FCC PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

DA 14-1628
November 7, 2014

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON IMPLEMENTATION OF EMERGENCY ALERT SYSTEM SECURITY BEST PRACTICES

Comment Date: December 30, 2014

On June 18, 2014, the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council IV (CSRIC IV)[1] unanimously adopted voluntary communications best practices to improve the security of the Emergency Alert System (EAS).[2] This effort is part of several important communications security initiatives currently being undertaken by CSRIC IV. The Public Safety and Homeland Security Bureau (Bureau) applauds the development of these new EAS security best practices and the development of mechanisms of measurement and accountability for the effectiveness of their implementation in concert with broader ongoing CSRIC efforts regarding communications security. As discussed further below, given the need to improve the security posture of EAS end points, the Bureau seeks comment on implementation of these best practices to date.

Participation in the national EAS is mandatory for broadcast stations, cable systems, wireline video systems, wireless cable systems, Direct Broadcast Satellite services, and the Satellite Digital Audio Radio Service.[3] The goal of EAS is to provide timely and accurate alerts and warnings so that members of the public may act quickly to protect themselves and their family members.[4] To meet this goal, the EAS must be secure and reliable. As with other communications-based systems, the EAS is subject to security vulnerabilities; these vulnerabilities are expected to continue to grow, particularly in light of the recent transition to alerting based on the Internet-based Common Alerting Protocol (CAP).[5] Absent proactive and effective management of cyber risks, security vulnerabilities could allow harmful cyber attacks on the EAS that result in the transmission of inaccurate information. For instance, in February 2013, an unidentified party gained unauthorized access through the Internet to several broadcasters' EAS equipment and sent a fake emergency message to the local public. The incident illustrates that at least

[1] CSRIC is a federal advisory committee that provides recommendations to the FCC to help ensure, among other things, security and reliability of commercial and public safety communications systems. The CSRIC is subject to the requirements of the Federal Advisory Committee Act. *See* 5 U.S.C. App. 2.

[2] *Initial Report, CSRIC WG3 EAS Security Subcommittee Report (Report)* is available through the FCC's website: http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf.

[3] *See* 47 C.F.R. Part 11.

[4] Review of Emergency Alert System, EB Docket No. 04-296, *Notice of Proposed Rulemaking*, 29 FCC Rcd 8123, 8150 ¶ 57 (2014) (*EAS NPRM*).

[5] *Id.* at 8129 ¶ 9.

some within the communications industry have not taken sufficient, or even basic, measures to thwart such attacks and ensure reliable delivery to the public of accurate public safety information.[6]

Because of the importance of the EAS to public safety and national security, EAS Participants play a critical role in ensuring the secure operation of the EAS. Poor security practices by EAS Participants cannot be allowed to degrade the overall system or the public's confidence in the integrity of the system.

As CSRIC IV stated in the *Report*, "[p]rotecting against information security risks is part of protecting the reliability of the Emergency Alert System, the credibility of the EAS participant, and the bottom line against the costs of recovering from a security incident."[7]

Request for Comment

By this Public Notice, the Bureau seeks public comment on the implementation and effectiveness of CSRIC IV's recommendations and/or alternatives that stakeholders have developed since the time of CSRIC's work in June 2014. The purpose of this Public Notice is to promote a robust, stakeholder-driven discourse drawing on broad perspectives from throughout the EAS ecosystem to provide the communications sector and the Commission new information, insights and situational awareness regarding innovative solutions to security risks within the EAS. To the extent that companies or other stakeholders may prefer that their submissions remain confidential, we intend to protect the confidentiality of submissions according to the requests and consistent with FCC rules, as described below. This inquiry is part of the Commission's larger effort to develop effective and proactive private sector-driven cyber risk management.[8]

The Bureau seeks public comment on the implementation status and effectiveness of the voluntary security best practice recommendations, or alternatives, in the attached Appendix, by EAS Participants, equipment manufacturers and other members of the EAS community. The Bureau is particularly interested in comment on the following questions:

1. What progress have EAS Participants including broadcast stations, cable operators, satellite radio and television providers and wireline video service providers made in implementing these best practices? What efforts have EAS equipment manufacturers, state and local governments and other EAS stakeholders taken to enhance EAS security?
2. What barriers have EAS stakeholders encountered in implementing the recommendations?
3. What significant success stories or breakthroughs have been achieved in implementing the recommendations?
4. What are stakeholders' views and/or plans for full implementation of these recommendations?
5. How effective are the recommendations at mitigating security risk when they have been implemented? Do stakeholders undertake qualitative or quantitative evaluations of the effectiveness of these recommendations?
6. What alternatives have been implemented? How effective are those alternatives?
7. What, if any, actions have EAS stakeholders taken, in addition, to these basic security best practices to help enhance the security of the EAS?

[6] *See* Letter from The Honorable Tom Wheeler, Chairman, Federal Communications Commission to Honorable Mike Pompeo, Member of Congress, July 29, 2014 *available at* http://appsint.fcc.gov/ecfs/document/view?id=7521752113.

[7] *Report* at 9.

[8] Remarks of FCC Chairman Tom Wheeler to the American Enterprise Institute, June 12, 2014 *available at* http://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc.

8. What recurring measures would ensure that EAS Participants sustain an effective security posture in light of continuously evolving threats and technology?

Also today, by separate public notice, the Bureau announces an inquiry into the circumstances of the retransmission on October 24, 2014, of a false EAS alert that affected several states. This incident did not involve a breach of the Federal Emergency Management Agency's Intergrated Public Alert and Warning System.[9]

Comment Submission

Interested parties are invited to comment by December 30, 2014. Please submit comment or meeting requests by email directly to Jeffery Goldthorp, Associate Chief, Public Safety and Homeland Security Bureau and CSRIC Designated Federal Officer, at Jeffery.goldthorp@fcc.gov, with a copy to Lauren Kravetz, Deputy Chief, Cybersecurity and Communications Reliability Division, and Deputy Designated Federal Officer, at lauren.kravetz@fcc.gov.

Requests for confidential treatment of information submitted should follow the procedures set forth in section 0.459 of the Commission's rules, under which all submissions with an appropriate request for confidential treatment will be treated as presumptively confidential pending a ruling on the request. Additionally, upon request and on a case-by-case basis, the Bureau may accommodate classified comment submissions or discussions.

Alternatively, those who desire to submit comments in hard copy only should submit an original and one copy of each set of comments. Hard copy comments can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All such submissions should be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission and reference DA-14-1628.

- All hand-delivered or messenger-delivered paper submissions for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th Street, SW, Room TW-A325, Washington, DC 20554. Delivery hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington, DC 20554.

To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Government Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

[9] *See* PSHSB Issues Advisory to AS Participants to Check Equipment for Possible Queuing of Unauthorized EAS Message for Future Transmission; Requests Comment on Impact of Unauthorized EAS Alerts and Announces Inquiry into Circumstances of Retransmission of Unauthorized EAS Message in Several States, *Public Notice*, PS Docket No. 14-200, DA 14-1626, rel. Nov. 7, 2014.

For further information on this subject, contact Jeffery Goldthorp, Associate Chief, Public Safety and Homeland Security Bureau and CSRIC Designated Federal Officer at (202) 418-1096 or jeffery.goldthorp@fcc.gov.

APPENDIX

EAS SECURITY PRACTICES

To help ensure the security of the EAS, the Bureau recommends implementation of the following security best practices.[10]

THE BUREAU HIGHLY RECOMMENDS THE FOLLOWING ACTIONS:

Internet-Facing Firewalls:

- At a minimum, EAS participants should always use a firewall between EAS equipment and the public Internet to reduce unknown external actors from compromising the system.

Passwords:

- Ensure default passwords are changed before connecting to Internet.
- Require password complexity.
- Change passwords after 90 days.
- Passwords should be kept confidential to prevent unauthorized access. Do not post passwords in plain sight, local to a system. Do not share passwords to individual user accounts with associates.
- Do not send passwords that are not encrypted through unprotected communications.

Update Awareness:

- EAS participants should regularly monitor EAS Manufacturer information resources (*e.g.* websites) to obtain vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.
- EAS participants should always make sure that they have provided the EAS Manufacturer with their current and accurate contact information.

User Accounts:

- There should not be any shared accounts. Each user should have a single individual account for access.
- Create individual user accounts.
- Do not give administrator access to users that do not require it.
- Disable or remove default users accounts.
- Remove unnecessary user accounts.
- Do not use administrative accounts for normal usage.

Establish 'Least Access' User Restrictions:

- Poorly specified access controls can result in giving an EAS Device user too many or too few privileges. Depending on the capabilities of the EAS device, provide the user with the appropriate level of device and system access (*e.g*., administrator account vs. user account).

IT Network and Equipment Inspection:

[10] *See Report*, Section 5 generally, with particular emphases on 5.2.1 Recommended Security Best Practices for EAS Participants, and 5.2.3 Recommended Best Practices for Device Manufacturers.

- EAS participants should develop and implement periodic physical inspections and maintenance as required for EAS equipment and all interfacing equipment.

Regularly Seek and Install Software Updates and Patches:

- EAS participants should establish and implement procedures to
  - Periodically check with EAS manufacturers for patches and updates (usually issued monthly).
  - Ensure that all security patches and updates relevant to the EAS device are promptly applied.
- If required, the system should be rebooted immediately after patching for the patch to take effect.

Expedite General System Updates and Security Patching:

- EAS participants should have processes in place to quickly patch/update EAS devices when the manufacturer makes security and reliability patches available.
- If possible, this should include expedited lab testing of the patches and their effect on network and component devices.
- EAS participants should perform a verification process to ensure that patches/fixes are actually applied to EAS devices.

Limit or Restrict Remote Access to EAS equipment:

- Whenever possible, remote access to EAS devices should be severely restricted and logged. Remote access should always be made via a secure pathway, such as Virtual Private Network.
- Remote access should never be made possible by an EAS device that is not secured by a firewall, or other network security means.
- Remote access to EAS equipment should only be from a system that is secured to the same level as the EAS equipment.

Restricting Access Privileges:

- There should be a clear process and policy to update access and accounts to EAS equipment when the roles of users change such as terminations, exits or transfers.

Disable Unnecessary Services:

- EAS participants should identify and disable unneeded network-accessible services, or provide for additional compensating controls, such as proxy servers, firewalls, or router filter lists, if such services are required.

Integrity:

- 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.

Keep CAP EAS Equipment in a Secure Location:

- EAS participants should always maintain EAS equipment in a secure network environment.
- This equipment has been designated by the FCC to be Internet facing, therefore basic network security protocols should be followed.

THE BUREAU SUGGESTS THE FOLLOWING ACTIONS:

Security Training:

- Staff should be aware of the importance of practicing “safe computing.” All users of IT equipment should be required to complete basic information assurance training on an annual basis.

Internal-Facing Firewalls:

- EAS participants should consider using a firewall between EAS equipment and all other participant network enabled equipment to reduce insider-threat.

Segment Networks or VLANS:

- EAS participants should ensure network accessible administrative ports on EAS equipment are within their own isolated network and monitor for unauthorized access.

Keep CAP EAS Equipment Physically Secure:

- EAS participants should always maintain EAS equipment in a secure physical environment. Access controls may include limitations on the ability for unauthorized individuals to access the equipment, and other measures.

THE BUREAU URGES CONSIDERATION OF THE FOLLOWING ACTIONS:

Configuration Management

- Have a security professional audit the EAS participant’s system security and configurations to mitigate risks.

Response and Recovery

- Have an incident response plan.

Device Security

- EAS participants should ensure that the equipment that they use is in adherence with the CSRIC IV EAS Best Practices for Device Manufacturers.