased demonstrations of the Lexington-Fayette Urban Division of Emergency Management and Fairfax County Office of Emergency Management on how to test their alert origination software with the IPAWS Lab at JITC.

FEMA intends to continue these outreach efforts, and distribute information related to the security of EAS, including CSRIC's EAS security recommendations, as appropriate.

5.1.2 Industry Stakeholders & Constituencies

Below is a non-exhaustive list of industry organizations that could be instrumental in supporting the Commission's efforts to educate EAS Participants regarding cybersecurity. Many of these groups have annual or periodic conventions, conferences or meetings, regularly distribute news updates and emails to their members, and offer other educational content. WG3 recommends that the Commission invite these and similar organizations to extend its cybersecurity outreach efforts through targeted guidance to their constituencies.

- American Cable Association (ACA)
- Association of Public Television Association (APTS)
- Consumer Electronics Association (CEA)
- CTIA – The Wireless Association
- Low power FM radio organizations

- National Alliance of State Broadcasting Associations (NASBA)
- National Association of Broadcasters (NAB)
- National Association of College Broadcasters (NACB)
- National Cable & Telecommunications Association (NCTA)
- National Federation of Community Broadcasters
- National Public Radio (NPR)
- NTCA – The Rural Broadcast Association
- Public Broadcasting Service (PBS)
- State Broadcasters Associations (various)
- Society of Broadcast Engineers (SBE)
- Society of Cable Telecommunications Engineers (SCTE)

5.2 Outreach Methods

WG3 recommends that the Commission develop a series of best practices based on the recommendations in the WG3 Initial Report, and publicize these practices through a webcast and other means. The FCC's efforts could be supplemented by targeted outreach from industry organizations to their constituencies through some of the methods listed below. Where noted, outreach by specific groups are offered only as examples of existing projects in this area.

Webcasts, webinars, teleconferences. Broadcast engineering trade groups such as SBE and SCTE frequently offer educational and training webinars to their membership. The completion of these webinars may be applied by members toward professional certification and other goals, which serves to encourage members to participate. Offering webinars in EAS security, or perhaps even an EAS security certification, is one method of reaching engineers, increasing their awareness of EAS security issues and best practices, and informing them of specific steps needed to protect the EAS infrastructure at the facilities they oversee.

Trade Publications. Widely-read trade publications such as *Radio World* and *Broadcasting & Cable* often welcome contributions on subjects relevant to their readership. Contributions from Commission or industry experts in the field of EAS security to such journals would greatly improve awareness of EAS security concerns among EAS Participants.

Newsletters and Social media. NCTA and other groups routinely communicate with their members through regularly scheduled newsletters as well as social media websites, and also provide timely information on their websites. WG3 recommends that the FCC invite organizations to highlight EAS security on these outlets; in particular, groups should be encouraged to create a webpage devoted to EAS security and link to that page from the group's primary homepage. Groups may also provide links to additional resources for relevant information, including a link to the appropriate page on the Commission's website.

Email blasts. Many industry associations periodically distribute email blasts designed to remind or inform their constituencies of current “hot topics” or upcoming deadlines. EAS security would be a suitable topic for such communications.

Conferences, conventions, policy forums. Industry groups hold conventions and conferences on at least an annual basis at which panel discussions regarding EAS security could be provided. For example, NAB is planning a session concerning cybersecurity for broadcasters at its annual convention in April 2015, as well as another session focused on the future of EAS, featuring FCC personnel. State Broadcasters Associations also hold annual conferences during which EAS security could be addressed.

Cybersecurity Awareness Month. The Commission should lead an annual program during Cybersecurity Awareness Month that invites participation from industry organizations to press the issue of EAS security among all categories of EAS Participants.

6 Conclusions

Outreach pathways already in place and commonly used by both public and private entities provide a suitable model for delivering EAS security content to EAS Participants. The message needs to be tailored to the specific audience addressed by the outreach method. EAS Security should be addressed in the FCC EAS Handbook.

Specifically, WG3 recommends that the Commission undertake an EAS security outreach effort that includes the following components:

- FCC development of a user-friendly list of EAS cybersecurity best practices, of general relevance to all EAS stakeholders.
- FCC development of additional lists of best practices that are tailored to specific segments of the EAS ecosystem, *e.g.*, small and rural radio stations, small and rural cable systems, large television groups.
- Prominent display of all best practices on the FCC's website, *e.g.*, the Public Safety & Homeland Security Bureau homepage, Media Bureau homepage, dedicated EAS page.
- Establish a process for ensuring that relevant documents include references to best practices.
- Amend the EAS Handbooks to reflect the cybersecurity best practices.
- Schedule and promote an interactive webcast for EAS participants.
- Coordinate with FEMA regarding consistent, periodic outreach concerning EAS security.
- Invite industry associations and organizations to support and extend the Commission's outreach through member communications, such as webcasts, newsletters, convention programs and sessions, policy forums, and social media.
- Commission staff volunteers for industry endeavors.
- Schedule a series of reminder events (webinar, advisories) during Cybersecurity Awareness Month.

As discussed in the WG3 Initial Report, the FCC's work regarding EAS security can never be considered complete since the threats to EAS will continue to evolve. Accordingly, the FCC should periodically assess the content and process of its EAS security outreach and continually correct any deficiencies.