Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of Part 11 of the Commission’s	)	PS Docket No. 15-94
Rules Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Protecting the Nation’s Communications	)	PS Docket No. 22-329
Systems from Cybersecurity Threats	)	

COMMENTS OF THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

The Alliance for Telecommunications Industry Solutions (ATIS) hereby submits these comments in response to the *Notice of Proposed Rulemaking* (*FNPRM*), released by October 27, 2022, in the above-referenced dockets. In the *NPRM*, the Federal Communications Commission (Commission) seeks input regarding perceived threats to the security of the Wireless Emergency Alert (WEA) System, citing concerns about exploits that may result in panic and endanger the public. ATIS supports a robust and secure WEA system but urges the Commission to undertake an end-to-end evaluation of WEA and to focus on the areas that may potentially pose the greatest threat, where a successful attack would cause the most widespread disruption. ATIS strongly believes that the point of origination of the alert is the largest security vulnerability, as it provides for the greatest reach of any potential exploit. Thus, the Commission should make the origination point the primary focus of this evaluation.

I. Background

ATIS is a global standards development and technical planning organization that develops technical and operational standards for the information and communications technologies (ICT) sector. ATIS' diverse membership includes key stakeholders, including wireless, wireline, and VoIP service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, and internet service providers. ATIS is also a founding partner and the North American Organizational Partner of the Third Generation Partnership Project (3GPP), the global collaborative effort that has developed the 4G Long-Term Evolution (LTE) and 5G New Radio (NR) wireless specifications.

Nearly 600 industry subject matter experts work collaboratively in ATIS' open industry committees. ATIS' Wireless Technologies and Systems Committee (WTSC) develops wireless radio access, system, and network solutions related to wireless and/or mobile services and systems, including WEA. ATIS WTSC continues to enhance solutions necessary to support WEA. These efforts are spearheaded by ATIS' WTSC WEA subcommittee. WTSC WEA is currently considering a feasibility study for WEA enhancements via a data transport path between Alert Originators and a managed App, and is producing a guidance document for the State/Local WEA Test. Recent publications by WTSC WEA include: (1) December 2021 *Wireless Emergency Alert (WEA) 3.0 Operational Considerations for Commercial Mobile Service Providers (CMSPs)* (ATIS-0700050), which provides guidance to CMSPs on operational considerations and details enhancements to the user experience associated with the flexible operational settings allowed by the WEA design; and (2) August 2021 *WEA 3.0 Practical Hints* *for Alert Originators* (ATIS-0700049), which examines the user experience based on the input from the Alert Originator.

II. Comments

A. WEA System: Critical Focal Point for Security

In the *NPRM*, the Commission seeks input regarding perceived threats to the security of the WEA system, with a strong focus toward prevention of the distribution of false information that may result in causing panic and general disruption and danger for the public.[1] ATIS strongly supports a robust and secure WEA system and believes that any efforts should be focused on the point of greatest vulnerability – specifically at the alert origination point.

In the *NPRM*, the Commission notes that some university papers have presented hypothetical scenarios under which false alerts may be sent from false base stations, or the broadcast itself hijacked.[2] The University of Colorado paper entitled "This is Your President Speaking," for example, claims that with only four malicious portable base stations, almost all of a 50,000-seat stadium can be attacked with a 90% success rate.[3] However, in reality such an attack would have little chance of success. As experience demonstrates, cellular deployments in venues of this size (flagship venues) would have, to the best of the carrier's ability, the capacity to provide high-capacity service for all attendees. Carriers typically, at a minimum, would configure cell sites (including macro-cells, as well as temporary capacity enhancements using "Cell on Wheels/Wings/Trucks," small cells, and distributed antenna systems) throughout the

[1] *NPRM* at ¶37.
[2] *NPRM* at ¶8.
[3] Gyuhong Lee, et al., This is Your President Speaking: Spoofing Alerts in 4G-LTE Networks (2019), https://dl.acm.org/doi/pdf/10.1145/3307334.3326082 (using for their research experiment a COTS eNodeB with 0.1 Watt transmission power to send a false alert to Samsung Galaxy S8 and Motorola G6 handsets within a 70 to 120 meter range) ("*University of Colorado Paper*").

venue to provide adequate coverage and capacity. The number of authentic base stations vying for the user equipment would significantly reduce the ability of false base stations to attract user equipment. Moreover, in order to attack the full capacity of the stadium, the rogue base stations would need to spoof at least three top-tier carriers, not just a single carrier. The potential of the attack is overstated, given its focus on user equipment in the idle state. In reality, a large percentage of user equipment would not be vulnerable because it would be in a connected state for voice calls or video streaming, or regularly transitioning to a connected state for data exchanges (inbound and outbound) for every email, social media interaction, background app, and texting exchange throughout the event. Finally, ATIS notes that the studies fail to consider the mitigating effect of user behavior on the potential attack. As noted by Alert Originators based on studies by the National Academies of Sciences,[4] users will attempt to validate an alert before acting, which further reduces the potential impact of false alerts. Based on these factors, ATIS believes that the chance of successfully exploiting this scenario is extremely small. Even more important is the fact that the potential reach of this type of exploit pales in significance when compared to the possible reach of an exploit from the alert origination point in the WEA chain.

In the *NPRM*, the Commission cites the false Hawaii Missile Alert as an example of the level of public panic that may result from the dissemination of false information.[5] ATIS notes this particular incident was not the result of either a technical or security vulnerability, but of a failure in the alert origination practices for the alerting agency, and it demonstrates areas of possible improvement. The false Hawaii Missile Alert is, however, an excellent example of the

[4] National Academies of Sciences, Engineering, and Medicine. 2018. Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions. Washington, DC: The National Academies Press. https://doi.org/10.17226/24935

[5] *NPRM* at ¶37.

wide reaching, significant public disruption that could happen due to potential vulnerabilities received from an Alert Originator. A malicious alert initiated at an authorized alert origination point would be undetectable during the automated alert processing by any other downstream WEA stakeholder. No additional security measures could be applied by the Federal Emergency Management Agency (FEMA) or the Commercial Mobile Service Providers (CMSPs) to mitigate a malicious alert received from an Alert Originator.

B. Challenges Associated with Modifying Security Protocols

ATIS notes that, following the Hawaii incident, the Commission's Seventh Communications Security, Reliability, and Interoperability Council (CSRIC VII) was tasked with recommending Best Practices for Alert Originators.[6] Among the tasks assigned to CSRIC VII was false alert prevention, which included detection, handling and retraction. Other Best Practices pertain to ensuring an always-ready state with well-maintained, structured and stable communications among the Alert Originator responsible parties, including establishing documented alternate lines of communications to allow for continued efficient operations in the face of unusual or extreme circumstances. Many of these same practices may be applied to improving the security of the WEA system and recovery practices following an unusual incident. Open and ready lines of communication among the Alert Origination stakeholders would allow for quick detection of a malicious WEA followed by cancelation of the WEA and the sending of an update to the public, thereby limiting the extent of the public disruption. ATIS would support an assessment by the Commission of the Best Practices recommended by CSRIC VII on this matter to determine the extent to which these Best Practices have already been applied, and

[6] CSRIC VII Working Group 1: Alert Originator Standard Operating Procedures. This working group report on this matter was published on September 16, 2020. This report is available from the Commission's website at https://www.fcc.gov/file/19311/download.

whether any modifications to the Alert Origination policies and procedures are warranted to address security vulnerabilities more fully.

In ATIS' analysis, it was determined that there is a much lower threat vector associated with the CMSP broadcast of WEA, due not only to the limited reach of a false base station in comparison to the reach of a WEA initiated by an Alert Originator, but also to the strong security already in place in the cellular system. WEA takes advantage of a critical aspect of the cellular system – the Cell Broadcast Service (CBS) – that is inherently designed for security because it provides support for all cellular system operations.

The industry also works to ensure that these critical systems remain secure as technology evolves. 3GPP has a dedicated group to address security – 3GPP SA3-Security and Privacy – that assesses risks and potential threat mitigation techniques and develops, with the appropriate protocols and architecture, specifications for security and privacy within the 3GPP network. Due to this work, each generation of cellular technology, including the recently-deployed 5G network,[7] sees new advances in security.

ATIS notes that 3GPP SA3 has already analyzed Public Warning System (PWS) security[8] and evaluated the complexities and associated risks of possible solutions against the potential threat and has determined that additional security measures for PWS should not be pursued.[9] Re-evaluating WEA security would require a re-evaluation of PWS security, which in turn would require extensive coordination between ATIS and 3GPP. Any changes would have global ramifications to all stakeholders, including service providers and equipment providers. Any changes to the 3GPP system would also require relevant 3GPP specification development groups

[7] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf.
[8] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2355.
[9] The global Public Warning System (PWS) specification from 3GPP enables the distribution of WEA and other global warning systems.

to explore potential adverse impacts to system functionality and services supported in the 3GPP network. This collaboration and standardization work would be significant, require years of work and would need to be completed before any security changes could be implemented. The expected time frame for all steps, including the initial study and risk analysis, specification work, development, testing, integration testing, and deployment is expected to be a minimum of seven (7) years, followed by several more years for the number of supported devices to reach critical mass. If pursued, the resulting implementation would not apply to legacy devices, and may not be fully applicable to future network generations as the security model continues to evolve.

ATIS also notes that it extensively studied WEA security at the Commission's request, based on the *University of Colorado Paper*. Although ATIS found that this hypothetical exploit – false alerts sent from false base stations – was very unlikely to be successful, ATIS did analyze several potential mitigation techniques to address this hypothetical threat vector. ATIS concluded that no technique could be recommended due to each potential mitigation's limitations and the extremely low threat risk associated with this potential exploit, especially when coupled with the following negative impacts:

- Add complexity to WEA, which may result in potential new failures;
- Increase latency;
- Pose a risk that some users may not receive alerts, impacting reliability;
- Impact a device's battery life;
- Require international standards agreements on methods to be used;
- Jeopardize the receipt of PWS/WEA alerts for international roaming (for both inbound and outbound roamers);
- Require years of standardization, product development, deployment, and testing;
- Complicate operational aspects of mixed generation devices, including any management and distribution of security credentials; and
- Not likely be implementable in legacy devices.

In addition to the above, ATIS found that the techniques would have limited benefit and apply to a very constrained geographic area at any given time.

ATIS notes that FEMA and the CMSPs have optimized the WEA system for performance and have specifically leveraged the CBS for WEA because it offers high reliability while minimizing latency. ATIS, like 3GPP, was unable to identify any unique WEA security mitigation technique that did not pose an unacceptable risk to reliability and latency. Decreased reliability and increased latency would have significant impacts on time-sensitive alerts, such as those from the United Stated Geological Survey (USGS) or those associated with tornado and tsunami warnings from the National Weather Service (NWS). If such messages are delayed by seconds or minutes, or in the worst case, are not received at all, it would no longer be feasible to use WEA to distribute such life-saving alerts.

III. Conclusion and Next Steps

ATIS urges the Commission, in its evaluation of WEA security, to focus on securing the origination point of the alert. ATIS believes that this is the largest security vulnerability and the only one that poses a risk of widescale disruption. ATIS further recommends that the Commission and FEMA focus on: (a) increasing training and education for Alert Originators; (b) developing alert origination policies and procedures to assist in the prevention, handling and retraction of malicious WEAs for minimization of impact to the public; and (c) adding additional checks and balances within the Alert Originators' systems.

ATIS does not believe that any new security requirements are needed to protect against false alerts from false base stations. Evaluations by ATIS and 3GPP have concluded that there is a low risk, and thus limited vulnerability to disruption, associated with such a threat. ATIS has also determined that possible mitigation techniques to address such a false base station scenario would be of limited benefit and would negatively impact latency and reliability of the WEA system, which would affect all alerts, and therefore all alert recipients, nationwide.

Respectfully submitted,

Thomas Goode
General Counsel
Alliance for Telecommunications Industry Solutions
1200 G Street, NW
Suite 500
Washington, D.C. 20005
(202) 628-6380

December 23, 2022