260.72, 260.73, 260.74, 260.75, and 260.76.

PART 261—ENSURING THAT RECIPIENTS WORK

■ 14. The authority citation for part 261 continues to read as follows:

Authority: 42 U.S.C. 601, 602, 607, and 609; Pub. L. 109–171.

§§ 261.1 261.10, 261.11, 261.12, 261.13, 261.14, 261.15, 261.16, 261.21, 261.23, 261.30, 261.33, 261.35, 261.36, 261.54, 261.70, and 261.80 [Removed and reserved]

■ 15. Remove and reserve §§ 261.1, 261.10, 261.11, 261.12, 261.13, 261.14, 261.15, 261.16, 261.21, 261.23, 261.30, 261.33, 261.35, 261.36, 261.54, 261.70, and 261.80.

PART 262—ACCOUNTABILITY PROVISIONS—GENERAL

■ 16. The authority citation for part 262 continues to read as follows:

Authority: 31 U.S.C. 7501 *et seq.;* 42 U.S.C. 606, 609, and 610; Sec. 7102, Pub. L. 109–171, 120 Stat. 135; Sec. 4004, Pub. L. 112–96, 126 Stat. 197.

§§ 262.0 and 262.1 [Removed and reserved]

■ 17. Remove and reserve §§ 262.0 and 262.1.

PART 263—EXPENDITURES OF STATE AND FEDERAL TANF FUNDS

■ 18. The authority citation for part 263 continues to read as follows:

Authority: 42 U.S.C. 604, 607, 609, and 862a; Pub. L. 109–171.

§§ 263.1, 263.3, 263.8, 263.9, 263.20, 263.21, and 263.22 [Removed and reserved]

■ 19. Remove and reserve §§ 263.1, 263.3, 263.8, 263.9, 263.20, 263.21, and 263.22.

PART 264—OTHER ACCOUNTABILITY PROVISIONS

■ 20. The authority citation for part 264 continues to read as follows:

Authority: 31 U.S.C. 7501 *et seq.;* 42 U.S.C. 608, 609, 654, 1302, 1308, and 1337.

§§ 264.0, 264.2, 264.40, 264.60, 264.61, 264.70, 264.71, 264.83, and 264.85 [Removed and reserved]

■ 21. Remove and reserve §§ 264.0, 264.2, 264.40, 264.60, 264.61, 264.70, 264.71, 264.83, and 264.85.

PART 265—DATA COLLECTION AND REPORTING REQUIREMENTS

■ 22. The authority citation for part 265 continues to read as follows:

Authority: 42 U.S.C. 603, 605, 607, 609, 611, and 613.

§ 265.6 [Removed and reserved]

■ 23. Remove and reserve § 265.6.

PART 270—[REMOVED AND RESERVED]

■ 24. Under the authority of 42 U.S.C. 603(a)(4), remove and reserve part 270.

PART 283—[REMOVED AND RESERVED]

■ 25. Under the authority of 42 U.S.C. 603, remove and reserve part 283.

PART 284—[REMOVED AND RESERVED]

■ 26. Under the authority of 42 U.S.C. 613(i), remove and reserve part 284.

PART 286—TRIBAL TANF PROVISIONS

■ 27. The authority citation for part 286 continues to read as follows:

Authority: 42 U.S.C. 601. 604, and 612; Public Law 111–5.

§§ 286.15, 286.60, 286.130, 286.175, 286.180, 286.235, and 286.285 [Removed and reserved]

■ 28. Remove and reserve §§ 286.15, 286.60, 286.130, 286.175, 286.180, 286.235, and 286.285.

PART 287—THE NATIVE EMPLOYMENT WORKS (NEW) PROGRAM

■ 29. The authority citation for part 287 continues to read as follows:

Authority: 42 U.S.C. 612.

§§ 287.5, 287.15, 287.20, 287.35, 287.40, 287.60, 287.65, 287.90, 287.95, 287.100, 287.105, 287.165, and 287.170 [Removed and reserved]

■ 30. Remove and reserve §§ 287.5, 287.15, 287.20, 287.35, 287.40, 287.60, 287.65, 287.90, 287.95, 287.100, 287.105, 287.165, and 287.170.

Robert F. Kennedy, Jr.,

Secretary, Department of Health and Human Services.

[FR Doc. 2026–15567 Filed 7–30–26; 8:45 am]

BILLING CODE 4184–36–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 11

[PS Docket Nos. 22–329, 25–224; FCC 26–38; FR ID 359234]

Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems From Cybersecurity Threats

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In the Report and Order, the Federal Communications Commission (the FCC or the Commission) seeks to preserve the public's trust in the Emergency Alert System (EAS) by requiring targeted cybersecurity improvements that will help protect against hijacking by cybercriminals and our nation's adversaries.

DATES: This rule is effective September 29, 2026.

FOR FURTHER INFORMATION CONTACT: For further information concerning the information contained in this document, please contact David Kirschner, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at 202–418–0695, or by email to *David.Kirschner@fcc.gov,* or George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at 202–418–0729, or by email to *George.Donato@fcc.gov*.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order (*Order*) in PS Docket Nos. 22–329 and 25–224, FCC 26–38, adopted on June 25, 2026, and released on June 29, 2026. A summary of the accompanying proposed rule in PS Docket Nos. 25–224, 15–94, and 15–91, FCC 26–38, adopted on June 25, 2026 and released on June 29, 2026 is published elsewhere in this issue of the **Federal Register**. The full text of this document is available at *https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf.*

Procedural Matters

Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.''

Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this Report and Order on small entities.

Congressional Review Act. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

Paperwork Reduction Act Analysis. This Report and Order does not contain proposed information collections subject to the Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. 3501–3521. In addition, therefore, it does not contain any new or modified information collection burden for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. 3506(c)(4).

Synopsis

Goals of the Nation's Alerting Systems

In the *Alerting Modernization NPRM,* we sought comment on the objectives that effective alert and warning systems should serve. Specifically, we sought comment on three possible core goals: (1) alerting systems should provide authorities with the ability to rapidly notify the public of emergencies that may put the public at risk; (2) alerting systems should be capable of delivering instructions that facilitate the protection of life and property; and (3) alerting systems should provide a mechanism for government officials to provide additional authoritative communications with the public before, during, and after an emergency. Commenters generally agree that these should be the overarching goals of the nation's alert and warning systems. The Alliance for Telecommunications Industry Solutions (ATIS) ''fully supports these three goals and notes that the industry has continuously evolved WEA to meet these objectives.'' The Competitive Carriers Association (CCA) believes that these ''broad but simple goals proposed for the nation's alerting systems . . . seem appropriate . . . [as they] are worthwhile, important to public safety, and consistent with statutory instructions and intent.'' North Carolina Emergency Management et al., the Harris County Office of Homeland Security & Emergency Management (Harris County), APCO International (APCO), and the National Weather Service (NWS) also agree with the three stated objectives, with the NWS noting that, ''[w]hile a perfect alerting system is not possible, it should have the main goal of being easy to use and available to anyone.''

The U.S. Geological Survey (USGS) supports the three core goals the Commission proposed for alerting systems, but contends that they ''are focused on the capabilities of the system rather than on the public safety outcomes they are intended to achieve.'' Sonoma County Department of Emergency Management, Snohomish County Department of Emergency Management, former California Office of Emergency Services Director Art Botterrell, and Washington State Emergency Management Division likewise emphasize that public safety outcomes are of utmost importance. iHeartMedia, Inc. supports the three objectives that we identified, but believes we should consider a fourth: ''(4) alerting systems should include resilient and reliable delivery systems proven capable of functioning during emergencies, including when other emergency alerting technologies may be unavailable.'' The New York City Emergency Management Department (NYCEM) agrees with us that ''the speed of notification is a critical component of any alerting system'' but proposes the following alternative to our third objective focused on ensuring the ability for authorities to send authoritative alerts to the public: ''Alerting systems should be designed and utilized to ensure that all members of the public receive an alert and are aware of actions that they may take to protect life and property. . . . [A]lerting systems should be available in a wide array of languages, able to be displayed on various devices, and include considerations for members of the public with various accessibility needs.'' Although we understand and appreciate the proposals for additional goals of alerting, we conclude that the three goals we proposed already encompass these important public safety-, resiliency-, and accessibility-focused concerns within the objectives that effective alert and warning systems should serve. For example, while we agree with iHeartMedia, Inc. that alerting systems must be resilient and reliable, and capable of functioning when other emergency alerting technologies may be unavailable, that objective is subsumed within our goal of providing authorities with the ability to rapidly notify the public of emergencies that may put them at risk. NYCEM's view that alerting systems should be available in a wide array of languages and on a variety of devices falls within the core goal of notifying the public of emergencies, as that notification can only occur if recipients can receive and understand the message.

Commenters recognize that the Commission should continue to evaluate ways to improve these systems, and we agree. As Sinclair comments: ''Ultimately, the nation's alerting systems are critical to the preservation of public health and safety, and examining ways to enhance or improve these systems can save lives.'' We also find that commenters generally recommend that, while alerting systems can be improved, we should refrain from making fundamental changes to EAS and WEA. We agree with commenters that these systems generally meet today's alerting objectives, and determine that incremental improvements advance the core goals of the nation's alerting systems. At this time, we therefore decline to overhaul or phase out the legacy EAS architecture. Legacy EAS continues to effectively support public safety by creating alerting pathway redundancy, making alerting more resilient, and by warning the public and informing them about protective actions to take during emergencies. Eliminating it would create a gap in alert delivery that would threaten the achievement of our three goals. Consistent with the record, we take steps to improve EAS and WEA as they exist today.

Cybersecurity Requirements Targeting Specific EAS Attack Vectors

Central to our effort to modernize the nation's alerting systems is ensuring those systems are secure. Commenters to both the *Alerting Modernization NPRM* and the *Alerting Security NPRM* broadly agree that it is vital to ensure the security of EAS and WEA. Foreign adversaries, criminals, and other bad actors can wreak havoc if they gain access to alerting systems, by sending a false alert that causes public panic or delivers false information about a disaster or crisis, or by preventing a real alert from being transmitted to the public. As one former broadcaster who submitted comments points out, the dissemination of false alerts can also undermine public trust in alerting capabilities, which depends on ''ensuring that every message originates from an authorized and verifiable source.'' Because of these risks, keeping these systems ''secure against cyberattacks from our nation's adversaries'' and ''[m]aintaining trust in

these systems is vital for both national security and achieving the nation's alerting goals.''

Today, we adopt three targeted measures that aim to ensure that EAS Participants secure their equipment to prevent cyberattacks that could result in the transmission of false EAS alerts or disrupt the transmission of legitimate alerts. Specifically, we require EAS Participants to do the following with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream: (1) prior to operation, change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised; (2) test and install security patches and security-related software and firmware upgrades issued by equipment manufacturers promptly after those patches or upgrades become available; and (3) use a network firewall or comparable network segmentation practice to limit remote management access to authorized devices and authorized users.

These three requirements represent a subset of the six basic cybersecurity hygiene requirements that the Commission proposed to require EAS Participants to implement as part of their cybersecurity risk management plans in the *Alerting Security NPRM.* In the *Alerting Security NPRM,* the Commission proposed to require EAS Participants to implement these cybersecurity measures in the context of their implementation of broader cybersecurity risk management plans. The Commission sought comment on whether that approach ''strik[es] the appropriate balance between improving EAS security, complementing EAS Participants' existing cybersecurity activities, and reducing burdens on small EAS Participants?'' In response, commenters express concern that compliance with precise cybersecurity risk management requirements would be costly, could hinder their ability to adapt to changing cybersecurity needs, and could subject them to strict liability enforcement in the event an EAS Participant is victimized by a cyberattack. The approach we adopt today responds to those concerns by eliminating the broader cybersecurity risk management and threat assessment components of the proposed requirement, as well as the proposed requirements that EAS Participants employ ''sufficient security controls to ensure the confidentiality, integrity, and availability of the EAS.''

The *Alerting Security NPRM* asked whether, ''[i]nstead of requiring the use of a risk management plan, should [the Commission] require EAS Participants to take specific steps to secure their EAS equipment?'' In addition, the *Alerting Modernization NPRM* asked if there are ''specific authentication, validation, and security measures that EAS and WEA should be designed to incorporate?'' In response to the *Alerting Modernization NPRM,* APCO and other commenters agree that the Commission should adopt specific security requirements for EAS Participants. As with other commenters to the *Alerting Security NPRM,* National Public Radio (NPR) is concerned about the costs of cybersecurity risk management plan requirements and asks that EAS Participants be required to, instead, only implement the basic security measures that the Commission proposed without requiring the creation of broader risk management plans. REC Networks agrees that ''security of EAS equipment is of paramount importance'' but asks that smaller EAS Participants be required to ''implement a simpler plan of good network operating practices, which involve network configuration, password management and protection, periodic password changes[,] and other 'common sense' methods to assure that EAS equipment is not compromised.'' The approach we adopt today is consistent with NPR's view that we should require EAS Participants to implement minimum security controls, rather than comprehensive risk management plans, while also respecting REC Networks' view that some of the specific security measures we proposed to require, such as addressing the replacement of end-of-life equipment and wiping, clearing, or encrypting user information before disposing of old devices, may be more complicated than is appropriate to require of some EAS Participants. Other commenters, such as NCTA, express concern that requiring EAS Participants to implement a specific cybersecurity framework would ''freeze cybersecurity practices in time and hamper an EAS Participant's ability to develop and implement cybersecurity measures in response to its specific cybersecurity risk profile, to the detriment of public safety.'' The requirements we adopt today will not hamper an EAS Participant's ability to respond to evolving cybersecurity threats. Rather, they represent a minimum acceptable baseline that will harden critical communications infrastructure against today's threats, while being flexible enough to adapt to changes in the threat environment.

The cybersecurity requirements we adopt today are narrowly tailored to address vulnerabilities that have been repeatedly exploited through a series of cyberattacks on EAS Participants in recent months. In these attacks, bad actors gained control of radio broadcasters' systems by exploiting improperly secured, remotely accessible equipment in the broadcast signal processing system to transmit unauthorized audio that included EAS alert tones, an offensive song that included racial slurs, and promotional content. In response to the attacks, the Public Safety and Homeland Security Bureau (Bureau) released a Public Notice on November 23, 2025, urging broadcasters to immediately implement basic cybersecurity hygiene best practices to secure their systems and protect EAS, including installing software security patches for broadcast equipment issued by the manufacturer as soon as they become available; upgrading equipment firmware and software to the most recent versions recommended by the manufacturer; changing devices' default passwords and replacing them with robust alternatives; regularly changing passwords to promote continued security; and, where reasonably feasible, installing EAS, studio-transmitter link equipment, and other equipment interconnected to the broadcast signal processing system behind network firewalls. Similar attacks on broadcasters going back more than a decade have included hoax radio broadcasts about a zombie attack and false alerts about a ''radiological hazard'' sent to cable subscribers through the infiltration of EAS equipment connected to the internet. The Bureau recently convened a cybersecurity workshop for broadcasters that brought together public and private sector representatives to raise awareness of emerging cybersecurity risks, share and promote the adoption of best practices, and highlight opportunities for public-private partnerships on cybersecurity issues facing broadcasters. Despite our repeated efforts urging EAS Participants to take basic steps to secure their networks, including the November 2025 Public Notice, an August 2022 Public Notice recommending similar steps to those we recommended last year, and an April 2020 email to EAS Participants encouraging them to secure their EAS equipment by installing current security patches, successful attacks have continued into 2026.

Because some EAS Participants have not taken adequate steps to remediate these vulnerabilities and address the

significant risk posed by a false alert or non-transmission of a real alert, we find that each of the three requirements we adopt today are necessary to protect the security and integrity of EAS.

Password requirements. Strong password security is essential to protecting EAS equipment, studio-transmitter link equipment, and remotely accessible equipment from unauthorized access that exploits weak or default credentials. Digital Alert Systems, Inc. (DAS) and former broadcaster, Jonah Kibin, caution against using default passwords and recommend changing required credentials upon setup as default passwords, particularly on encoders, ''are widely available on the internet and have led to high-profile intrusions of the EAS in the last couple of decades.'' We require that default passwords for EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream be changed prior to any use to broadcast to the public. Passwords used for this equipment must employ a minimum of 15 characters, not use dictionary words (because they can be cracked through brute force), and not be reused for other accounts, equipment, applications, and services that the EAS Participant uses.

As an alternative to a strong password, we permit EAS Participants to use alternative authentication measures that are reasonably sufficient to mitigate the risk of unauthorized access. We believe that there are numerous authentication methods available to EAS Participants that would be reasonably sufficient, including methods that have been highlighted by the National Institute of Standards and Technology (NIST) as meeting one of three authentication assurance levels. For example, NIST's guidance provides that authentication properly implemented at Authentication Assurance Level 1 can include, in addition to passwords, look-up secrets, which are ''[a] secret determined by the claimant by looking up a prompted value in a list held by the subscriber''; out-of-band devices, consisting of ''[a] secret sent or received through a separate communication channel with the subscriber''; single- or multi-factor one-time password devices, in which a one-time secret is obtained from a device or application held by the subscriber, which may or may not require activation by a second authentication factor; and single- or multi-factor cryptographic authentication, which entails ''[p]roof of possession and control via an authentication protocol of a cryptographic key held by the subscriber,'' which may or may not require activation by a second authentication factor. We recognize that, were we to simply require use of specifically structured passwords, our rule could preclude the use of other authentication methods offering equal or better security. To ensure our requirements do not result in reducing the security of currently secure systems, the rule we adopt today continues to allow EAS Participants to secure their equipment through means that are equally or more secure than the password requirements we adopt today.

As DAS observes, ''systemic risks'' are created when EAS Participants use ''[w]eak passwords [and] shared accounts.'' These risks are present throughout the industry. As the National Television Association concedes, many EAS Participants ''had never changed the default password on their EAS device(s).'' A former broadcaster further emphasizes that the use of default passwords to widely owned broadcast equipment—many of which are publicly available—has contributed to multiple high-profile intrusions over the past decade, demonstrating that these risks are neither hypothetical nor isolated. NPR characterizes requirements to change default passwords and secure equipment as reasonable and sound. Prometheus Radio Project supports Low Power FM stations ''maintaining a firewall, following password management best practices, and implementing multi-factor authentication.'' REC Networks supports the immediate changing of default passwords, and includes this as one of the recommendations in its Practice of Good Network Security for Small Stations. This requirement aligns with authoritative, industry-recognized cybersecurity standards, including the Cybersecurity & Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs), which are designed for operators of critical infrastructure such as communications networks. We have elsewhere pointed to the CISA CPGs as an instructive suite of cybersecurity best practices for communications service providers. The Submarine Cable Second Report and Order adopts certain national security standards that, if met, will presumptively exempt a submarine cable application from referral to the Executive Branch agencies, including that the applicant must affirm, as part of its required cybersecurity and physical security risk management plan certification, that the plan meets a set of established cybersecurity best practices such as the standards and controls set forth in the CISA CPGs. Specifically, CISA CPG 3.A, ''Changing Default Passwords,'' encourages companies to address the risk that ''[a]dversaries might acquire and exploit default account credentials to gain initial access, maintain persistence, escalate privileges, or evade defenses'' by ''[i]mplement[ing] an organization-wide policy that requires changing default manufacturer passwords for all hardware, software, and firmware before connecting them to any internal or external network.'' We disagree with NCTA's suggestion that cybersecurity protections should be limited to EAS equipment alone, as this would be insufficient to protect EAS when unprotected studio transmitter link equipment and remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream create similar opportunities to transmit false alerts or disrupt the transmission of real alerts. The password characteristics that we require reflect the CISA and NIST guidance on minimum password strength and unique credentials. We expect compliance with the requirement to be straightforward for EAS Participants, which need only log into each relevant piece of equipment, locate the account-management or security settings, and replace the factory-set default password or existing weak password with a strong, unique password—a process that should be repeated whenever the EAS Participant has reason to believe that the password has been compromised.

Firmware and Software Patching. Prompt firmware and software patching are key to reducing the risk that bad actors will exploit known vulnerabilities to infiltrate broadcast and cable systems to insert false EAS tones or alerts. The record includes support for requiring EAS Participants to promptly install security patches and firmware and software updates. DAS also points to the failure to apply software updates as a ''systemic risk[]'' to EAS. One comment submitted by a radio broadcast engineer recommends that the Commission require EAS equipment to automatically query a centralized database to confirm EAS codec firmware and certificate updates. APCO opines that ''[t]he Commission should consider rules requiring EAS and WEA participants to maintain current software and replace outdated equipment in a timely manner,'' citing

findings from the Commission's 2023 Nationwide Emergency Alert Test showing that ''approximately 23 percent of the EAS equipment units were either using outdated software or operating equipment that was no longer supported with regular software updates.'' The fact that nearly a quarter of EAS devices may potentially be exposed to known, readily addressed vulnerabilities because they are operating obsolete or out-of-date equipment represents a significant gap in the security of the nation's alerting capacity that poses national security risks. Promptly testing and installing security patches and software and firmware upgrades will also address DAS's concern that ''[g]ray-market EAS encoders/decoders (*i.e.,* used equipment sold on auction websites) can ship with outdated firmware and unremoved configurations or credentials, allowing attackers to exploit known vulnerabilities or use retained settings to impersonate sources and inject false alerts.'' Going forward, EAS Participants will be responsible for ensuring that their EAS devices are properly patched and updated, regardless of the devices' provenance. The requirement to install patches and update software promptly also aligns with CISA's CPGs. Specifically, CISA CPG 2.B encourages companies to ''Mitigate Known Vulnerabilities'' by ''[i]mplement[ing] a vulnerability management program to patch and mitigate misconfigured software in a timely manner'' to protect against the risk that ''[a]dversaries frequently target unpatched and misconfigured systems, particularly those exposed to the internet,'' and ''often leverage software vulnerabilities, temporary malfunctions, or configuration errors to gain initial access to a network.'' Here, too, we expect implementation to be simple. Once a security patch, or security-related software or firmware upgrade, becomes available for EAS equipment, studio transmitter link equipment, or any other remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming, EAS Participants must promptly download and install the patch or upgrade. EAS Participants are permitted to test that patch or upgrade to ensure that it does not introduce performance issues, provided that the testing begins promptly and is completed in a timeframe that is consistent with industry best practices. No commenter specifically opposes prompt patching as a security requirement.

Use of a Firewall or Comparable Network Segmentation. We require EAS Participants to use a network firewall or comparable network segmentation practices to limit remote management access to authorized devices and authorized users, which will secure EAS and other vulnerable equipment on a private network inaccessible to the public internet. This requirement addresses a widespread EAS vulnerability. In response to the *Alerting Security NPRM,* REC Networks identified 730 EAS Participant servers through which the password screen for Sage Alerting Systems' ENDEC EAS device was directly exposed. Of those servers, 288 operated on port 80, which is the default port for HTTP web services. In contrast with the servers operating on port 80, web services that use the more secure transport layer security (HTTPS) use port 443. It is thus easy and cheap for even low-capability malicious actors to locate EAS Participant equipment. To comply with the requirement we adopt today, EAS Participants must ensure that their EAS equipment is secured behind a firewall or other segmentation mechanism—such as a dedicated Virtual Local Area Network (VLAN), demilitarized zone, or physically isolated management network—with access restricted to only those internal systems and ports necessary for EAS operations. EAS Participants must either deploy a hardware or software firewall with appropriate filters, reconfigure existing routers to block inbound public internet connectivity to EAS devices, or otherwise isolate EAS equipment from general-purpose business networks so that unauthorized external access is not possible. These measures constitute essential, straightforward safeguards that EAS Participants of all sizes can realistically implement. As with the other two requirements we impose, this network segmentation requirement is consistent with established cybersecurity best practices. For example, CISA CPG 3.S calls on companies to ''Secure Internet Facing Devices'' by ''[m]inimiz[ing] internet-facing assets whenever possible'' to address the risk that ''[a]dversaries might exploit weaknesses in internet-facing hosts or systems to gain initial network access, targeting software bugs, temporary glitches, or misconfigurations,'' and CISA CPG 3.I recommends that networks should be logically segmented. No commenter specifically opposes network segmentation as a security requirement.

Based on commenters' assertions that EAS Participants already implement cybersecurity risk management plans, we suspect that many EAS Participants already implement the baseline cybersecurity requirements we adopt today. But EAS is only as secure as its weakest link. Not only does the hack of even a single EAS Participant's systems potentially expose that entity's audience to false information about an emergency, but also the architecture of legacy EAS means that certain types of EAS Participants could pass a false alert along to other EAS Participants. As DAS explains, ''Commission rules can help ensure consistent implementation [of security requirements] across thousands of EAS Participants, preventing weakest-link vulnerabilities.'' As REC Networks notes, small broadcasters are especially likely not to have implemented basic cybersecurity practices, and would benefit from straightforward and easily implemented rules rather than ''an extensive and elaborate cybersecurity plan'' requirement, as proposed in the *Alerting Security NPRM.* We accordingly find that the requirements we adopt today are particularly important to protect EAS Participants that are small- and medium-sized businesses. We therefore reject comments that suggest smaller EAS Participants should be exempt from cybersecurity requirements. Native Public Media and other commenters state that small stations typically lack the budget, resources, and expertise to manage IT security responsibilities, noting that many EAS Participants are very small, and are often nonprofit or municipal operations with minimal funding. But that concern cuts both ways. Smaller broadcasters with fewer security protections in place are often a more attractive target for bad actors, as the recent attacks on small radio broadcasters demonstrate. Moreover, while having limited resources might have made it burdensome to adopt the far-reaching cybersecurity risk management requirements imposed in the *Alerting Security NPRM,* the minimal requirements we adopt today will be far easier and less resource-intensive to implement. We further disagree with Cox Media Group and NAB that the Commission should focus on education of EAS Participants to secure the nation's public alert and warning capability. While we recognize the value of education, we find that it is not sufficient, on its own, to effectively reduce the dynamic and evolving risks posed by cybersecurity threats to emergency alert systems. We conclude that all EAS Participants can and must implement the cybersecurity safeguards we adopt today.

While we appreciate DAS's view that EAS equipment manufacturers should be expected to implement security

practices in their equipment, including by following secure coding practices, providing digitally signed software and firmware updates, shipping devices with hardened default settings, and supporting role-based access controls, we find that the primary responsibility for securing vulnerable equipment rests with EAS Participants themselves. The vulnerabilities identified in the record stem mainly from insecure password practices, unpatched EAS participant-managed systems, inadequate network segmentation, or exposure of devices to the open internet—not from defects in underlying equipment design and development. This approach to responsibility for EAS security delineates clear roles. Manufacturers develop, validate, and make available security patches. EAS Participants, in turn, are responsible for applying patches to their equipment, and ensuring their systems are updated.

We disagree with NAB that, rather than imposing uniform requirements for EAS Participants to secure their systems, the Commission should engage in targeted outreach to those EAS Participants found to be using outdated software or unsupported equipment. We similarly disagree with security researcher Shawn Merdinger, who suggests that ''[w]hat is needed is direct outreach . . . . Someone at the FCC who identifies the EAS device . . . , finds out who the asset owner is, and reaches out to the person running, or in charge of running, that EAS device.'' We recognize the value of outreach to EAS Participants to identify ways to better secure their systems, and take a variety of actions to promote public-private partnership and voluntary efforts to protect networks and EAS from cybersecurity threats. These include releasing Public Notices warning about recent threat vectors and providing guidance about how EAS Participants can better secure their equipment against such threats; hosting workshops that raise situational awareness of the threat landscape and share best practices for protecting communications networks and incident response; and investigating reports about false EAS alerts that suggest the breach of an EAS device or willful misuse of the EAS tones or Attention Signal. Despite these efforts, cyberattacks on EAS Participant facilities continue to occur with disturbing frequency. It is neither practical, administratively efficient, nor a reasonable use of public funds, for the Commission to respond to these threats by assessing the security status of equipment operated by thousands of EAS Participants across the United States and working with each such participant individually to implement the cybersecurity practices that we have been urging them to adopt for years. Moreover, there is no guarantee that the Commission will be able to identify every EAS Participant whose systems may be vulnerable because of flawed passwords, patching, or network segmentation practices. The far more efficient approach is to impose a minimally burdensome requirement on each EAS Participant to implement the basic security requirements we adopt today for its own equipment.

We also disagree with commenters like NCTA that recommend the Commission first focus on modernizing EAS technology prior to considering any additional or updated cybersecurity or resiliency requirements. Maintaining strong passwords, routinely installing security upgrades, and segmenting sensitive equipment from the public internet are vital to preventing unauthorized access to EAS encoding and decoding functions and unauthorized transmission of EAS header tones and audio messages, irrespective of where in the EAS Participant's signal processing system those functions and transmission may be activated. We decline to wait additional months to secure these systems against cybersecurity vulnerabilities that are actively being exploited.

We do not apply the targeted cybersecurity requirements we adopt today to WEA at this time. As discussed above, there is a long history of attackers exploiting vulnerabilities in EAS Participants that have resulted in false EAS alerts reaching the public. While a 2016 report on WEA's security found risks of blocking valid WEA messages, changing the content of a valid WEA message, injecting false WEA alerts into operator equipment, and sending false alerts from false base stations, there have been no reported instances of those kinds of attacks on WEA being successful. We find this to be evidence, as CTIA and ATIS assert, that additional security requirements are not needed at this time. Consistent with the overarching recommendation of CSRIC V, we find that that best practices, rather than requirements, are currently suitable for addressing cybersecurity threats to WEA. Three alerting authorities and two individuals generally support improvements to WEA's cybersecurity posture, but focus on end-to-end cryptographic authentication, auditing, and other more burdensome security measures. None of these commenters adequately explain how the security benefits of additional WEA requirements would outweigh the costs, particularly when the lack of successful attacks on WEA suggests that the benefits of adding security measures for WEA may currently be limited.

Compliance Timeframe

We adopt a compliance timeframe for the rule changes adopted in this Order of 60 days after the rule's publication in the **Federal Register**, balancing the need to quickly secure vulnerable equipment against known vulnerabilities with the time EAS Participants require to implement the security controls. We find that sixty days provides sufficient time for compliance with these changes. Many EAS Participants and their representative organizations state that EAS Participants have already implemented cybersecurity risk management plans that include these specific security measures, and the Commission and FEMA have repeatedly raised the security of EAS as an urgent priority. EAS Participants that have not already implemented these basic cybersecurity hygiene measures will need only make a handful of straightforward changes to certain equipment to comply with these requirements. Minimal time is required, for instance, to log into the equipment subject to these requirements—which, for many EAS Participants is likely to comprise only a few devices—and change the passwords. Indeed, most Americans routinely manage passwords to a variety of devices and applications as a matter of course, which consumes no more than a few minutes each week. Similarly, it will take little time for most EAS Participants to test and install any currently available patches and updates for equipment subject to the requirement. As DAS explains, installing patches and updating equipment to the latest software version is minimally burdensome, because over-the-air software updates and software patching are both feasible and supported by modern, internet-connected EAS equipment. Here, too, the burden is no greater than that experienced by many Americans who routinely install security-related updates to their device operating systems and applications on a regular basis. While installing a firewall may require some EAS Participants to identify a vendor who can configure their systems appropriately, we do not expect that this will be burdensome or time-consuming for EAS Participants to identify because firewalls are widely recognized as a basic and cost-effective cybersecurity safeguard appropriate even for organizations with limited resources.

Further, there is an urgency to protect against threats from malicious actors by implementing these security measures as soon as practicable. Cyber threats that we warned EAS Participants about several years ago continue today. At the same time, cyber threat activities are becoming more sophisticated. For example, CISA recently issued an advisory that warned of ''China-nexus cyber actors . . . using large scale networks of compromised devices (covert networks) to route their cyber activity.'' Given the apparent inadequacy of voluntary approaches to implementing basic security safeguards to remediate these threats—and the significant risk posed by a false alert or non-transmission of a real alert—we find that each of the three requirements we adopt today are reasonable and necessary to protect the security and integrity of EAS.

Benefits and Costs

We find that the targeted rules adopted today will promote EAS security without imposing substantial costs on EAS Participants. These measures are necessary to protect EAS from future false alerts that are damaging to public safety. Improved EAS security will also provide benefits to EAS Participants in the form of avoided reputational harm that may arise from cyberattacks and false alerts being transmitted from their stations. While the new rules may require hiring outside contractors in some cases, EAS Participants will have the flexibility to satisfy this requirement in a manner tailored to their particular business needs.

Costs. While commenters, including FEMA, Altice, Gray Television, and Sage, raise concerns about the increased costs and burdens that the proposals in the *Alerting Security NPRM* would place on EAS Participants, the basic cybersecurity hygiene practices we adopt today represent a narrow subset of those proposals, which EAS Participants should be able to implement without significant expenditure. For instance, the American Militia Association states that the Commission's estimated total cost of $11,600 per year is ''grossly understated [as applied to] legal fees to review new rules and reporting requirements, payments to networking professionals and other costs . . . to ensure compliance.'' However, the requirements in this Report and Order are less burdensome than what was proposed in the *Alerting Security NPRM* as they do not include reporting of unauthorized access incidents, nor do they include creating, updating, or annually certifying to having a sufficient cybersecurity risk management plan that covers a broader range of established best practices.

We estimate that the costs of changing and regularly updating default passwords, installing security patches as available, and implementing firewalls or other network segmentation practices will not exceed $26 million. We estimate the total cost of implementing the EAS security measures as follows: 25,800 entities × (10 hours per entity per year) × ($65 mean hourly wage) × (1 + 7% inflation adjustment) × (1 + 46% benefit mark-up) = $26,198,094 total cost per year, rounded to $26 million. According to the Bureau of Labor Statistics, as of December 2025, civilian wages and salaries averaged $33.45/hour and benefits averaged $15.33/hour. Total compensation therefore averaged $33.45 + $15.33 = 48.78. Using these figures, benefits constitute a markup of $15.33/$33.45 = 46%. We therefore mark up wages by 46% to account for benefits. The figure 25,797 includes 21,658 broadcaster stations and 4,139 headends. With two direct broadcast satellite (DBS) providers and one satellite digital audio radio service (SDARS) provider, the total number of providers is 25,800. Based on Commission staff review of the S&P Global Market Intelligence, S&P Capital IQ Pro, U.S. MediaCensus, Operator Subscribers by Geography, there were 4,139 cable headends in the United States. This methodology likely overestimates the number of radio and television broadcasters that participate in the EAS, as some are exempted from the Commission's rules that govern EAS. For example, if a hub station satisfies the EAS requirements, an analog or digital broadcast satellite station that rebroadcasts 100% of the hub station's programming would not be required to comply with the proposed rules. This estimate is adjusted to reflect the requirements adopted today in light of the record. In the *Alerting Security NPRM,* we estimated that EAS Participants would require, on average, 10 hours annually to draft a cybersecurity risk management plan, update the plan, and submit their certification to the Commission, at an overall cost of $21 million. We instead find that 10 hours is a reasonable average burden estimate across all EAS Participants for the three limited requirements that we adopt today. As DAS states, changing default passwords and installing certain security patches can be accomplished in the normal course of business and at little or no additional cost to EAS Participants. Further, NAB points out that many EAS Participants are already taking some or all of the actions adopted in this Report and Order, recommending that ''the FCC should target its efforts at the fairly small number of entities that may lag in updating their equipment or software.'' To the extent that these entities already engage in password security and regular software update practices, we expect that the amount of additional time required to comply with the rules we adopt today would be low. Some EAS Participants may incur costs, however, to implement firewalls or other comparable network segmentation practices to limit remote management access, if they do not already do so. Therefore, we find that the cost estimate we adopt today is very conservative, due to the relatively narrow scope of requirements in this Report and Order, but the benefits will outweigh even this overestimated cost.

Benefits. We find, as suggested in the *Alerting Security NPRM,* that while it is impossible to quantify the precise dollar value of improvements to the public's safety, life, and health, as a general matter, substantial public safety benefits will result from the adoption of robust security requirements for EAS providers, such as the rules adopted today. We agree with the D.C. Homeland Security and Emergency Management Agency that ''[o]ne of the most damaging and dangerous impacts we have [of a cybersecurity incident] is that we don't have the ability to launch Wireless Emergency Alerts or push to EAS.'' The rules we adopt today will help to ensure the security and operability of EAS Participants. Additionally, as the Commission previously found, ''a foreign adversary's access to American communications networks could result in hostile actions to disrupt and surveil our communications networks, impacting our nation's economy generally and online commerce specifically, and result in the breach of confidential data.'' Consistent with the Commission's past analysis, our national gross domestic product (GDP) was over $30 trillion in 2025. As the requirements we adopt today apply narrowly to EAS Participants and their EAS equipment, studio transmitter link equipment, and any other remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming, rather than the more broad proposals we sought comment on in the *Alerting Security NPRM,* if these requirements prevent even a 0.00009% disruption of our economy, that would offset the costs. Likewise, local radio and television broadcasting, a subset of EAS

Participants, supported $1.19 trillion of our GDP in 2025, so preventing the disruption of even 0.0022% would outweigh the costs. As the Commission also noted in the *Alerting Security NPRM,* the cost of malicious cyber activity on the U.S. economy in 2016 was between $57 billion and $109 billion, so reducing this activity (or preventing an expansion of such damage) by even 0.046% (significantly less than the 1% considered in the *Alerting Security NPRM*) would produce benefits that outweigh the costs. We find that our reasoning in the *Alerting Security NPRM* remains applicable to the rules we adopt today, notwithstanding their narrowed scope, because the security measures we adopt today will significantly harden EAS Participants' systems against these types of attack and mitigate the risk of occurrence. Thus, we conclude that the minor costs associated with implementing the targeted security requirements in this Report and Order will be more than offset by its public safety and economic benefits.

Terminating the 2022 Alerting Security NPRM

We believe that the most effective and proportionate path to mitigating threats against EAS Participants and Participating CMS Providers is to address specific, repeatedly exploited cybersecurity vulnerabilities rather than adopting the broader cybersecurity risk management framework proposed in the *Alerting Security NPRM.* We agree with Nexstar Media that the cyber incidents this Report and Order is intended to prevent could have been easily avoided by undertaking basic network security measures such as those we require today. After further consideration, we conclude that adopting wide-ranging cybersecurity risk management requirements that apply to all of an EAS Participant or Participating CMS Provider's systems and services would impose extremely high costs that outweigh the security benefits.

NPR highlights the high costs of the Commission's proposals by pointing out that the *Alerting Security NPRM*'s estimate is ''off by a factor of 10 or more—it would take a local General Manager or Operations Manager many hours just to understand the baseline framework involved, not to mention developing and implementing a cybersecurity risk plan.'' On further consideration, we conclude that costs to EAS Participants and Participating CMS Providers would include not only the creation of a cybersecurity risk management plan, but also the implementation of that plan, which the Commission failed to take into account in designing its proposal. Based on additional evidence and additional consideration, we agree with the view that ''compliance with the FCC's proposals in the Notice could easily run into the thousands of dollars, directly impacting a station's bottom line.'' These costs would be particularly high for small broadcasters. In light of these costs, we disagree with the Center for Internet Security's view that requiring alerting participants to implement a cybersecurity framework, such as their Critical Security Controls, is appropriate because those requirements would be ''narrowly tailored'' or ''minimally intrusive.'' On balance, we find that addressing the most immediate threats to EAS Participants by adopting narrowly targeted security requirements to be more cost-effective than adopting the Commission's broad and burdensome proposal.

We decline to adopt a rule at this time that would require Participating CMS Providers to take further action to prevent false alerts from fake base stations. No commenter to the *Alerting Security NPRM* supported the Commission's adoption of rules to address this risk. To the contrary, AT&T and CTIA state that the ongoing international standard process is best positioned to address this issue, and ATIS questions whether such an attack on WEA would have a realistic chance of success. We acknowledge that the 3GPP SA3 (Security) working group published a study in 2023 on 5G security enhancements against false base stations, which identifies key issues and multiple candidate solutions. We encourage the 3GPP security working group to continue this work to move from candidate solutions to implementable best practice recommendations.

We decline at this time to make changes to the rules that allow for continued operations for a period of 60 days despite having defective equipment that precludes their participation in EAS. The Commission did not receive a sufficient record on this issue in response to the *Alerting Security NPRM* and several commenters were opposed to elimination of the 60-day rule arguing that the 60-day timeframe is necessary to complete repairs on EAS equipment. We note that our proposal in the accompanying Further Notice to allow EAS Participants to use software to fulfill their EAS obligations could have implications for the ability to receive timely repair and replacement of defective EAS equipment, and we seek comment on this issue below.

We also decline to adopt the Commission's proposal that EAS Participants and Participating CMS Providers report any substantial incident of unauthorized access of their systems to the Commission. We agree with commenters that adopting additional cybersecurity incident reporting requirements for alerting participants would be premature in light of CISA's pending rulemaking implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Rather than adopting potentially duplicative incident requirements, we will continue to monitor CISA's work.

We decline to remove language from Sections 10.330 and 10.500 of the Commission's rules that provide that WEA functionality, both in Participating CMS Providers' networks and in mobile devices, ''are dependent upon the capabilities of the delivery technologies implemented by a Participating CMS Provider'' and certain WEA protocols ''are defined and controlled by each Participating CMS Provider.'' The Commission proposed these changes because it was concerned that the rules might ''create the mistaken impression that Participating CMS Providers' compliance with the rules . . . , would be conditioned on the Participating CMS Providers' delivery technology.'' CTIA opposes changing Section 10.330 because ''it provides CMSPs the necessary flexibility to develop and deploy network technologies driven by consumer demand'' and FEMA opposes changing it because they wanted to preserve Participating CMS Providers' flexibility to use technologies other than cell broadcast to support WEA. No commenter supported the elimination of this language, nor have we observed any non-compliance with the WEA rules attributable to the flexibility this rule provides. For these reasons, we decline to remove the language in question at this time.

The actions we take today are consistent with the approach to cybersecurity that we described in the 2025 CALEA Order on Reconsideration. The Commission continues to pursue targeted, legally robust regulatory and enforcement measures alongside a collaborative approach that emphasizes public-private partnerships that protect and secure communications networks. For instance, the Commission hosted cybersecurity workshops for broadcasters and telecommunications companies in May 2026 that brought together public- and private-sector representatives to raise awareness of emerging cybersecurity risks, share and promote adoption of best practices, and

highlight opportunities for public-private partnership on cybersecurity issues facing communications providers. Unlike the one-size-fits-all proposals in the *Alerting Security NPRM,* our flexible and coordinated approach is proven to make networks more secure. For these reasons, we terminate PS Docket No. 22–329.

Final Regulatory Flexibility Analysis

As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Modernization of the Nation's Alerting Systems Notice of Proposed Rulemaking* (*Alerting Modernization NPRM*), released in August 2025, and the *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats* (*Alerting Security NPRM*), released October 2022. The Commission sought written public comment on the proposals in the NPRMs, including comment on the IRFA. The comments received are addressed below.

Need for, and Objectives of, the Rules. The Report and Order adopts targeted measures to enhance Emergency Alert System (EAS) security that address the public safety risks arising from breaches of EAS equipment that can result in false alerts or hijacked broadcasts. The Commission requires EAS Participants to do the following with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming: (1) prior to operation, change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised; (2) test and install security patches, security-related software and firmware upgrades issued by equipment manufacturers promptly after those patches or upgrades become available; and (3) use a network firewall or comparable network segmentation practice to limit remote management access to authorized devices and authorized users. These rules support the Commission's goals of strengthening the security of alerting systems to ensure these systems are designed to be secure from attacks by foreign adversaries and other malicious actors. When criminals can gain access to these systems, they can cause alarm by sending out false alerts that cause public panic or deliver false information about crises and disasters. This unauthorized access can also prevent real alerts from being transmitted. The Commission has observed attacks in recent months where threat actors exploited improperly secured, remotely accessible equipment in broadcasters' signal processing systems to gain control of station transmissions and insert unauthorized audio that included EAS tones, offensive language, and promotional content.

Summary of Significant Issues Raised by Public Comments in Response to the IRFA. In 2022, the Commission released the *Alerting Security NPRM* seeking comment on ways to strengthen the operational readiness of EAS equipment. The *Alerting Security NPRM* proposed requiring EAS Participants to report compromises of their EAS equipment, communications systems, and services to the Commission, and also proposed requiring EAS Participants and Commercial Mobile Service providers that participate in Wireless Emergency Alerts (WEA) (Participating CMS Providers) to annually certify that they have a cybersecurity risk management plan in place, and to employ sufficient security measures to ensure the confidentiality, integrity, and availability of their respective alerting systems. The proposal would have required an annual certification attesting that the EAS Participant has created, updated, and implemented a cybersecurity risk management plan that includes security controls sufficient to ensure the confidentiality, integrity and availability of the EAS through the following best practices: (1) changing default passwords prior to operation; (2) installing security updates in a timely manner; (3) securing equipment behind properly configured firewalls or using other segmentation practices; (4) requiring multifactor authentication where applicable; (5) addressing the replacement of end-of-life equipment; and (6) wiping, clearing, or encrypting user information before disposing of old devices. It also proposed requiring Participating CMS Providers take steps to ensure that only valid alerts are being displayed on consumer devices.

Several commenters raise concerns about the burdens associated with these specific proposals. In the record of this proceeding, Prometheus Radio Project (Prometheus), NPR, and REC Networks comment on the impact of the proposed rules on small entities. Prometheus comments that it supports cybersecurity best practices for all broadcasters, but notes that compliance will be ''onerous for small, rural and LPFM broadcasters, most of whom lack in-house technical expertise and will have to shoulder significant additional financial burden.'' Prometheus also states that the Commission ''must take a more nuanced approach to ensuring the security of EAS equipment, by providing cybersecurity assistance to EAS Participants directly and by placing compliance burden on EAS equipment manufacturers when technically feasible.'' Prometheus agrees, however, with the Commission's ''initiative to strengthen security practices and EAS and supports the implementation of cybersecurity practices for all broadcasters, big and small.'' NPR agrees that there should be ''secure, reliable communications during emergencies without relying on the internet, which may be offline or become unreliable, particularly during power outages'' but raises concerns ''that some of the proposed rules would create costly obligations for stations without clear public benefits [and] [s]ome of the proposed rules would be especially burdensome for noncommercial public radio stations—stations that already provide consistent and trusted emergency alerting service despite significant staffing and monetary constraints.'' REC Networks similarly states ''that security of EAS equipment is of paramount importance'' but emphasizes the limited resources of '' 'small stations' [ ] normally operated by small nonprofit organizations, minority groups, 'mom and pop' and individual owners with limited budgets and very limited information technology resources.'' REC Networks states that they ''will oppose the 'one size fits all' approach to information security as proposed by the Commission including any requirements that involve the immediate reporting of any security breaches . . . as well as the requirements to develop, update and maintain complex extensive cyber-security risk management policies as they would be applied to small stations.'' Finally, DAS notes in its reply comments that while sometimes equipment manufacturers provide firmware and software updates ''sometimes at no cost or sometimes with a charge,'' others in the record accurately note that ''(e)ven small operators should consider these [firmware and software] updates to be the normal cost of doing business.''

In response to the *Alerting Modernization NPRM,* DAS expresses concerns that ''large operators may move ahead quickly, but small-market and rural licensees might find it hard to keep up'' and urges a ''comprehensive cost-benefit and small-entity impact

assessment before final rule adoption.'' The Competitive Carriers Association comments that there needs to be ''relief and/or reduction of the cadence of imposition of new regulatory requirements related to public safety'' and that small providers are at risk of a disadvantage in sales because ''smaller carriers would likely lose customers to larger providers that offer [alerting] but with potentially less coverage and quality of service in rural and remote areas.''

We are persuaded by these views. We agree that the practices proposed in the *Alerting Security NPRM* are overly burdensome, especially for smaller providers. As such, we adopt a very narrowly tailored subset of these proposals. These requirements have been streamlined with smaller providers in mind and are adaptable for various providers, regardless of size.

Response to Comments by the Chief Counsel for the Small Business Administration Office of Advocacy. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and provide a detailed statement of any change made to the proposed rules as a result of those comments. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

Description and Estimate of the Number of Small Entities to Which the Rules Will Apply. The rules we adopt in the Report and Order will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Where available, we also provide additional information regarding the number of potentially affected entities in the identified industries below.

TABLE 1—2022 U.S. CENSUS BUREAU DATA BY NAICS CODE

Regulated industry (footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS code	SBA size standard	Total firms	Total small firms	Percent small firms
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing.	334220	1,250 employees	155	136	87.74
Communications Equipment Manufacturing	334290	800 employees	310	294	94.84
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23
Radio Broadcasting Stations	516110	$47 million	2,616	2,136	81.65
Television Broadcasting Stations	516120	$47 million	413	316	76.51
Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content Providers.	516210	$47 million	5,217	3,673	70.40
Wired Telecommunications Carriers	517111	1,500 employees	3,403	3,027	88.95
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30
Satellite Telecommunications	517410	$44 million	332	195	58.73

TABLE 2—TELECOMMUNICATIONS SERVICE PROVIDER DATA

2024 Universal service monitoring report telecommunications service provider data (data as of December 2023)	SBA size standard (1,500 employees)		
Affected entity	Total number FCC Form 499A filers	Small firms	Percent small entities
Wired Telecommunications Carriers	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)	585	498	85.13

TABLE 3—BROADCAST ENTITY DATA

Broadcast station owners (as of August 8, 2025)	SBA size standard ($47 million)		
Affected entity	Number commercial licensed	Small firms	Percent small entities
Radio Stations (AM & FM) Groups	2,881	2,863	99.38
Television Stations	171	142	83.04

TABLE 4—CABLE ENTITIES DATA

Cable entities	Size standard	Total firms	Small firms	Percent small firms in industry
Cable System Operators (Telecom Act Standard) Small Cable Operator.	Serves fewer than 498,000 subscribers, either directly or through affiliates.	530	524	98.87

Description of Economic Impact and Projected Reporting, Recordkeeping and Other Compliance Requirements for Small Entities. The RFA directs agencies to describe the economic impact of adopted rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.

The rules we adopt in today's Report and Order affect small entities that are EAS Participants, but also reflect a preference for narrowly tailored, specific security controls that are less burdensome on small entities by adopting only a segment of the most crucial cybersecurity hygiene practices. Additionally, the requirements we adopt today provide sufficient flexibility for providers to adopt these rules, whether they are large or small. These rules focus on enhancing protections and securing systems against threats but are not one-size-fits-all. EAS Participants have the flexibility to satisfy these requirements in a manner tailored to their particular business needs, which will differ depending on business size, the geographic area served, etc. Further, the rules we adopt today follow Altice USA's recommendation that these ''rules allow the greatest possible flexibility in cybersecurity policies and practices so that Participants can tailor them to the unique needs of their networks.'' While these requirements share the common goal of protecting EAS systems from malicious actors, there are multiple avenues to do so for any variant of provider resources.

The rules do not contain any new reporting or recordkeeping requirements. While we cannot conclusively determine whether the rules we adopt in the Report and Order will require small entities to hire professionals to assist with compliance, we find that the requirements in the Report and Order will promote public safety and alerting system security without imposing substantial costs on small and other entities. We estimate that the costs per entity of changing and regular updating default passwords, installing security patches as available, and implementing firewalls or other network segmentation practices will not exceed $1,000 annually, based on 10 hours of labor per entity per year. We expect this cost to be lower for those entities, including small entities, that already engage in password security and regular software update practices, for example, and small entities will have the flexibility to implement firewalls or other network segmentation practices to limit remote management access in the ways that best suit their particular business needs.

Discussion of Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered. The RFA requires an agency to provide ''a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.''

Through its review of the record in the *Alerting Security NPRM* proceeding, the Commission has sought to minimize significant economic impact on small entities and, in doing so, has considered alternatives to the rules we adopt today. The rules we adopt are a limited set of those proposed in the *Alerting Security NPRM.* We have declined to adopt several expansive cybersecurity requirements, including the requirement that providers annually certify the creation, updating, and implementation of a cybersecurity risk management plan. Instead, the rules we adopt are narrowly tailored to address threats for which small entities are particularly at risk. The requirements we adopt in the Report and Order provide sufficient flexibility to account for diverse operational environments, regardless of provider size, capabilities, and resources. We mandate steps to better secure EAS Participant systems and defend against threats to cybersecurity without strict, specific requirements that box providers into particular price points, or rigid restrictions that force them to choose between safety and spending beyond their means. Compliance with these rules should be attainable for all entities, including small entities that may be financially or resource-constrained. Further, the scope of these rules has been narrowed from any EAS Participant systems and services that could potentially affect the provision of the EAS to more specific types of equipment that are most vulnerable. We have made it our focus to advance cybersecurity protections and minimize threats without forcing costly system redesigns or adopting overly complex compliance plan requirements.

Report to Congress

The Commission will send a copy of the Report and Order, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the Report and Order, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for the SBA Office of Advocacy and will publish a copy of the Report and Order, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the **Federal Register**.

Ordering Clauses

Accordingly, *it is ordered,* pursuant to Sections 1, 2, 4(i), 4(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 624(g), 706, and 713 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 544(g), 606, and 613, as well as by sections 602(a), (b), (c), (f), 603, 604, and 606 of the WARN Act, 47 U.S.C. 1201 (a), (b), (c), (f), 1203, 1204 and 1206, and the National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283, 134 Stat. 3388, 9201, 47 U.S.C. 1201, 1206, that this Report and Order and Further Notice of Proposed Rulemaking *is adopted.*

It is further ordered that the Commission's rules *are hereby amended* as set forth in Appendix A and such amendments shall become effective 60 days after publication in the **Federal Register**.

It is further ordered that, should no petitions for reconsideration or petitions for judicial review be timely filed, PS Docket No. 22–329 *shall be terminated,* and the docket will be closed.

It is further ordered that the Commission's Office of the Secretary, *shall send* a copy of this Report and Order, including the Final Regulatory Flexibility Analyses, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

It is further ordered that the Office of Managing Director, Performance Program Management, *shall send* a copy of this Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, 5 U.S.C. 801(a)(1)(A).

List of Subjects in 47 CFR Part 11

Radio, Television

Federal Communications Commission.

Marlene Dortch,

Secretary, Office of the Secretary.

Final Rules

For the reasons set forth above, the Federal Communications Commission amends 47 CFR part 11 as follows:

PART 11—EMERGENCY ALERT SYSTEM (EAS)

■ 1. The authority citation for part 11 continues to read as follows:

Authority: 47 U.S.C. 151, 154 (i) and (n), 303(r), 544(g), 606, 1201, and 1206.

■ 2. Amend § 11.35 by adding paragraph (d) to read as follows:

§ 11.35 Equipment operational readiness.

* * * * *

(d) EAS Participants shall employ the following security controls with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the transmission of the EAS Participant's programming:

(1) Prior to any use to broadcast to the public, EAS Participants shall change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised.

(i) A strong password is any password that has a minimum of 15 characters and does not use dictionary words. Instead of using a strong password, EAS Participants may use alternative authentication measures, such as look-up secrets, out-of-band devices, single- or multi-factor one-time password devices, or single- or multi-factor cryptographic authentication, that are reasonably sufficient to mitigate the risk of unauthorized access.

(ii) Passwords employed to comply with this requirement shall not be reused for the EAS Participant's other accounts, equipment, applications, or services.

(2) Install security patches and security-related software and firmware updates issued by equipment manufacturers promptly after those patches or upgrades become available. Security patches and security-related software and firmware updates issued by equipment manufacturers may be tested before they are installed, provided that the testing begins promptly and is completed in a timeframe that is consistent with industry best practices; and

(3) Use a network firewall or comparable network segmentation practice that limits remote management access to authorized devices and authorized users.

[FR Doc. 2026–15601 Filed 7–30–26; 8:45 am]

BILLING CODE 6712–01–P

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

49 CFR Part 192

[Docket No. PHMSA–2026–1522]

RIN 2137–AG26

Pipeline Safety: Standards Update—NFPA 58

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Transportation (DOT).

ACTION: Direct final rule (DFR); confirmation of effective date.

SUMMARY: PHMSA is confirming the effective date for a DFR published in the **Federal Register** on April 24, 2026. The DFR amended PHMSA's regulations at 49 CFR part 192 to incorporate by reference the updated industry standard NFPA 58, Liquefied Petroleum Gas Code (NFPA 58).

DATES: The effective date of the DFR is January 1, 2027.

FOR FURTHER INFORMATION CONTACT: Brianna Wilson, Transportation Specialist, by phone at 771–215–0969 or by email at *brianna.wilson@dot.gov.*

SUPPLEMENTARY INFORMATION: On April 24, 2026, PHMSA published a DFR titled ''Pipeline Safety: Standards Update—NFPA 58'' (91 FR 21986). The DFR amended regulations at 49 CFR part 192 to incorporate the 2024 edition of NFPA 58, Liquefied Petroleum Gas Code (NFPA 58) by reference. Reference to the 2024 edition of NFPA 58 will replace the existing reference within 49 CFR 192.11 to NFPA, Liquefied Petroleum Gas Code, 2020 edition, effective August 25, 2019.

PHMSA issued the DFR under the procedures set forth at 49 CFR 190.339. In accordance with those procedures, PHMSA stated in the DFR that if no adverse comments were received, the DFR would become effective on January 1, 2027. PHMSA did not receive any comments that warranted withdrawal of the DFR; therefore, this rule will become effective as scheduled.

Issued in Washington, DC under authority delegated in 49 CFR 1.97.

Keith J. Coyle,

Chief Counsel.

[FR Doc. 2026–15571 Filed 7–30–26; 8:45 am]

BILLING CODE 4910–60–P

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

49 CFR Part 192

[Docket No. PHMSA–2026–1524]

RIN 2137–AG28

Pipeline Safety: Standards Update—ASTM A372/A372M

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA), Department of Transportation (DOT).

ACTION: Direct final rule (DFR); confirmation of effective date.

SUMMARY: PHMSA is confirming the effective date for a DFR published in the **Federal Register** on April 24, 2026. The DFR amended PHMSA's regulations at 49 CFR part 192 to incorporate by reference the updated industry standard ASTM A372/A372M, Standard Specification for Carbon and Alloy Steel Forgings for Thin-Walled Pressure Vessels (ASTM A372/A372M).

DATES: The effective date of the DFR is January 1, 2027.

FOR FURTHER INFORMATION CONTACT: Brianna Wilson, Transportation Specialist, by phone at 771–215–0969 or by email at *brianna.wilson@dot.gov.*

SUPPLEMENTARY INFORMATION: On April 24, 2026, PHMSA published a DFR titled ''Pipeline Safety: Standards Update—ASTM A372/A372M'' (91 FR 22008). The DFR amended regulations at 49 CFR part 192 to incorporate the reapproved 2025 edition of ASTM A372/A372M, Standard Specification for Carbon and Alloy Steel Forgings for Thin-Walled Pressure Vessels (ASTM A372/A372M) by reference. Reference to the reapproved 2025 edition of ASTM A372/A372M will replace existing references within § 192.177 to ASTM A372/A372M–20e1, Standard Specification for Carbon and Alloy Steel Forgings for Thin-Walled Pressure Vessels, approved March 1, 2020.

PHMSA issued the DFR under the procedures set forth at 49 CFR 190.339. In accordance with those procedures, PHMSA stated in the DFR that if no adverse comments were received, the DFR would become effective on January 1, 2027. PHMSA did not receive any