Summary of NPRM FCC 22-82 on EAS Cybersecurity NPRM Released: October 27, 2022

By Gary Timm, Wisconsin EAS Committee (FCC SECC), 2022/11/26

Note: This summary only addresses EAS proposals in this NPRM. It does not address the WEA proposals.

Comment Period end date: December 23, 2022 [30 days after publication in the Federal Register]
Reply Comment Period end date: January 23, 2023 [60 days after publication in the Federal Register]

The Apparent FCC Impetus for this NPRM: Despite the Commission's issuance of EAS cybersecurity guidance and Public Notices in the past few years, the 2021 Nationwide EAS Test results revealed over 5,000 EAS Participants with outdated software in their EAS units or using equipment that could no longer be updated, and over 500 others that were unable to carry the test due to EAS equipment missing, out for repair, or failed on test day. Therefore, the FCC felt compelled to act.

Promoting the Operational Readiness of EAS Equipment

- Currently, EAS Participants have 60 days to repair EAS equipment without notice to the FCC, but must note in the Station Log the date the EAS equipment was removed and then reinstalled.
- FCC asks if 60 days should be replaced with the phrase, "promptly with reasonable diligence"?
- For local situational awareness, should the FCC require immediate reporting of failed equipment and subsequent repair, and share that information with alert originators and SECCs, or keep it confidential?

Improving Awareness of Unauthorized Access to EAS Equipment

- FCC proposes to expand the current 11.45(b) false alert reporting rule to require EAS Participants report any incident of unauthorized access to its EAS equipment (regardless of whether it resulted in transmission of a false alert) to the FCC NORS website within 72 hours of when it knew or should have known that an incident had occurred.
- This rule would apply to all of EAS Participant's "communications systems or services", e.g. firewalls or VPNs.
- The FCC provides a definition of "unauthorized access" – is it accurate? [Para. 18] Is 72 hours too long/short?
- The FCC invites comment on info requested in the unauthorized-access reports [Para. 19], and suggests they should be considered "presumptively confidential" (shared only with Federal and State agencies), although Footnote 64 mentions disclosure of the identity of EAS Participants when it serves the public interest.
- FCC asks if these reports should be submitted to the FCC Ops Center email address as current false alert reports are, or to the NORS website for better Federal agency sharing, or to a new database?

Development, Implementation and Certification of a Cybersecurity Risk Management Plan (CRMP)

- The FCC proposes to require EAS Participants to submit an annual certification attesting that they have created, updated, and implemented a cybersecurity risk management plan. The CRMP would describe how the EAS Participant employs their organizational resources and processes to ensure the confidentiality, integrity, and availability of the EAS. The plan must discuss how the EAS Participant identifies the cyber risks that they face, the controls they use to mitigate those risks, and how they ensure that these controls are applied effectively to their operations. [quoted from Para. 23]
- FCC proposes to afford each EAS Participant flexibility to structure its plan in a manner that is tailored to its organization, provided that the plan demonstrates that the EAS Participant is taking affirmative steps to analyze security risks and improve its security posture. [Para. 24]
- FCC proposes that EAS Participants can successfully demonstrate that they have satisfied this requirement by structuring their plans to follow an established risk management framework, such as the National Institute of Standards and Technology (NIST) Risk Management Framework [URL in Footnote 69] or the NIST Cybersecurity Framework [URL in Footnote 70]. FCC asks if they should require the use of one of these NIST Frameworks, including any future updated version? [Footnote 72 has 3rd NIST document, current version of the Framework]

- FCC proposes that each cybersecurity risk management framework include security controls sufficient to ensure the confidentiality, integrity, and availability (CIA) of the EAS. FCC proposes that EAS Participants will have satisfied it if they demonstrate they have successfully implemented an established set of cybersecurity best practices, such as applicable CIS Critical Security Controls [URL in Footnote 74] or the CISA Cybersecurity Baseline [URL in Footnote 75].
- FCC proposes to require that each plan include security measures that address changing default passwords prior to operation, installing security updates in a timely manner, securing equipment behind properly configured firewalls or using other segmentation practices, addressing the replacement of end-of-life equipment, and wiping, clearing, or encrypting user information before disposing of old devices. [Footnotes 76-80 outline where in the CIS and CISA documents above this guidance is found.]
- Should FCC require network security audits and vulnerability assessments?
- Should FCC require reporting when assessments reveal "critical vulnerabilities" and how to define those?
- Should FCC require an Incident Response Plan for reacting to cyber events?
- Should FCC require employee cybersecurity training?
- Should FCC require EAS Participants to keep records that demonstrate how they have implemented each of the baseline security controls? If so, what specific types of information should the records include and for how long should they be kept?
- Is the proposed requirement too burdensome on small EAS Participants?
- Instead of a cybersecurity plan, should there just be specific steps to take?
- FCC proposes that beyond the EAS unit itself, the CRMP cover all aspects of the EAS Participant's "communications systems and services" that potentially could affect use of EAS.
- Are there industry groups, cybersecurity organizations, or other organizations that may be positioned to help EAS Participants create, implement, and maintain their cybersecurity risk management plan?
- FCC proposes that EAS Participants certify to creating, annually updating, and implementing a CRMP by checking a box as part of its annual filing of EAS Test Reporting System Form One.
- FCC proposes that the CRMP be made available to the Commission upon request. FCC asks how long EAS Participants should be required to retain prior versions of their CRMP?
- FCC proposes that the filing of, and subsequent compliance with, a CRMP would not serve as a safe harbor or excuse or any other diminishment of responsibility for negligent security practices. Any negligence in protecting the confidentially, integrity, and availability of EAS that results in transmission of false alerts or non-transmission of valid EAS messages would establish a violation of that duty, regardless of the content of the plan.
- FCC proposes that an EAS Participant's failure to sufficiently develop or implement their plan, would be treated as a violation of the proposed rules.
- FCC seeks comment on the criteria that should be considered when determining whether a plan is insufficient to mitigate cyber risk.
- FCC seeks comment on any measures that the Commission should take to verify whether EAS Participants have implemented their plans.
- FCC believes the benefits of the proposals outweigh the costs. [Para. 31]
- FCC estimates an average of 10 hours/year to draft and annually update the plan.

<u>Compliance Timeframes</u>
Operational Readiness of EAS Equipment: Asks 30 days after OMB approval published in Federal Register?
Awareness of Unauthorized Access: Proposes 60 days after OMB approval published in Federal Register.
Certifying Implementation of CRMP: Proposes 12 months after OMB approval published in Federal Register. (Asks if Small Business EAS Participants should get an additional 12 months, to 24 months after OMB in FR?)