<u>Urgent Advisory: Immediate actions to be taken regarding CAP EAS device security.</u>

All EAS Participants are required to take immediate action to secure their CAP EAS equipment, including resetting passwords, and ensuring CAP EAS equipment is secured behind properly configured firewalls and other defensive measures. All CAP EAS equipment manufacturer models are included in this advisory.

All Broadcast and Cable EAS Participants are urged to take the following actions immediately

1. EAS Participants must change all passwords on their CAP EAS equipment from default factory settings, including administrator and user accounts.

2. EAS Participants are also urged to ensure that their firewalls and other solutions are properly configured and up-to-date.

3. **EAS Participants are further advised to examine their CAP EAS equipment to ensure that no unauthorized alerts or messages have been set (queued) for future transmission.**

4. If you are unable to reset the default passwords on your equipment, you may consider disconnecting your device's Ethernet connection until those settings have been updated.

5. EAS Participants that have questions about securing their equipment should consult their equipment manufacturer.