GORMAN-REDLICH

GORMAN REDLICH
257 West Union St.
Athens, Ohio 45701
FAX: 740-592-3898
Ph: 740-593-3150

EAS Security Statement

2.13.2013

As you are probably aware, recent security breaches at several broadcast stations have resulted in the dissemination of false EAS messages. It appears that these breaches may have been the result of the networked EAS equipment being accessed using the equipment's default factory password settings which were not changed by the equipment owners/operators. The FCC has released an advisory (pasted below) with suggested actions regarding alerting equipment security.

Please note that such false messages are NOT capable of being generated from a proper installation of a stand-alone Gorman-Redlich EAS-1 unit, a combination of a Gorman-Redlich CAP-DEC 1 unit and a Gorman-Redlich EAS-1 unit or the combination of a Gorman-Redlich CAP-DEC 1 unit and non-network-connected "legacy" EAS equipment from other manufacturers. In such setups, the only networked equipment is the CAP-DEC 1 unit, which is not capable of originating EAS messages (rather, it is only capable of receiving CAP formatted alert messages from the specified alert feeds and translating them into EAS messages for the "legacy" equipment).

However, "legacy" EAS equipment may still be capable of originating an alert message when an operator is present at the equipment site. As such, appropriate physical security measures must be taken, including changing factory default access settings. Further, some CAP-DEC 1 units may be configured with remote access functionality. While this functionality would not allow the origination of a broadcast emergency message, appropriate network security measures and access restrictions should be in place to protect such remote access from unauthorized users.

Gorman-Redlich EAS-1 encoder/decoder equipment has two passwords: the Operator Password and the Technician Password. Please refer to your equipment documentation for default passwords and instructions for changing these passwords. Passwords of units with firmware v9.7+ may be changed within the utility menu. Additionally, EAS Setup Software for EAS-1 units may be found in the Software Downloads section of the Downloads page at www.Gorman-Redlich.com.

The following advisory was released by the FCC on 2.12.2013 regarding these recent events:

Urgent Advisory: Immediate actions to be taken regarding CAP EAS device security.

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.