CSRIC

Communications Security, Reliability and Interoperability Council

March 2016

WORKING GROUP 3
EMERGENCY ALERT SYSTEM

Final Report - EAS Security Best Practices Adoption

Table of Contents

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 help ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety." To achieve that goal, CSRIC V established and chartered various "Working Groups" to examine the various issues of concern in these areas.

Working Group 3 (WG3) was formed to make recommendations for the CSRIC's consideration in three major areas related to the continued improvement and development of the Emergency Alert System (EAS) as a secure, effective alerting tool for the American public:

1. EAS Security;
2. the provision of EAS in languages other than English; and
3. the development of an operational handbook for individual broadcasters, cable service providers and other EAS Participants

This Final Report was prepared by the CSRIC V WG3 Project Team on EAS security. In this report, the WG3 makes recommendations concerning the implementation of the EAS cybersecurity best practices adopted by the CSRIC IV. Subsequent to the CSRIC IV's adoption of these best practices, the Commission released a public notice in which it sought comment on the extent to which these best practices had been adopted.[1] On January 28, 2016, the Commission initiated a rulemaking intended to address EAS security issues, among other issues.[2] The FCC has stated that any recommendations adopted by the CSRIC will be incorporated into the record of the 2016 EAS NPRM.

The working group has been tasked with assessing any barriers to the adoption of the CSRIC IV best practices, and make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices. The working group was also tasked with recommending methods by which other EAS stakeholders may gain assurance that the best practices are being implemented.

The Project Team encountered several difficult challenges to completing the assigned tasks. First, we note that, in addition to approving EAS security best practices, the CSRIC IV also approved specific recommendations for Commission public outreach concerning those best practices. In the opinion of the working group, the commission did not perform a sufficient amount of outreach, and the EAS Security Public Notice unfortunately did not generate a sufficient record regarding industry implementation of the CSRIC-recommended best practices. Thus, the Project Team was unable to leverage any FCC information collection that could further an assessment of "barriers to the adoption of EAS security best practices." Moreover,

[1] Public Safety and Homeland Security Bureau Seeks Comment on Implementation of Emergency Alert System Security Best Practices, Public Notice, DA 14-1628 (Nov. 7, 2014) (EAS Security Public Notice).

[2] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, *Wireless Emergency Alerts*, PS Docket No. 15-91, Notice of Proposed Rulemaking, FCC 16-5 (Jan. 28, 2016) (2016 EAS NPRM).

the team was unable to identify any existing alternative resource for such information, and was prohibited by the Commission's administrative procedures for federal advisory groups from conducting our own industry surveys, further constraining our efforts.

Second, subsequent to the chartering of CSRIC V, the Commission released the 2016 EAS NPRM, which seeks comment on requiring an annual certification from EAS Participants that demonstrates implementation of specific EAS security measures based on the CSRIC-recommended EAS security best practices. Accordingly, this NPRM would seem to substantially supersede our assigned task to "make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices," since a federal certification requirement is likely all the incentive any EAS Participant would need.

Finally, the 2016 EAS NPRM also proposes specific procedures for the confidential treatment of the annual certification forms mentioned above, the information and security measures underlying the certification forms, as well as the potential sharing of such information with other federal agencies. Therefore, the NPRM also seems to largely supersede our task to recommend "methods by which other EAS stakeholders may gain assurance that the best practices are being implemented," because the FCC has already launched a comprehensive inquiry into the collection and sharing of information on industry implementation of EAS security best practices.

Nevertheless, the Project Team undertook to fulfill our assigned tasks with the information on hand, regardless of these challenges, particularly, adoption of the 2016 EAS NPRM. Below we offer the consensus view of Project team members concerning the confidentiality and use of EAS security information, and the public availability of the CSRIC best practices recommendations. Most importantly, WG3 strongly recommends that the Commission refrain from any enforcement actions related to EAS security breaches so long as an EAS Participant has implemented the CSRIC IV recommended EAS security best practices.

2 Introduction

CSRIC V Working Group 3 was established to make recommendations for the CSRIC's consideration in three major areas related to the continued improvement and development of the Emergency Alert System (EAS) as a secure, effective alerting tool for the American public: (1) EAS Security; (2) the provision of EAS in languages other than English; and (3) the development of an operational handbook for individual broadcasters, cable service providers and other EAS Participants.

In order to tackle the relevant issues, a diverse team of subject matter experts was recruited to participate. The following areas of expertise are represented within the group.

- Message Originators: FEMA; NWS; State & Local Emergency Managers; State EAS Networks
- EAS Participants: Radio; TV; Cable TV; Satellite TV; Satellite Radio; Wireline Video/IPTV
- EAS Equipment Manufacturers
- State Emergency Communications Committees
- EAS Experts and Consultants

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

- **EAS Security** – Recommend steps for assessing any barriers to the adoption of the CSRIC IV best practices, make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices, and recommend methods by which other EAS stakeholders may gain assurance that the best practices are being implemented.
- **Multilingual EAS** – The Working Group will recommend best practices for the delivery of multilingual EAS and emergency information.
- **EAS Operational Handbook –** Update and modernize the EAS Handbook which states in summary form the actions to be taken by personnel at EAS Participant facilities upon receipt of an EAN, an EAT, tests, or State and Local Area alerts.

The Commission is concerned about the severity, frequency and nature of cybersecurity threats to the EAS system, and the related implications for the readiness of EAS to alert and inform the public about threats to safety of life and property, particularly to support the need of the President to communicate with the public during times of emergency.

In this report, WG3 discusses recommendations for improving the security of EAS, expanding industry implementation of cybersecurity risk mitigation measures, and the cautious collection and sharing of information concerning EAS Participants' implementation of such measures. The actions that may follow will help to ensure the reliability of the EAS system as a critical mechanism for warning and informing the American public during severe weather, AMBER Alerts, natural disasters, and other emergency situations.

2.1 CSRIC Structure

<table>
<tr><th colspan="8">Communications Security, Reliability, and Interoperability Council (CSRIC) IV</th></tr>
<tr><td colspan="8">CSRIC Steering Committee</td></tr>
<tr><td>Chair(s):
WG # 1
Susan Sherwod
Jeff Cohen</td><td>Chair(s): WG # 2
Francisco Sanchez
Farrokh Khatibi</td><td>Chair(s):
WG # 3
Steven .Johnson
Kelly Williams</td><td>Chair(s):
WG # 4
Kent Bressie
Catherine Creese
Jennifer Manner</td><td>Chair(s):
WG # 5
Rod Rasmussen
Christopher Boyer
Brian Allen</td><td>Chair(s):
WG # 6
Brian Scarpelli
Joel Molinoff</td><td>Chair(s):
WG # 7
Bill Boni
Drew Morin</td><td>Chair(s):
WG # 8
William Reidway
Thomas Anderson</td></tr>
<tr><td>WG # 1:
Evolving 911 Services</td><td>WG # 2:
Emergency Alerting Platforms</td><td>WG # 3:
Emergency Alert System</td><td>WG # 4:
Communications Infrastructure Resiliency</td><td>WG # 5:
Cybersecurity Information Sharing</td><td>WG # 6:
Secure Hardware & Software</td><td>WG # 7:
Cybersecurity Workforce</td><td>WG # 8:
Priority Services</td></tr>
</table>

Table 1 - Working Group Structure

2.2 Working Group #3 Team Members

Working Group #3 consists of the members listed below.
* Indicates member, EAS Security Best Practices Adoption Project Team

Name	Company
Chair WG3 - Kelly Williams	National Association of Broadcasters
Chair WG3 – Steven Johnson	Johnson Telecom
Chair WG3 EAS Security Best Practices Adoption Project Team – Gary Smith*	Cherry Creek Radio
Adrienne Abbott-Gutierrez*	Nevada EAS Chair, NV SECC
Mark Annas	Riverside (CA) Fire Department
John Archer*	SiriusXM
John E. Benedict*	CenturyLink
Benjamin Brinitzer*	iHeart Media/SBE
Robert Bunge*	NOAA
Kay Chiodo	Def Link Inc.
Greg Cooke*	FCC
Edward Czarnecki*	Monroe Electronics
Jim Du Bois	Minnesota Broadcasters Association
Clay Freinwald	Washington State University, WA SECC
Daniel Geist*	Cox Communications, Inc.
Suzanne Goucher	Maine Association of Broadcasters
Neil Graves	SNR Systems
Ricardo Guerrero*	AT&T
Ryan Hedgpeth	DHS
Craig Hoden*	NOAA NWS
Al Kenyon	DHS FEMA
Jim Klas	Wisconsin Educational Communications Board
Wayne Luplow	LGE/Zenith Electronics
Lillian McDonald	Twin Cities Public Television & Emergency,

	Community, Health and Outreach
Brian Murray	Houston Area Urban Security Initiative's Emergency Public Information Work Group
Brian Oliger*	Hubbard Radio
Jerry Parkins*	Comcast
Harold Price*	Sage Alerting Systems, Inc.
Austin Randazzo*	FCC
Richard Rudman	Broadcast Warning Working Group – CA SECC
Francisco Sanchez	Harris County Office of Homeland Security & Emergency Management
Bill Schully*	DIRECTV
Andy Scott*	National Cable & Telecommunications Association
Matthew Straeb*	GSS Net
Mike Talbert	Verizon
Gary Timm	Wisconsin SECC
Leo Velazquez	AT&T
Larry Walke*	NAB
Herb White	NOAA NWS (contract support)

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

The working group has been tasked with assessing any barriers to the adoption of the CSRIC IV best practices, and make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices. The working group was also tasked with recommending methods by which other EAS stakeholders may gain assurance that the best practices are being implemented.

3.2 Scope

This document addresses the deliverables outlined in the CSRIC V charter for Working Group #3. The working group endeavored to present a report that assesses any barriers to the adoption of the CSRIC IV best practices, and make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices. The working group also sought to recommend methods by which other EAS stakeholders may gain assurance that the best practices are being implemented.

The Project Team took the following stakeholders into consideration regarding the security of EAS:

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

The team has written this report taking into consideration budgetary constraints, Commission resources, and challenges related to the confidentiality and sharing of cybersecurity related information.

The scope of our product was limited by several challenges outside of our control. First, because the Commission's EAS Security Public Notice did not generate an adequate record of industry implementation of the CSRIC-recommended best practices, we were unable to rely on any FCC information collection that could enable assessment of barriers to the adoption of EAS security best practices. Nor could the team identify any sufficient alternative resources for such information. Finally, pursuant to the Commission's administrative procedures for federal advisory groups, the team was not permitted to conduct our own industry survey to aggregate information about the implementation of security measures. As a result, WG3 was unable to compile an accurate assessment of industry's implementation of EAS security best practices.

Second, the Commission's adoption of the 2016 EAS NPRM diluted our mission by proposing specific requirements designed to resolve all of the questions assigned by the Commission to WG3. For example, the FCC has proposed an annual certification requirement in which EAS Participants could demonstrate their implementation of specific EAS security measures based on the CSRIC IV-recommended EAS security best practices. Accordingly, the NPRM substantially supersedes our assigned task to "make recommendations on incentives, both regulatory and non-regulatory for affected stakeholders to adopt the best practices," because avoiding penalty for violation of an FCC rule is sufficient incentive.

Finally, the 2016 EAS NPRM proposes specific procedures for the confidential treatment of the annual certification forms mentioned above, the information and security measures underlying the certification forms, and the potential sharing of such information with other federal agencies. Therefore, the NPRM also negates our task to recommend "methods by which other EAS stakeholders may gain assurance that the best practices are being implemented."

In spite of the above limitations, however, the working group has used the expertise of its own members to make recommendations.

3.3 Methodology

The Project Team used a collaborative, inclusive approach. Given the expertise of various team 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 chair, Gary Smith of Cherry Creek Radio.

4 Background

For a comprehensive discussion of the background relevant to this inquiry, WG3 refers the CSRIC to the 2016 EAS NPRM. At paragraphs 5 through 8, the Commission provides an accurate depiction of the EAS system's technical architecture. At paragraphs 97 through 107, the Commission discusses its concerns regarding security of the EAS system, describes recent EAS security incidents, and recaps earlier FCC efforts to improve EAS security. The Commission expresses concerns that all of these circumstances "reveal an unacceptably high risk of unauthorized EAS signal broadcasts and insufficient real-time Commission awareness of, and visibility into the possible negative impacts of unauthorized alerts." 2016 EAS NPRM at para. 103.

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) administered by the Federal Emergency Management Agency (FEMA) is the Nation’s public alerting system 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.

The addition of 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.

One of the key implications of the adoption of interconnected technologies by EAS participants is that the EAS system is now dependent on network delivered services. At that same time, EAS participants have become more dependent on network delivered services. CSRIC IV observed that CAP/EAS equipment is spanning these two domains - connecting to both internal and external networks to monitor and disseminate alert and warning content through increasingly complex operational environments, and endeavored to take a holistic approach in looking at how EAS participants, alert originators and EAS device manufacturers can defend and protect their organizations, and to help recover when things go wrong.

CSRIC V WG3 notes that best practices in general and the CSRIC IV Best Practices specifically should be considered voluntary and are not intended to be mandated but should be implemented in a manner that is appropriate to the needs, resources and capabilities of each individual organization.

As the Commission notes in the 2016 EAS NPRM, unauthorized EAS breaches over the past few 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.

5 Recommendations

CSRIC IV WG3[3] had made recommendations on how the FCC could increase its outreach of the voluntary security Best Practices. Additional outreach and education is needed to insure a healthy and secure EAS ecosystem. CSRIC V WG3 recommends that the FCC extend its outreach efforts regarding Best Practices utilizing those methods. The information included in the outreach should clearly set the expectation that EAS participants should implement voluntary security practices appropriate to the EAS participant's needs.[4]

Information about EAS Participants implementation of the security best practices should not be a matter of public record and should be held confidential. Discussion of security issues, the current level of protection, in public, with attribution, is an unacceptable level of exposure to EAS Stakeholders. The FCC should work in conjunction with the Department of Homeland Security and other federal agencies to establish processes for sharing information that is considered by EAS Participants to be sensitive and non-public.

The CSRIC IV voluntary Best Practices need to be readily available and EAS participants must know how to find them. CSRIC V WG3 recommends that the best practices be prominently displayed on the FCC's website, possibly in a new FCC document aimed at the station Chief Operator or other individual responsible for EAS operations at each participant facility. This document could be referenced by Alternative Broadcast Inspection Program (ABIP)[5] inspectors to discuss security best practices implementation during station inspections.

The CSRIC IV voluntary Best Practices are intended to be adaptable to the requirements of each EAS stakeholder's specific infrastructure. The Best Practices are part of a process that leads to securing an evolving EAS ecosystem. Due to the nature of cybersecurity, its complexity, and constant evolution, and the various unique requirements of each EAS stakeholder, CSRIC V WG3 recommends that:

a. the FCC gives maximum flexibility to EAS participants with respect to the differences between the Best Practices and the methods used to implement EAS security, especially where the methods used exceed the techniques established in the Best Practices;

b. that any confidential information shared in response to voluntary or mandated FCC information gathering not result in enforcement actions by the FCC; and,

[3] *see appendix 1, Excerpt from CSRIC IV WG3 EAS Security Committee Final Report on Outreach*

[4] *CSRIC V WG3 notes that in January 2016, the FCC issued an NPRM in which it proposed new rules regarding security.*

[5] *The Alternative Broadcast Inspection Program is a cooperative program between the FCC Enforcement Bureau and State Broadcast Associations under which stations that participate can receive a three-year exemption from routine FCC inspections. Once the station passes the inspections, which is carried out by authorized inspector, the state association issues a certificate which is also be provided to the FCC.*

c. in the event of a security breach an EAS participant is not subject to enforcement action, particularly if the methods used to implement EAS security fulfill the intent of the techniques outlined in the Best Practices.

6 Conclusions

Working Group #3 encountered several challenges concerning the assigned project, as described above, including the intervening 2016 EAS NPRM, which largely superseded our task. Nevertheless, the Project Team conducted weekly, fruitful discussions in good faith towards the resolution of the delegated question with the information on hand at the time, and subject to certain administrative procedures that limited our efforts and scope.

Our recommendations may be summarized as follows:

(1) Information about how EAS Participants have implemented the security best practices should not be a matter of public record and should be held confidential. The Commission should work with other federal agencies to establish processes for sharing information that is considered by EAS Participants to be sensitive and non-public.

(2) The CSRIC IV EAS Security "Recommended Best Practices" need to be readily available and EAS participants must know how to find them.

(3) Due to the complex and evolving nature of cybersecurity, a) the FCC should give maximum flexibility to EAS participants with respect to the differences between the Best Practices and the methods used to implement EAS security, especially where the methods used exceed the techniques established in the Best Practices, b) any confidential information shared in response to voluntary or mandated FCC information gathering not result in enforcement actions by the FCC, and c) in the event of a security breach an EAS participant is not subject to enforcement action, particularly if the methods used to implement EAS security fulfill the intent of the techniques outlined in the Best Practices.

Appendix 1: Excerpt from 2015 CSRIC IV Working Group #3 Final Report

Section 5: Recommendations

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.