May 2014

WORKING GROUP 3
Emergency Alert System (EAS)

Initial Report
CSRIC WG3 EAS Security Subcommittee Report

Table of Contents

1 Results in Brief 3
1.1 Executive Summary 3
2 Introduction 4
2.1 CSRIC Structure 5
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 9
5 Recommendations 10
5.1 Recommended Best Practices 10
5.2 Recommendation Table Explanation 10
5.2.1 Recommended Security Best Practices for EAS Participants 10
5.2.1.1 Recommended Network and Operational Controls 11
5.2.1.2 Suggested Additional Controls 13
5.2.2 Emergency Alert Originators 13
5.2.2.1 Recommended Best Practices for Originators 14
5.2.3 EAS Device Manufacturers 15
5.2.3.1 Recommended Best Practices for Device Manufacturers 16
5.2.4 U.S. Government Agencies 18
5.2.4.1 Suggested Additional Controls 18
6 Conclusions 20
7 Appendix 21
7.1 References 21
7.1.1 CSRIC 21
7.1.2 NRIC 21
7.1.3 SANS Critical Controls 21
7.1.3.1 Critical Security Controls for Effective Cyber Defense 21
7.1.4 Additional Resources 22
7.2 Glossary 23

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 questions, including those raised by the FCC in their recent Public Notice on Nationwide EAS Test Issues.

This document was prepared by the CSRIC WG 3 EAS Security Sub-Group. It identifies the principal groups associated with EAS as: EAS Participants, emergency alert originators, EAS device manufacturers, and the federal government. This document addresses the need for information assurance (IA) and security controls throughout the EAS in the form of best practices guidelines for each of the defined groups.

CSRIC IV is focusing largely on cyber initiatives. The recommendations contained in this document should be aligned with the recommendations and strategy of the larger CSRIC, writ large.

These suggestions cover a lot of the same basic security recommendations and security hygiene that many other documents will cover but with a more specific focus on EAS operators, participants, and manufacturers. The simple processes of using firewalls, configuring related devices properly, and managing them smartly are all laid out in appropriate detail.

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.

In order to tackle the issues of EAS a diverse team of Subject Matter Experts were 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.
- EAS Equipment Manufacturers.
- State Emergency Communications Committees
- EAS Experts and Consultants.
- Public Interest, Persons with Disabilities.

The Working Group also developed recommendations for many actions, including best practices that the Commission should take to promote the security of the EAS. In addition, FCC staff tasked this Working Group to explore operational issues that arose during the nationwide EAS test in November 2011.

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.
- **EAS Security** - Recommend actions to improve promote the security of the EAS.
- **Nationwide EAS Test/Operational Issues** - Address other EAS-related issues as assigned to CSRIC by the FCC.

The CSRIC WG 3 EAS Security Sub-Group was charged with providing an initial deliverable that describes a set of “best practices” for each aspect of EAS. This is the first of two reports; the follow-on report will address changes to the fundamental operating mechanisms of EAS.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
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 sub-group for EAS Security consists of two Co-Chairs: Neil Graves and Richard Perlotto.

Name	Affiliation(s)	Security Sub-Group
Adrienne Abbott	Nevada EAS Chair	
John Archer	SiriusXM	
John Benedict	CenturyLink	
Ron Boyer	Boyer Broadband	
Ted Buehner	Warning Coordination Meteorologist National Weather Service	
Lynn Claudy	National Association of Broadcasters	
Roswell Clark	Cox Media Group	
Kimberly Culp	Larimer Emergency Telephone Authority	
Edward Czarnecki	Monroe Electronics	Yes
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 (EAS Security co-chair)	SNR Systems (formerly FEMA IPAWS)	Yes
William Hickey	Premiere Radio Networks	
Craig Hoden	NOAA	Yes
Chris Homer	Public Broadcasting Service	
Steve Johnson	Johnson Telecom	Yes
Alfred Kenyon	FEMA IPAWS	Yes
Mark Lucero	FEMA	Yes
Wayne Luplow	LGE/Zenith Electronics	Yes
Bruce McFarlane	Fairfax County	
Dan Mettler	Clear Channel Media + Entertainment / Chair Indiana SECC	
David Munson	FCC Liaison	Yes

Brian Oliger	Hubbard Radio/WTOP	
Darryl Parker	TFT, Inc.	
Rich Parker	Vermont Public Radio /Chair, Vermont SECC	
Jerry Parkins	Comcast Cable	Yes
Efraim Petel	AtHoc, Inc.	
Richard Perlotto (EAS Security co-chair)	Shadowserver Foundation	Yes
Joey Peters	MyStateUSA, Inc.	Yes
Peter Poulos	Citi	
Harold Price	Sage Alerting Systems	Yes
Richard Rudman	Broadcast Warning Working Group / Vice Chair, California SECC	
Francisco Sanchez, Jr.	Harris County (TX) Office of Homeland Security	
Tim Schott	NOAA	Yes
Andy Scott	V.P. Engineering, NCTA	Yes
Bill Schully	DIRECTV	Yes
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	Yes
Michael Watson	Gray Television Group	
Kelly Williams	NAB	Yes
Reed Wilson	Belo Corp.	

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

The FCC charter for CSRIC IV called on WG3 specifically to "develop recommendations for any actions, including best practices; the Commission should take to promote the security of the EAS." The objective of this report is to provide security best practices to the EAS and responsible and related parties.

3.2 Scope

The EAS Security Subcommittee took the following bodies into consideration regarding the security of EAS:

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

This document addresses the immediate need of improvement to the security of EAS by reviewing each of the above elements against industry best practices, including the SANS 20 Critical Security Controls (v5)[1], the Communications Sector-Specific Plan Annex to the National Infrastructure Protection Plan[2], and the NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0[3]. While the SANS Top 20 document addresses specific controls, the NIPP and NIST Framework address the importance (and guidance for) instituting an overall security program

This document serves as a best practices guide that EAS Participants, that once implemented, will result in a more secure EAS. The subcommittee has written the best practices guide taking into consideration budgetary constraints and complexity of computer systems.

There is also the future work that needs to be completed related to legacy EAS capabilities. This document is primarily focused on IP-based capabilities and only covers a part of the related systems that can also affect EAS capabilities and messaging.

3.3 Methodology

Building any best practices document is a difficult task that depends heavily on the audience and constituents who are to abide by the document. This is increasingly complex when one party is heavily reliant on other businesses and areas of responsibilities. The best practices should be developed to include the entire

[1] http://www.sans.org/critical-security-controls
[2] http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf
[3] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

ecosystem, and not be limited to one of its subsets.

This concept expands the research into best practices to those who have an effect on broadcast organizations to include alert originators, device manufacturers, and the U.S. Government.

4 Background

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.

We observe 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.

This Task Group 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.

As the FCC itself has noted "Every business that uses the Internet is responsible for creating a culture of security that will enhance business and consumer confidence."[4] The EAS needs to be part of that culture. Protecting 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.

[4] http://www.fcc.gov/cyberforsmallbiz

5 Recommendations

5.1 Recommended Best Practices

The recommendations presented by the subcommittee are divided into the following groups:

1. EAS Participants: These are the obligated to participate with the EAS according to 47 CFR Part 11.[5]
2. Emergency Alert Originators: These are the authorized alerting authorities across the United States at the national, tribal, state, territorial, county, and city level who have been identified as having the responsibility of alerting their constituents of imminent threats to life and property.
3. EAS Device Manufacturers: This group is the set of companies that develop and manufacture EAS devices according to 47 CFR Part 11 and are authorized by the FCC.
4. U.S. Government: Agencies and commissions of the U.S. Federal Government with responsibility for the EAS.

Securing EAS is not a one-time effort, but is a continuous process, which should be applied, assessed, and revised. It is essential for each of these groups to approach EAS as they would any other critical IT system. EAS should be incorporated into the existing business IT security program, or if such a program does not exist, one should be established according to this best practices document and referenced guidance.

5.2 Recommendation Table Explanation

For each group there is a table of recommendations. There are five columns in each table with the following titles and descriptions:

- Control – A sequence number to identify each individual recommendation.
- Summary – A short name to describe the recommendation.
- Detail – Detailed description of the recommendation.
- Priority – Level of importance of the recommendation. A “1” is highly recommended, while a “2” is suggested and a “3” should be considered.
- References – Any third-party reference documents for this recommendation

5.2.1 Recommended Security Best Practices for EAS Participants

EAS Participants are responsible for delivering alerts and warnings to the population. Equipment that is capable of inserting content into the transmission stream of a broadcast organization, or is able to communicate via command channels to such devices should be considered part of the overall EAS. The equipment required for transmitting, receiving, and retransmitting EAS alerts is located within an organization’s facilities. Therefore, the role of securing the equipment rests with that organization.

[5] CITE FCC Rule 47 CFR 11.11

Network Controls refers to the EAS devices that are accessible over a network, and guidelines for providing a more secure networked environment for EAS. EAS Operational Controls refers to the software configuration and operating standards for EAS devices.

5.2.1.1Recommended Network and Operational Controls

Control	Summary	Detail	Priority	References
1	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 the EAS Manufacturer their current and accurate contact information.	1	
2	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.	1	
3	Passwords	• Ensure default passwords are changed before connecting to Internet. Require password complexity[6]. 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.	1	NRIC 9.9.8018
4	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).	1	NRIC 9-8-8014; NRIC 9-9-8086

[6] An example of password complexity can be found in 8500.2… make this citation complete

5	IT Network and Equipment Inspection	• EAS Participants should develop and implement periodic physical inspections and maintenance as required for EAS equipment and all interfacing equipment.	1	SANS 1-4

6	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
		  ○ 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.
			1	SANS 6-1

7	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.[7] • 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.	1	NRIC 9.8.8020
8	Limit or Restrict Remote Access to your EAS equipment	• Whenever possible, remote access to EAS devices should be severely restricted. Remote access should always be made via a secure pathway, such as VPN. • Remote access should never be made possible by an EAS device that is not secured by a firewall, or other network security means.	1	
9	Removal of 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.		NRIC 9.8.8098
10	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.	1	SANS 11-1, SANS 11-2
11	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.	1	
12	Keep CAP EAS Equipment in a Secure Network.	• 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.	1	SANS 11-7

[7] 11.35 – functional availability

13	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.	1	SANS 11-7
14	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.	2	
15	Internal-Facing Firewalls	• EAS Participants should consider using a firewall between EAS equipment and all other Participant network enabled equipment to reduce insider-threat.	2	
16	Segment Networks or VLANS	• EAS Participants should ensure network accessible administrative ports on EAS equipment are within their own isolated network.	2	NRIC 9.8.8015; SANS 11-5
17	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.	2	
18	Configuration Management	• Have a security professional audit your configurations to mitigate risks	3	SANS 10-1

5.2.1.2Suggested Additional Controls

The Task Group identified the following additional controls for EAS Participants. These controls are suggested supplemental best practices for EAS Participants.

Control	Summary	Detail	References
3	Ensure Message Source Integrity	• EAS Participants should use good engineering practice to ensure that EAS monitor source signals are of high quality.	

5.2.2 Emergency Alert Originators

Emergency Alert Originators are the organizations authorized to create the emergency alerts that are to be disseminated via the EAS. Although Originators are not provided oversight by the FCC, they are directly related to the EAS and if compromised could cause either a denial of service to the EAS for that area or false alerts to be distributed. Securing the message origination and communication methods is imperative to the security of the EAS.

5.2.2.1Recommended Best Practices for Originators

Control	Summary	Detail	Priority	References
1	CAP Software	• Originators should include security in their evaluation criteria when selecting alerting software and or any alternative means for EAS Common Alerting Protocol (CAP) message delivery	1	
2	CAP Delivery	• All means for EAS/CAP message delivery should demonstrate their design provisions for non-repudiation and general security.	1	
3	Aggregation Systems	• Alert aggregators should develop and maintain security controls for their servers.	1	
4	Physical Security	• Originators should keep all EAS and CAP related hardware and software within a secured area to limit the ability for unauthorized individuals to access the equipment.	1	
5	Physical Inspections	• Originators should develop and implement periodic physical inspections and maintenance for all critical EAS related systems.	1	
6	Network Security	• Originators should maintain their EAS equipment in a secure network environment.	1	
7	Internet-Facing Firewalls	• Originators should always use a firewall between their alerting tools and the public Internet to reduce unknown external actors from compromising the system.	1	SANS 11-7
8	Internal-Facing Firewalls	• Originators should use a firewall between their alerting tools and all other originator network enabled equipment to reduce insider-threat.	1	
9	Segment Networks or VLANS	• Originators should ensure network accessible administrative ports on alert origination machines are within their own isolated network.	1	NRIC 9.8.8015; SANS 11-5
10	Disable Unnecessary Services	• Originators 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. • Originators should always harden the access control capabilities of each EAS related machine or network element before deployment to the extent possible.	1	SANS 11-1, SANS 11-2

11	Regularly Seek And Install Software Updates and Patches	• Originators should establish and implement procedures to:
		  ○ Periodically check with their alert origination software developers for patches and updates.
		  ○ Ensure that all security patches and updates relevant to the software are promptly applied.
		• If required, the system should be rebooted immediately after patching for the patch to take effect.
			1	SANS 6-1

12	Expedite Security Patching and General Updates	• Originators should have processes in place to quickly patch/update origination software and other key systems when the manufacturer makes important updates and security patches available. If possible, this should include expedited lab testing of the patches and their effect on network and component devices. • Originators should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Originators should perform a verification process to ensure that patches/fixes are actually applied to origination machines.	1	NRIC 9.8.8020
13	Limit or Restrict Remote Access to EAS equipment	• Whenever possible, remote access to origination machines should be severely restricted. Remote access should always be made via a secure pathway, such as VPN. Remote access should never be made possible by an origination machine that is not secured by a firewall, or other network security means.	1	
14	Passwords	• Ensure default passwords are changed before connecting to Internet. Require password complexity. Expire passwords after 90 days. Limit failed password attempts.	1	
15	User Accounts	• Disable or remove default user accounts. Remove unnecessary user accounts.	1	
16	IPAWS	• Those using IPAWS for origination are connecting to a DHS system and should follow DHS 4300A in addition to abiding by the rules of behavior required by FEMA.[8]	2	

5.2.3 EAS Device Manufacturers

EAS Device Manufacturers are required to build their devices according to 47 CFR Part 11. This section defines the operating standard in which an EAS device transmits, receives, and retransmits EAS alerts. The following standards should be followed to help secure the EAS devices for when they are put into operation.

[8] DHS Sensitive Systems Policy Directive 4300A, Version 8.0, March 14, 2011
http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf

5.2.3.1Recommended Best Practices for Device Manufacturers

Control	Summary	Detail	Priority	References
1	Updating	• Ensure EAS devices can be updated. • If automatic updating is available, ensure it is enabled by default. • If automatic updating is not easily achievable, the manufacturer should provide guidance on how the user should apply updates manually.	1	
2	Passwords	• Device should require users to change their password upon first use. • Device should require complexity when users select their passwords. • Devices should let users know when their passwords have reached 90 days and prompt for change.	1	
3	Access	• Devices should default to a least privilege state.		
4	Default Configurations	• EAS Devices should be in a basic secure state by default. • Manufacturers should work closely and regularly with customers to provide recommendations concerning existing default settings and to identify future default settings that may introduce vulnerabilities. • Manufacturers should proactively collaborate with network operators to identify and provide recommendations on configurable default parameters and provide guidelines on system deployment and integration such that initial configurations are as secure as allowed by the technology.	1	NRIC 9.8.8004
5	Security Guidance	• Manufacturers should incorporate security guidance in their documentation that is complete and easy-to-use. • The availability of electronic media to customers for documentation is essential.	1	NRIC 9.7.0561
6	Vulnerability and Patch notification	• Manufacturers should ensure that vulnerability and remediation (patch) notification to end users is timely.	1	NRIC 9.8.8916
7	Device Operating System	• EAS devices should utilize operating systems that are currently supported. • Manufacturers should provide updates if and when the operating system becomes unsupported. If not, the manufacturer should specify compensating controls to be implemented by the user (such as firewalls, proxies, severely restricting remote access, etc.).	1	NRIC 9.9.8019

8	Notification to End Users	• EAS manufacturers should develop and maintain critical notification methods to communicate threat or vulnerability information with their customers. • EAS Manufacturers should decide the most appropriate method or methods for providing notification to their customers, and should use additional methods if the chosen method is not effective. The range of notification options may vary by the severity and/or criticality of the problem.	1	NRIC 9.8.8917
9	Recommended Network Configuration for Users	• EAS Manufacturers should advise users to use a minimum of a three-tier architecture (DMZ, middleware, and private network). • Any CAP/EAS system with sensitive data should reside on the private network and never be directly accessible from the Internet. • DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.	1	NRIC 9.8.8000
10	Recommended EAS Device Configuration	• Manufacturers should work closely and regularly with customers to provide recommendations concerning existing default settings and to identify future default settings, which may introduce vulnerabilities.	1	
11	Vulnerability Mitigation	• Manufacturers should support time-sensitive issuance of security and reliability-related software/firmware updates and patches, once a potential vulnerability has been verified.	1	NRIC 9.9.0536
12	USB	• If USB devices are required, the device should not autorun files. • The device should not write unprotected data that would normally be secured if accessed via any other means. • An inventory of all authorized devices should be maintained.	1	SANS 5-3; SANS 17-8
13	Contact Information	• Manufacturers should assemble and maintain information on third-party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@manufacturer.com or have a web page http://www.manufacturer.com/security).	1	
14	System Integrity	• Manufacturers should include a mechanism to ensure files are checked for integrity against a white-list. If any system files are changed, a notification should be generated.	2	

15	Sharing Information with Industry & Government	• Manufacturers should participate in regional and national information sharing groups such as the National Coordinating Center (NCC), and other pertinent bodies. • Formal membership and participation will enhance the receipt of timely threat information and will provide a forum for response and coordination. • Membership will also afford access to proprietary threat and vulnerability information (under NDA) that may precede public release of similar data.	2	NRIC 9.8.8066; NRIC 9.9.8053
16	Security Assessment	• Manufacturers should perform a security audit using a third-party organization of their EAS devices for the purpose of increasing the security and controls of these devices. • These reviews should be periodically renewed as new major versions of operating systems, applications, and hardware are released.	2	
17	Anti-Virus	• Manufacturers should include a host based security system such as anti-virus.	3	

5.2.4 U.S. Government Agencies

The Sub-Group identified a number of additional security-related matters that are recommended for the responsible Federal agencies to pursue.

5.2.4.1Suggested Additional Controls

The Task Group identified the following additional controls for US Federal Agencies. These controls are suggested supplemental best practices for EAS Participants.

Control	Summary	Detail	References
1	EAS Forum	• Government should create an ongoing forum for public-private collaboration on EAS security (e.g. a public private partnership for cybersecurity and EAS)	
2	Security Roadmap	• Industry and government should collaboratively create an industry security roadmap, engaging both EAS Participants, CAP EAS manufacturers and Federal agencies.	
3	EAS as PCII	• Include EAS Participants and CAP EAS manufacturers under the DHS Protected Critical Infrastructure Information (PCII) Program.	
4	Security Guidance to Users	• Government should provide clear guidance to EAS Participants on cybersecurity best practices, including the specific best practices identified above. Such guidance should identify the risks, benefits, consequences, and potential penalties for not following basic security best practices.	

5	Security Points of Contact	• Government should provide EAS Participants, Alert Originators and EAS Manufacturers with contact information appropriate for each community to be used to report a security incident relating to the EAS and its component parts.	
6	Threat Awareness	• Government should provide EAS Participants, Alert Originators and EAS Manufacturers, as appropriate, with information and updates regarding EAS-specific threats and general cybersecurity issues.	

6 Conclusions

The EAS Security sub-committee recommends that the EAS community should adopt these modest guidelines to secure EAS in its current state. The sub-committee recommends that all stakeholders incorporate EAS into their existing IT security program, or establish one if it does not exist. Coordination and collaboration between the EAS participants, EAS device manufacturers, alert originators, and the government will reduce the likeliness of EAS being compromised.

This work can never be considered complete since the threats and vulnerabilities of the EAS eco-system, the devices themselves, the participants and operators of the gear will continue to change and evolve. This document is a starting point that should be reviewed and renewed on a regular basis or become stale and unreliable as a source of ground truth for security recommendations for EAS. As a baseline it is an excellent start but the level of expected security for the EAS eco-systems may need to change based on future threats and vulnerabilities.

7 Appendix

7.1 References

The EAS security sub-committee utilized several bodies of knowledge as benchmarks for the creation of the recommended best practices contained in this document, including previous CSRIC and NRIC recommendations, as well as the updated SANS critical controls. In addition, the sub-committee notes a range of additional resources, compiled below, meant to support security cooperation and shared best practices.

7.1.1 CSRIC

Two previous sessions of the FCC-chartered Communications, Security, Reliability, and Interoperability Council (CSRIC) revised cybersecurity best practices presented by previous FCC advisory councils, as well as creating a number of additional best practices.

- CSRIC Working Group 2A Final Report, Cyber Security Best Practices (March 2011)
- CSRIC Working Group 11 Final Report, Consensus Cyber Security Controls (March 2013)

7.1.2 NRIC

The FCC-chartered Network Reliability and Interoperability Councils (NRIC) were Federal advisory committees that preceded CSRIC. The former NRICs were comprised of representatives from communications companies, communications industry associations, and government entities. The NRICs operated for 14 years (January 1992 through December 2005) and developed over 800 Best Practices. Since the charter of the CSRIC in 2007, over 200 additional new Best Practices have been established. An archive of NRIC best practices is hosted at http://www.atis.org/bestpractices/.

7.1.3 SANS Critical Controls

Taken from the SANS web site: http://www.sans.org/critical-security-controls/

7.1.3.1Critical Security Controls for Effective Cyber Defense

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly

evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (the Controls) were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the Controls was transferred to the Council on CyberSecurity (the Council), an independent, global non-profit entity committed to a secure and open Internet.

The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53. The Controls do not attempt to replace the work of NIST, including the Cybersecurity Framework developed in response to Executive Order 13636. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.

7.1.4 Additional Resources

- CAP, EAS AND IPAWS: Introducing a Defense in Depth Security Strategy for Cable and IPTV Operations, September 2011, Monroe Electronics. (http://www.monroe-electronics.com/EAS_pages/pdf/ME-WhitePaper_IndAdvisory_Network_Security_091211.pdf)
- CAP, EAS AND IPAWS: Introducing a Defense in Depth Security Strategy for Broadcasters, September 2011, Monroe Electronics / Digital Alert Systems. (http://www.digitalalertsystems.com/pdf/wpdas-122.pdf)
- Control Systems Cyber Security: Defense in Depth Strategies, October 2009, U.S. Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT. (https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf)
- Critical Controls for Effective Cyber Defense, SANS. (http://www.sans.org/critical-security-controls/cag4-1.pdf)
- Cyber Security Policy Guidebook, Jennifer L. Bayuk, Jason Healey, et al., Wiley, 2012.
- Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (Premier Reference Source), Junaid Ahmed Zubairi and Athar Mahboob, IGI Global, 2011.

- Developing a Framework To Improve Critical Infrastructure Cybersecurity, National Institute of Standards, February 12, 2013.
- DHS Sensitive Systems Policy Directive 4300A, Version 8.0, March 14, 2011 http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf
- Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper, Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, Tech America, March 8, 2011 (https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf).
- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook, National Institute of Standards. (http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)
- NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013, National Institute of Standards. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf)
- NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, National Institute of Standards.
- Password Security, Protection and Management, US CERT, 2012 (http://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf).
- Understanding Security for Your EAS Equipment: Best Practices and Recommendations for Users, Monroe Electronics/Digital Alert Systems, January 15, 2014 (http://www.digitalalertsystems.com/pdf/DAS%20EAS%20Security%20WhitePaper%2001152014.pdf)

7.2 Glossary

Access Control	Access Control ensures that resources are only granted to those users who are entitled to them.
Access Type	Privilege to perform an action on an object.
Administrative Account	A user account with full privileges on the computer, appliance or system.
Authentication	Authentication is the process of confirming the correctness of the claimed identity.
Basic Authentication	Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.
CERT	Computer Emergency Response Team. An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Data Owner	A Data Owner is the entity having responsibility and authority for the data.
Day Zero	The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one"-> day at which the patch is made available).
DDoS	A Denial of Service attack that uses numerous hosts to perform the attack
Defense in Depth	Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.
Denial of Service	The prevention of authorized access to a system resource or the delaying of system operations and functions.
DHS	Department of Homeland Security
Disaster Recovery Plan	A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.
DMZ	In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet that is used for servers accessible from the outside is referred to as a DMZ.
Filtering Router	An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.
Firewall	A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A security tool that protects an individual computer or even an entire network from unauthorized attempts to access your system.
Gateway	A network point that acts as an entrance to another network.

Hacker	A hacker is someone who has the technical know-how to intentionally breach or "hack" into a computer system to steal confidential information or to cause damage to a computer or whole network.
Hardening	Hardening is the process of identifying and fixing vulnerabilities on a system.
Hash Function	An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.
Header	A header is the extra information in a packet that is needed for the protocol stack to process the packet.
ICS-CERT	The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.
Intranet	A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.
Intrusion Detection	A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
Least Privilege	Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.
Malware	A generic term for a number of different types of malicious code.
NCCIC	The National Cybersecurity & Communications Integration Center (NCCIC), within the DHS Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated.
Network Mapping	To compile an electronic inventory of the systems and the services on your network.

NIST	National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.
NSTAC	The President's National Security Telecommunications Advisory Committee (NSTAC) mission is to provide the U.S. Government the best possible industry advice on telecommunications availability and reliability.
Risk Assessment	A Risk Assessment is the process by which risks are identified and the impact of those risks determined.
Router	Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
Threat Assessment	A threat assessment is the identification of types of threats that an organization might be exposed to.
Threat Model	A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.
Threat Vector	The method a threat uses to get to the target.
Trust	Trust determine which permissions and what actions other systems or users can perform on remote machines.
US-CERT	The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation
Virus	A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed.
VLAN	VLAN is a virtual LAN. A VLAN is a broadcast domain created by switches, usual created by a router. With VLAN's, a switch can create the broadcast domain.

VPN	A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. Establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions creates a VPN.