Cooley

FCC Proposes Cybersecurity Requirements for Broadcasters and MVPDs

February 1, 2016

The Federal Communications Commission has proposed rules requiring all participants in the nation's emergency alert system ("EAS") to implement certain cybersecurity risk management practices. The proposed rules could apply to all of the 27,468 radio and TV broadcast stations, cable systems, and direct broadcast satellite service providers that participate in the EAS ("EAS Participants"). Comments on the proposals are due thirty days after publication of the FCC's notice in the Federal Register.

The FCC's notice makes clear its disappointment with what it perceives as industry's failure to take steps needed to protect the nation's emergency alert system from hacking and false alerts: "[I]f EAS Participants cannot effectively secure the system through voluntary mechanisms, the Commission must explore regulatory solutions to achieve EAS security. Accordingly, we now propose rules designed to safeguard the EAS and maintain continued public trust in the system."

Proposed rules to codify best practices

The FCC's proposals would "codify best practices consistent with" certain of the recommendations made by the Communications Security, Reliability and Interoperability Council ("CSRIC"), an industry-led advisory committee that released comprehensive reports on cybersecurity risk management best practices in 2014. The proposed rules cover three main areas: (1) an annual certification of compliance with four specific best practices described below; (2) reporting of false alerts and "lock outs," which occur when the EAS is triggered and viewers are prevented from watching any channel other than the one carrying the alert; and (3) ensuring that alerts are properly authenticated and validated in order to prevent issuance of false alerts.

Annual certifications. The FCC proposed that EAS Participants submit an annual reliability certification "attesting to performance of required security measures with a baseline security posture in four core areas." The certification, which would be signed by a corporate officer under penalty of perjury, would require EAS Participants to certify compliance with the following:

- **Patch management.** That they keep their systems updated with the latest firmware and software patches.
- **Account management.** That they have a control system in place to restrict access to EAS devices, that all EAS devices and connected system passwords have been changed from the default passwords, that password complexity is required, and that default, unnecessary, and expired accounts have been removed or disabled.
- **Segmentation.** That none of their EAS devices is directly accessible through the Internet, (for example, by configuring a firewall to deny access from the public Internet) and that any other type of remote access is properly secured and logged.
- **Validation.** That their EAS devices are configured to validate digital signatures on Common Alerting Protocol ("CAP") messages if the source of the CAP message includes this feature. CAP is used to distribute alerts to stations over the Internet.

Mandatory reporting and notification. The FCC proposed requiring EAS Participants to report, within 30 minutes, the issuance or retransmission of a false EAS message and to report within 15 minutes instances when their EAS equipment causes, contributes to, or participates in a lockout that adversely affects the public (*e.g.*, when multiple cable set top boxes s cannot return to normal operation due to the failure to receive the appropriate "unlock" signal or otherwise correctly process an EAS alert). The FCC proposed that the fact of filing such a report would **not** be confidential but details in the report would be confidential.

Alert authentication. The FCC proposed to require that EAS Participants process and validate digital signatures when handling CAP-formatted EAS alerts, and discard as invalid any CAP message where the digital signature does not match an authorized source.

Questions regarding reach and cost

The FCC is seeking comment on a host of questions regarding these proposed rules, including whether to limit their application to only national alerts that are triggered by the President, or to require compliance only by certain stations based either on their position in the alert dissemination system or to exclude small companies.

The FCC is also seeking comment on whether and how broadcasters and cable operators are or should be making EAS alerts available to consumers who access their programming via social media or other platforms, such as streaming video over the Internet or through an app. The FCC asks whether consumers may expect that alerts will be available regardless of technology platform; whether current technologies support the standardization of alerts across technologies, applications and platforms; and whether the FCC has the statutory authority to expand alert requirements beyond current EAS Participants.

One of the more significant questions involves the costs to the industry of complying with these proposed rules. The FCC assumes de minimus compliance costs based in part on an assumption that only ten percent of stations are not already taking these steps. For stations not currently able to make the certifications, the FCC assumes coming into compliance would take four hours at a cost of $80 per hour. This assumption seems in direct tension with the FCC's statement that it needs to adopt rules because the industry has not taken voluntary steps.

Questions regarding information sharing

The FCC devoted an entire section of its discussion to confidentiality and information sharing. Much interest in the area of information sharing has developed as a result of the passage of the **Cybersecurity Act of 2015 ("CSA")**. The CSA establishes a framework to allow effective sharing of information between the private and public sector. The FCC echoes the goals of the CSA by pointing out that it "must weigh the public's presumed benefit in being able to assess, in real time, the security of its EAS, and we tend to generally favor disclosure over [the] confidentiality" approach used in other FCC scenarios.

Cooley expertise

Cooley has significant expertise counseling clients regarding cybersecurity and EAS issues. If you would like more information regarding the FCC's proposals, or would like to explore filing comments in the proceeding, please contact one of the attorneys identified on this alert.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140