Public Safety Communications

Ten Keys to Improving Emergency Alerts, Warnings & Notifications

April 2019

CISA
CYBER+INFRASTRUCTURE

SAFECOM® NCSWIC®

EXECUTIVE SUMMARY

Emergency alert, warning, and notification (AWN) systems help protect lives and property by identifying information about an impending threat, communicating that information to those who need it, and facilitating the timely taking of protective actions. SAFECOM, the National Council of Statewide Interoperability Coordinators (NCSWIC), and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed these best practices, known as the "Ten Keys," in conjunction with the AWN community as recommendations to help organizations enhance critical information sharing. Alert originators (AOs), partners, and stakeholders should work together to implement these best practices into existing AWN structures:

- **Establish Governance:** Establish strong governance and collaborate with existing authorities to create communication pathways to facilitate timely and efficient information sharing
- **Identify and Coordinate with Others:** Partner and coordinate with existing AOs, emergency managers, organizations within a jurisdiction and neighboring jurisdictions, public safety communications centers and answering points, public information officers, critical infrastructure sectors, community members and organizations, and communications providers
- **Develop Plans, Policies and Procedures:** Identify, establish, document, field-test, and continually evaluate plans, policies, and procedures against the evolving AWN landscape
- **Account for Diverse Populations:** Ensure whole community inclusion, as diversity and accessibility influence the ways in which people receive, interpret, and respond to messages. Understanding how messages reach these various demographics and using a variety of communications pathways is necessary for ensuring AWN effectiveness
- **Maintain Security and Resiliency:** Ensure cybersecurity across networks, devices, systems, and user interfaces. Secure infrastructure and foster resiliency as manmade and natural disasters can impact AWN issuances if not properly mitigated
- **Incorporate Safeguards:** Incorporate internal safeguards, across the entire AWN lifecycle—human and machine—to protect against system misuse and prevent false messaging
- **Train, Exercise and Test Systems:** Conduct trainings, exercises, and tests of AWN systems with stakeholders and partners on a regular basis to maintain proficiencies; lessons observed from these activities should be evaluated, documented, and incorporated into future operations
- **Eliminate Issuance and Dissemination Delays:** Eliminate issuance and dissemination delays by creating message templates, expediting information sharing, identifying and establishing triggers, and avoiding ad-hoc decision making
- **Deliver Actionable Messaging:** Provide comprehensive, targeted, and specific messaging. Remain mindful of creating alert fatigue, but err on the side of public safety when dealing with conflicting or uncertain information
- **Monitor and Correct Misinformation:** Monitor for changes in the situation and inaccurate spreading of information, and correct inaccurate or false messaging accordingly

AOs, managers, system administrators, system operators, and emergency managers across all agencies and organizations (including non-government) tasked with the implementation of AWN systems will benefit from the review of these "Ten Keys." Though this document does not contain specific requirements for AWN system design, maintenance, operating procedures, or governance considerations, it does contain numerous references from throughout the AWN community on how to enhance critical information sharing through accurate, timely, secure and inclusive messaging.

TABLE OF CONTENTS

ALERTS, WARNINGS & NOTIFICATIONS

AOs issue AWNs to provide potential threat and safety-related information to advise and protect the public.[1] AWNs allow the public to make informed decisions to save lives and help mitigate property loss, effectively reducing disaster impacts and speeding community recovery efforts.[2] For the purpose of this document, "AOs" include any individual or organization issuing AWNs to protect the public.

Federal, state, local, tribal, and territorial (SLTT) AOs may also be authorized to access national-level systems in disseminating AWNs, including those administered by the National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS), the Emergency Alert System (EAS), and Wireless Emergency Alerts (WEA). These authorized AOs are known as "alerting authorities." The Integrated Public Alert and Warning System (IPAWS), managed by the Federal Emergency Management Agency (FEMA), receives AWNs from participating AOs and authenticates them through its Open Platform for Emergency Networks (OPEN). Afterwards, the different national-level systems disseminate the validated AWNs.

In addition to these systems, many states, regions, or local jurisdictions have their own AWN systems. Other localized AWN systems include siren warning systems, hazard warning systems, digital signage, and reverse 911 systems. Private companies and social media platforms provide another layer of structure within this ecosystem.

Public safety officials at any level of government may issue emergency AWNs to the public prior to, during, or after incidents. As Table 1 illustrates, these communications serve different purposes.

Type	Timeframe	Purpose	Examples
Warnings	Prior to incident	Distribute guidance to prepare for an anticipated incident	Weather watches/warnings, fire warnings, volcano warnings, evacuation orders
Alerts	At the beginning of and during incident with an ongoing immediate threat	Gain the attention of the public and draw their attention to a risk or hazard	Active shooter and other civil dangers, hazmat concerns, 911 outage, AMBER alerts
Notifications	During and after immediate threats	Instruct immediate protective actions and provide ongoing communications relevant to an incident to reduce milling and encourage public action. Convey time-sensitive information on response and recovery-related services	Protective actions, evacuation routes, boil water, return from evacuation notices, area accessibility updates, all-clear notices

Table 1. Warnings, Alerts, and Notifications Prior to, During, and After an Incident

Prior to an incident or during an ongoing immediate threat, communications would typically provide information regarding the source, threat, location, guidance/timeframe, and expiration time.[3] As the incident stabilizes, and immediate threats are contained, additional messages may focus upon recovery and restoration efforts. The line between AWN types may blur as messages may serve multiple purposes, but the best practices associated with each type of message generally remain the same.

In addition to government sources,[4] AWNs may originate from other non-government or private sources (e.g., AWNs issued by colleges and universities to their employees and students on a campus, or AWNs issued by a company to its employees). Private organizations, mainstream media, social media platforms, grassroots efforts, and individuals are also increasingly contributing to public sector awareness during disasters (e.g., Facebook Crisis Response, Zello, and The Weather Channel).

[1] Department of Homeland Security (DHS), "National Emergency Communications Plan," 2014

[2] DHS Federal Emergency Management Agency (FEMA), "IPAWS Toolkit for Alerting Authorities," n.d.

[3] D. Mileti and J. Sorensen, "A Guide to Public Alerts and Warnings for Dam and Levee Emergencies," *U.S. Army Corps of Engineers Risk Management Center*, June 5, 2015.

[4] This document focuses on government-to-citizen AWNs, government-to-government AWNs also occur as a part of incident response and coordination but are not the primary focus of this paper.

1 Establish Governance

Governance is a framework of processes, organizational rules, communications protocols, and behavioral standards that enable rapid decision making and effective communications. A governing body provides strategic direction and ensures that its stakeholders achieve their objectives, manage risks, and use resources responsibly.[5] As many state and local statutes address who has the authority and responsibility to protect and alert the public, AOs should work to identify existing governance structures, and ensure all governance is accomplished within existing regulatory and legislative guidelines. To establish an oversight body:

- **Engage Stakeholders:** The oversight body should represent the full range of the AWN community (see "Identify and Coordinate with Others" section). Additionally, decision makers—such as interoperability coordinators, AOs, and key executive and legislative leaders—should be solicited and engaged to actively participate in and champion efforts.
- **Encourage Transparency:** Governing body membership, operations, and actions should be clearly articulated and understood. System limitations and progress should be documented and communicated. A governing board should embrace open meetings (e.g., town hall and civic group meetings), and use various information outlets to promote activities and accomplishments to all interested parties.
- **Promote Sustainability:** AWN program management is a long-term and complex technical effort. As such, a governing body should account for succession planning and membership rotation.
- **Establish Authority:** The oversight body should establish voting authority and develop issuance authority procedures.[6]

Refer to Chapter 4 (pp. 23-25) of the DHS Science and Technology Directorate (S&T) First Responders Group's *Best Practices in Wireless Emergency Alerts*[7] publication, as well as SAFECOM's emergency communications governance resources[8] for further guidance on establishing and maintaining effective governance structures.

2 Identify and Coordinate with Others

Laws identifying AWN entities vary across the Federal, SLTT, and non-governmental landscapes. Typically, an elected official holds this responsibility and delegates their authority to an emergency management agency, which serves as the jurisdiction's AO. Additionally, some states recognize the value of allowing local districts to use statewide systems, while in other cases, individual localities are responsible for AWNs. AOs should understand these structures, the laws governing AWN issuance, their roles and responsibilities, and establish clear lines of authority as well as efficient communications between organizations with related AWN responsibilities.[9] AOs should coordinate with the following groups:

[5] DHS Science and Technology Directorate (S&T), "Best Practices in Wireless Emergency Alerts," September 2013.

[6] When joining established AWN systems, such as the FEMA's Integrated Public Alert and Warning System (IPAWS), typically public safety bodies need to apply to become an alerting authority. Refer to the FEMA website for more information on completing this process, DHS's Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report (pp. 1-14) for a detailed real-world example of the IPAWS application process (listed above), and the Chemical Stockpile Emergency Preparedness Program's (CSEPP) Guide to Implementing the Integrated Public Alert and Warning System (IPAWS), a comprehensive tool for implementing and integrating IPAWS.

[7] DHS S&T, "Best Practices in Wireless Emergency Alerts," September 2013.

[8] See the SAFECOM website.

[9] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.

- **Public Safety Answering Points (PSAPs), Public Safety Communication Centers (PSCCs), and Emergency Communication Centers (ECCs):** Staffed around the clock, PSAPs, PSCCs, and ECCs communicate situational awareness information to decision makers and often issue AWNs on their behalf. Additionally, these answering points and communication centers commonly receive an influx of calls following an AWN issuance, whether the facility issued the AWN or not. As such, public safety officials should coordinate with these entities—within and around their jurisdictions—to prepare staff to issue AWNs if required and respond to any public inquiries that follow.

- **Emergency Management Community:** As the emergency manager typically becomes the principal authority when issuing AWNs to the public,[10] coordination between municipal, county, state,[11] and regional emergency managers serving a community is imperative. Additionally, AOs should understand the National Incident Management System (NIMS),[12] as this doctrine often influences how information passes between authorities. For example, in the case of an active emergency, an incident commander (IC) might either issue an AWN themselves or request an AWN issuance by contacting their associated public safety answering point or communications center. The public safety answering point or communications center may then issue the AWN and/or pass the request to the jurisdiction's designated emergency manager, who similarly may issue the AWN and/or coordinate with another agency or level of government that holds alerting authority. The National Emergency Management Association (NEMA)[13] and the International Emergency Management Association (IAEM)[14] can help inform AWN efforts regarding the emergency management community and its structures.

- **Departments and Agencies within an AO's Jurisdiction:** AOs should coordinate with departments and agencies such as government offices, transit authorities, and military bases, as well as fire, police, and emergency medical service departments. Describing AWN capabilities, the types of incidents for which AWNs will be issued, and how messages may display across platforms will aid these partners in their own emergency response operations. Additionally, AOs should be mindful that within a jurisdiction, multiple entities may have authority to issue public AWNs. When multiple entities can issue AWNs in a single area, confusion can arise from redundant or contradictory AWNs. AOs can avoid this situation by coordinating across all departments and agencies involved in AWN provision and discussing the possibility of issuing AWNs for other entities.[15,16]

- **Public Information Officers (PIOs):** PIOs are responsible for developing and releasing information about an incident to news media, incident personnel, and other appropriate departments, agencies, and organizations. As such, PIOs should have direct involvement in the AWN process for major emergencies and disasters to ensure safety related information is integrated into public messaging and consistency of all released information.[17]

- **Agencies within Neighboring Jurisdictions:** A single hazard can have broad and cascading impacts that occur across multiple jurisdictions. As such, the same AWNs may need to be issued across jurisdictional boundaries. To ensure synchronized incident management efforts, neighboring jurisdictions' public safety officials, emergency management agencies, government offices, public safety answering points and communications centers, and other AWN entities should coordinate

[10] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.

[11] Organizational structures for day-to-day state emergency management agency operations vary between states, and change from year to year, especially when a new governor takes office. Currently, state emergency management agencies exist within states' departments of public safety (14 states), military departments under the auspices of the adjutant general (18 states), governor's offices (9 states), state police agencies (2 states), or in a combined emergency management/homeland security agency (11 states). [NEMA website, n.d.]

[12] Refer to FEMA's "National Incident Management System," October 2017 for more information.

[13] See the NEMA website.

[14] See the IAEM website.

[15] DHS S&T, "Best Practices in Wireless Emergency Alerts," September 2013.

[16] DHS S&T, "Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report," February 2013.

[17] FEMA, "Basic Guidance for Public information Officers," November 2007.

with one another. AOs should notify neighboring jurisdictions of AWN disseminations to provide situational awareness information and ensure consistent message templates and content. Agencies should also coordinate geo-targeting settings to ensure complete coverage and avoid overlap.

- **General Public:** AOs should coordinate the use of agency and government-generated materials, webpages, press releases, media, interviews, social media, radio news, and presentations at town hall and civic group meetings to drive targeted education campaigns, create AWN awareness, and solicit feedback. AOs should create audience-friendly materials and set appropriate expectations. Moreover, AOs should engage communities within the AWN ecosystem by identifying those responsible for AWN issuance, characterizing incident types warranting AWNs, outlining associated AWN costs, and classifying relevant AWN distribution channels and outlets.[18] AOs should also instruct the community on what certain tones, sirens, color codes, or threat levels represent, what community hazards exist, what protective actions to anticipate, where to find additional authoritative information sources,[19] and how to subscribe for AWNs.[20]
- **Community Organizations and Facilities:** AOs should leverage partnerships with schools, hospitals, nursing homes, faith-based organizations, major businesses, neighborhood associations, and other major groups to better integrate community groups into the AWN planning process, as well as increase message reach and effectiveness. Partnerships and coordination with these groups will ensure consistency and validity of information, reduce rumors, and re-affirm messages following an AWN dissemination. Coordination should include the establishment of operation, back-up, and notification planning, which can be facilitated through informal or formal agreements, like Memorandums of Understanding (MOU) or Memorandums of Agreement (MOA).
- **Critical Infrastructure Sectors:** Critical infrastructure provides essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. Public safety officials and AOs need to establish lasting partnerships with the stakeholders coordinating these assets, systems, and networks (e.g., physical and virtual) to ensure effective communication and coordination throughout the entire AWN cycle.
- **Communications Providers:** Partnerships and coordination with communications providers is crucial to the success of AWN dissemination. These include, but are not limited to:

  - AM, FM, and satellite radio
  - Digital, analog, and satellite TV
  - Newspapers and magazines
  - Alert origination software vendors
  - Internet, web browsers, social media,[21] and web services and applications
  - Telecommunications service providers and mobile application providers

[18] Ibid.

[19] National Research Council, "Public Response to Alerts and Warnings Using Social Media," *The National Academies Press*: 5-6, 2013.

[20] California Governor's Office of Emergency Services, "Public Alert and Warning Program Assessment for Sonoma County," February 26, 2018.

[21] Social media reaches most of the American population. In the US, 68% of all US adults use Facebook, and specifically within the 18-24 age bracket, a high number of young adults use Snapchat (78%), Instagram (71%), and Twitter (45%). [Pew Research Center, 2018] Thus, AOs should identify all possible barriers to utilizing social media in their AWN arsenals and consider each platform's applications. AOs should "have a plan in advance on how to use social media as a complementary means of communications, and integrate any plans to use social media into standard operating procedures." [Public Safety and Homeland Security Bureau, 2018] AOs should also consider that social media can bring about rapid misinformation sharing that is not easily contained. [National Academies Press, 2013] Conversely, relevant and actionable AWN information may become buried within these platforms' large content volumes. Social media platforms reach a wide audience and AOs should understand that those engaged with this type of messaging will not only include members of their specific community, but a global audience as well. [National Academies Press, 2018] Finally, AOs should recognize that social media [and other communication platforms] are two-way channels of communication where the public expects AOs to address their concerns following an AWN dissemination. [S. Bernier, "Social Media and Disasters: Best Practices and Lessons Learned," presentation at the Disaster Preparedness Summit, August 21, American Red Cross, Chicago, IL.]

3 Develop Plans, Policies and Procedures

Plans,[22] policies, and procedures should be well-documented, supplemented with any necessary additional guidance, field-tested, consistently evaluated for potential gaps and updated accordingly, able to dynamically adapt as the AWN landscape and technologies evolve, based on community threats and hazards,[23] and integrated into operations. These frameworks reduce AWN issuance delays and prevent inconsistencies, by outlining coordination structures between AOs within a jurisdiction and neighboring jurisdictions, roles and responsibilities, system utilization scope and expectations, and the steps required for carrying out time sensitive and essential tasks. Some examples of these frameworks include:

- SOPs
- Public AWN plans
- Emergency communications plans
- Tactical interoperable communications plans
- Regional interoperable communications plans
- EAS plans[24]

Plans, policies, and procedures should define roles and responsibilities including identifying who can request, approve, and disseminate an AWN, how to select an appropriate system for an AWN dissemination, and what to do in the event of an incorrect or false message issuance.

Technology lifecycle management should be employed in planning, operations, and maintenance of AWN systems. AWN entities should manage technology and infrastructure lifecycle risk[25] by remaining aware of technology and infrastructure changes, instituting technology governance best practices, and performing requirements generation, solution design and testing prior to solution selection. Considering funding and sustainment models in advance of technology deployment is also important. After implementation, AWN entities should provide continuous risk management and value assessments of their systems.

During requirements generation, AWN entities should consider the impact of solutions on public users. Systems that require recipients to subscribe or necessitate multiple time intensive steps prior to message issuance may impede the objectives of AWNs that contain life-safety information. Using these systems for non-immediate or reinforcing messaging, instead of as primary AWN mechanisms, can help ensure messages are received by all those at risk in a timely fashion. Familiarization with supporting telecommunications infrastructure and processes, as well as AWN software requirements, can also help improve message dissemination speed and reach. AWN entities may also provide operators with an instruction manual that clearly outlines the process for navigating a multi-step AWN system to help mitigate potential delays (e.g., step-by-step instructions with screen shots). AOs should also work to identify the various strengths, weaknesses, opportunities, and threats that each AWN system presents in conjunction with their area's hazard profile prior to implementation.

The nature, location, and timeline of an incident as well as the relationships established with local organizations and agencies influence the tactics AOs should use when disseminating AWNs; these tactics can change as an incident evolves in size, scope and complexity. Use of the "sliding scale" approach for Type V (least complex) through Type I (most complex) incidents can help ensure message dissemination route choice aligns with incident severity. Refer to DHS S&T's *Report on Alerting Tactics*[26] for more information on alerting tactics, their associated benefits and barriers, and information on the "sliding scale."

[22] Refer to FEMA's "Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide 101, Version 2.0," November 2010 for guidance on the fundamentals of planning and development of emergency operations plans.
[23] Refer to FEMA's "Threat and Hazard Risk Assessment and Stakeholder Preparedness Review Guide, Comprehensive Preparedness Guide 201, 3rd Edition," May 2018 for information on identifying and quantifying community specific threats and hazards, evaluating preparedness, and setting capability targets.
[24] A minimum requirement for all states that should be developed in accordance with 47 C.F.R. Part 11.
[25] Refer to SAFECOM's "Technology Lifecycle Framework," (forthcoming) for more information on technology lifecycle management.
[26] DHS S&T, "Report on Alerting Tactics," August 7, 2018.

4 Account for Diverse Populations

Diversity within a population can influence an individual or group's access to AWNs, their level of risk faced, as well as the way they receive, interpret, and act upon a message. Understanding how messages reach the public as well as the needs of diverse groups throughout the whole community is key to ensuring AWN effectiveness.

Ensure Inclusivity: Gender, age, ethnicity, socioeconomic status, transitory or recently arrived status, familial relationships, an individual's or community's past experiences, environmental and social factors, access and functional needs, language, literacy, ability, remoteness or isolation, access to technology, and other factors, can all affect how people interpret and subsequently respond to AWNs. AOs should work to understand these factors, along with the threats and risks that these diverse populations face prior to emergencies. AOs should actively engage these diverse populations to facilitate their inclusion in AWN planning efforts to ensure appropriateness and accessibility of messages; advocacy groups can help AOs understand community needs and may act as conduits for message dissemination.

Ensure Accessibility: Different populations have varying levels of access to different communication pathways. One technology is usually insufficient because often, use of multi-modal technologies, both modern and traditional, are necessary to reach people with varying levels of access.[27] When appropriate, AOs should also consider the use of more dynamic, visual, and spatial content, outside of text messages, to reach diverse populations, ensure accessibility, and better convey risk. Additionally, pre-messaging and alternative guidance can help those who need more time to prepare or cannot take the recommended protective actions. Still, provision of translations and other variants should not delay an initial AWN.[28]

Follow the Information Model for Access to Emergency Alerts:[29]

- Be compatible with various transmission systems
- Provide message details in text, audio, tactile, image, or other visual forms
- Provide message details in multiple languages
- Use multiple forms of presentation appropriate to the needs of individual recipients
- Make appropriate use of font size, foreground/background color and other visual attributes in image and text presentations
- Use appropriate language for comprehension by the intended audience
- Allow extension of the information format to meet future needs
- Facilitate delivery of the message to all recipients through multiple channels

Additionally, refer to Chapter 7 of the Communications Security, Reliability, and Interoperability Council's *Final Report – Re-imagining of Emergency Alerting*[30] publication (pp. 36-47) for a range of AWN system considerations for reaching diverse populations.

5 Maintain Security and Resiliency

Systems that instruct significant portions of the population to act are targets for attack, which can affect availability of these services and the validity of the messages they provide.[31] Thus, AOs should ensure

[27] D. Mileti, "PrepTalks: Modernizing Public Warning Messaging," *FEMA*, February 13, 2018.

[28] California Governor's Office of Emergency Services, "California State Warning Plan," December 2016.

[29] National Center for Accessible Media at WGBH, "Access to Emergency Alerts for People with Disabilities Recommendations for Accessible Emergency Notifications," March 2009.

[30] Communications Security, Reliability, and Interoperability Council, "Final Report – Re-imagining of Emergency Alerting," June 2018.

[31] National Academies of Sciences, Engineering, and Medicine, "Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions," 2018.

AWN networks, devices, systems, and user interfaces are secure from cyberattacks, and are resilient in the case of an attack or outage.

Follow the Cybersecurity Risk Management (CSRM) Strategy:[32]

- *Stage 1*: Identify all components within the AWN pipeline, including system lifecycle phases such as adoption, operations, and sustainment. Describe the operating environment and system's response to an incident.
- *Stage 2*: Conduct a cybersecurity risk assessment and vulnerability analysis of the overall system, including network, software, and operational procedures to identify and mitigate cyber vulnerabilities, threats, and risks.
- *Stage 3*: Evaluate the likelihood and potential impact of the cyber threat(s) and prioritize mitigation efforts accordingly.
- *Stage 4*: Establish positions and assign mitigation tasks based on the cybersecurity analysis and risk assessment. Determine when to implement mitigation efforts in the AWN lifecycle.

Counter Cyber Risks with Policies and Procedures:[33]

- *User Privilege*: Develop security policies based on a user's role.
- *Employee Use Policies*: Maintain policies on the installation and use of programs, devices (e.g., personal and portable storage), and Internet browsing.
- *Strong Passwords*: Establish password policies regarding length, combination of letter cases and special characters, and expiration periods that will require users to change passwords on a regular, pre-determined basis (e.g., 30, 60, or 90 days).
- *Multi-factor Authentication*: Utilize additional authentication controls like smart cards (e.g., personal identity verification cards), tokens, and biometrics to ensure multi-layered authentication.
- *Editorial Review*: Establish an AWN review process to eliminate dissemination of erroneous information.

Choose the Right Software: AWN software should meet certain technical standards and AOs should carefully consider which product they use. Cybersecurity and resiliency should be built into AWN networks from the start and software should easily integrate with existing programs and systems. Software should provide AOs the ability to preview and cancel an AWN, send a message to the AO when the software license or password is about to expire, provide an intuitive user interface, be able to send AWNs through multiple channels, and allow AOs to see AWN histories and logs.[34] Additional software considerations for AOs are provided by FEMA,[35] and within (pp. 16-17) of the DHS *Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report*.[36]

Maintain Access Controls: Access controls should be built into AWN structures. System administrators should control user permissions and their ability to send out live messages. Credentials should be required for logging into an AWN system and operators should have their own uniquely identifiable account so system administrators can track system use and AWN issuances; login credentials should not be stored on an AWN system.[37] Operators should continually ensure their proficiency in accessing and navigating AWN system applications, as in some jurisdictions, AWN systems are rarely used, and passwords as well as system use requirements can easily be forgotten.

Maintain Secure Software and Cybersecurity: Attacks on AWN systems can result in property destruction, financial loss, infrastructure disruption, injury, and death. Attacks can also damage the credibility of an AO.[38] Refer to Chapter 4 (pp. 26-34) of the DHS S&T First Responders Group *Best*

[32] DHS S&T, "Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators," September 2013.
[33] DHS, "Emergency Services Sector Roadmap to Secure Voice and Data Systems," March 2014.
[34] Office of Inspector General, "FEMA's Oversight of the Integrated Public Alert & Warning System: OIG-19-08," November 19, 2018
[35] See the FEMA website.
[36] DHS S&T, "Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report," February 2013.
[37] J. Rosen, "Preventing Another Hawaii: Emergency Notification Best Practices," *Security Magazine*, February 13, 2018.
[38] DHS S&T, "Best Practices in Wireless Emergency Alerts," September 2013.

Practices in Wireless Emergency Alerts[39] publication as well as Chapter 4 (pp. 58-67) of the DHS *Emergency Service Sector Roadmap to Secure Voice and Data Systems*[40] for additional guidance on how to maintain secure software and cybersecurity.

Ensure System Sustainment, Continuity, and Redundancy: Consolidation of various jurisdictions' AWN programs (into a system of systems) may provide benefits such as increased responsiveness, operational redundancy, greater adherence to standards, and costs savings in procurement and administration.[41] Employing back-up AWN systems, and preventative care and maintenance of primary and backup systems can further increase resiliency. Such practices may keep AWN capabilities in place, even in the case of a cyberattack, loss of power, or other type of system or network outage. For additional information, refer to CISA's Communications Resiliency Resources and FEMA's Continuity Resource Toolkit.

Consider Impact on Networks: AOs should also consider the impact of their AWNs on networks. Communications networks often suffer congestion during public safety incidents and may incur damage from manmade or natural disasters. AOs should understand the impact of their messaging to avoid overloading already taxed systems.

6 Incorporate Safeguards

To ensure a false message is not mistakenly disseminated, AOs should consider the entire AWN lifecycle—specifically the impacts of human and machine involvement—and incorporate safeguards accordingly. Forcing a message to go through redundancy measures can prevent manmade and unintentional errors from occurring.[42] In some cases, local AOs may at times, only staff one or two operators. With this said, efforts should be made to ensure two operators confirm the accuracy and validity of AWNs before issuing a wide-reaching message that will affect a large portion of a population.

Maintaining a separation of duties between the operator developing the message and entering the data, with the operator who reviews and authenticates the information prior to sending the AWN, further ensures accuracy.[43] SOPs for canceling, revoking, or correcting inaccurate or false messages should also be developed[44,45] (see the "Monitor and Correct" section for more information). Additionally, AOs should consider utilizing distinctly different AWN software system interfaces (i.e., different colors and clear training/test labels, not different system navigation steps and processes) to distinguish test and live environments. All these mitigations, like others, should be seamless and not delay or prevent the issuance of an AWN.

7 Train, Exercise and Test Systems

Trainings, exercises, and tests are essential for ensuring proficiency with AWN tools (i.e., processes, operations, technologies, and rules). AOs should ensure courses and materials remain current and are used by their staff and AWN partners on a recurring basis. AWN software vendors should also provide training to AOs on their software's functionality and capabilities.[46] Additionally, having

[39] Ibid.

[40] DHS S&T, "Emergency Service Sector Roadmap to Secure Voice and Data Systems," March 2014

[41] Sonoma County California, "Assessment Report: Community Alert and Warning," June 11, 2018.

[42] DHS, "Emergency Services Sector Roadmap to Secure Voice and Data Systems," March 2014.

[43] Federal Communications Commission (FCC), "Report and Recommendations Hawaii Emergency Management Agency January 13, 2018 False Alert," April 10, 2018.

[44] Sonoma County California, "Assessment Report: Community Alert and Warning," June 11, 2018.

[45] FCC, "Report and Recommendations Hawaii Emergency Management Agency January 13, 2018 False Alert," April 10, 2018.

[46] Office of Inspector General, "FEMA's Oversight of the Integrated Public Alert & Warning System: OIG-19-08," November 19, 2018

vendors present during tests can help mitigate for potential issues and aid AOs in solving problems, should any arise.

Prepare and Conduct Trainings and Exercises: The Chemical Stockpile Emergency Preparedness Program's (CSEPP's) *Guide to Implementing the Integrated Public Alert and Warning System (IPAWS)*[47] (pp. 50-55), provides guidance for AWN training. AOs should utilize FEMA's IS-247 Course: Integrated Public Alerts and Warning Systems (IPAWS) in conjunction with other AWN training provided by local jurisdictions, industry organizations, and software vendors.

Prepare and Conduct Internal Tests: Internal tests should be appropriately supervised in controlled environments to prevent false message dissemination; agencies can develop a second separate system designed specifically for the testing environment with distinct usernames and passwords. AOs can also use FEMA's IPAWS Lab as a resource for testing their systems. To minimize potential confusion, AOs should limit employee access to create or modify internal drill messages. In addition, AOs should avoid phrases like "this is not a drill" or "real world" in test messages to ensure clear distinctions between test and live messages. Instead, test messages should be clearly identified with language like "this is a test."[48] The DHS S&T First Responders Group *Best Practices in Wireless Emergency Alerts*[49] publication (pp. 14-18) offers additional resources on testing topics and overall training structures.

Prepare and Conduct Live End-to-End Tests: AOs should plan out these tests and their steps thoroughly to prevent any false messaging or other errors. These live (real-world) AWN system tests are beneficial for confirming system functionality and increasing public awareness of AWN systems but should be conducted sparingly to avoid causing "alert fatigue" (see "Deliver Actionable Messaging" section). Additionally, working with PIOs to conduct public outreach before these tests and then seeking internal and public feedback afterwards will increase test receptiveness, reduce confusion, and provide valuable lessons for incorporation into future operations. Finally, to prevent confusion, live tests should be rescheduled to a later date if they conflict with a real-world incident or major event occurring within the same jurisdiction for which the test is scheduled. The DHS *Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report*[50] (pp. 10-14) provides an example of a live end-to-end test.

Incorporate Lessons Observed: Following the above activities, an after-action discussion and evaluation should occur to discuss whether the goals and objectives of the test or exercise were met. These discussions should capture lessons observed through well documented after-action reports to identify areas for improvement and necessary actions for integrating lessons expeditiously into operations (this same process should also follow incidents). This process mitigates for potential future mistakes and works to enhance the confidence of end users.

8 Eliminate Issuance and Dissemination Delays

Delayed AWN issuance and audience dissemination can lead to potentially disastrous outcomes. AOs should work with all stakeholders to minimize issuance delays, from the point of a hazard's detection, to the dissemination of an AWN.

Create Message Templates: While impossible to pre-script messages for every possible hazard, AOs should prepare standardized message templates and recommended protective actions in advance, and know how to tailor these messages during an incident.[51,52] Messages should be tailored according to the audience, incident, and expected public response, and account for a community's diverse needs (see the "Account for

[47] CSEPP, "Guide to Implementing the Integrated Public Alert and Warning System (IPAWS)," October 2015.
[48] Ibid.
[49] DHS S&T, "Best Practices in Wireless Emergency Alerts," September 2013.
[50] DHS S&T, "Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report," February 2013.
[51] California Governor's Office of Emergency Services, "California State Warning Plan," December 2016.
[52] Sonoma County California, "Assessment Report: Community Alert and Warning," June 11, 2018.

Diverse Populations" section). Additionally, AOs should include their agency's PIO and public affairs office when crafting message templates.

Expedite Information Sharing: Although a hazard may be identified early by a particular entity, information regarding a threat is not useful unless all AOs and incident response entities are also informed of the threat quickly, so they may disseminate information to those at risk accordingly. If timely information sharing does not occur, the issuing of messages may be delayed, the public may be unaware of the need to take protective actions, and response efforts may be hindered from a lack of situational awareness. Prevent delayed information sharing by ensuring MOUs or MOAs are in place between necessary partners (see "Identify and Coordinate with Others" section) and interacting with these partners regularly.

Identify and Establish Triggers: AOs should consider identifying triggers based on a hazards severity, urgency, and certainty to distinguish threat levels (e.g., none, low, medium, and high) or classes (e.g., Information Statement, Advisory, Watch, and Warning),[53,54,55] the corresponding officials to notify, AWNs to disseminate (including hazard-specific protective actions), and which system (or combination of systems) to use for various incidents.[56] AOs may also consider revising thresholds for planned events, which can change the associated time needed for a community to take protective actions (e.g., large congregations of people or event-related road closures could slow evacuations). Additionally, although sensor generated AWNs can quickly and automatically provide information regarding an impending hazard, AOs should use caution when considering disseminating automated messages. Validating these warnings and tailoring messaging before disseminating an AWN can help prevent false alerts and ensure accuracy. Still, AWNs may be triggered automatically for extremely fast-moving hazards to provide enough time for the public to take protective actions,[57] but a risk assessment should be conducted to weigh the potential benefits and consequences of automatically disseminating AWNs generated without human intervention.

Establish a Rapid and Redundant Decision Tree: AOs should establish a decision-making apparatus for rapid AWN issuance, cancellation, revocation, and clarification which clearly defines roles and responsibilities. This mechanism should be formalized through a defined chain of command, not ad-hoc pronouncements. Multiple officials who hold regular day-to-day decision making authority should have permission for approving and/or issuing AWNs to ensure redundancy in the case where particular approved officials are unavailable, while the number of people required to approve and issue an AWN should be minimal to avoid delays.[58,59] AOs should have redundant communication tools like satellite phones to communicate with partners and make decisions during network outages, procedures for making decisions to issue AWNs outside of standard work hours, and be able to improvise if circumstances keep them from following procedures.[60] Additionally, AOs should have a secure method to issue AWNs remotely to reduce delays caused by an operator needing to travel to their facility to issue a message.

9 Deliver Actionable Messaging

The public's perception of risk is an important factor to consider when crafting and disseminating information regarding hazardous situations. AOs should ensure that messages contain information that convey the true level of risk associated with a hazard, encourage the taking of protective actions, remain

[53] DHS S&T, "Best Practices in Wireless Emergency Alerts," September 2013.
[54] Sonoma County California, "Assessment Report: Community Alert and Warning," June 11, 2018.
[55] D. Mileti and J. Sorensen, "A Guide to Public Alerts and Warnings for Dam and Levee Emergencies," *U.S. Army Corps of Engineers Risk Management Center*, June 5, 2015.
[56] California Governor's Office of Emergency Services, "Public Alert and Warning Program Assessment for Sonoma County," February 26, 2018.
[57] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.
[58] G. Davies, "Connecting the Dots: Lessons from the Virginia Tech Shootings," *Change: The Magazine of Higher Learning* 40 (1): 8-15, 2008.
[59] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.
[60] D. Mileti and J. Sorensen, "A Guide to Public Alerts and Warnings for Dam and Levee Emergencies," *U.S. Army Corps of Engineers Risk Management Center*, June 5, 2015.

transparent, and avoid causing "alert fatigue," while still erring on the side of public safety when dealing with conflicting or uncertain information about a threat.

Provide the Right Information: AOs should work to understand how the public responds to AWNs. How individuals receive AWNs influences their perception of risk, which consequently impacts their timeliness in initiating protective actions.[61] Provision of comprehensive, targeted, and specific messaging enables the public to make informed decisions. This tactic limits milling, that is, people delaying taking protective actions after receiving an AWN to search for more information, to decide what, if anything, to do.[62] AWNs should contain the following information: identification of the AO issuing the message (source), hazard type and impact consequences (threat), the impact area boundaries (location), protective actions to take including when to take them, how to take them, and how taking them reduces impacts (guidance/time), and when the AWN expires and/or new information will be distributed (expiration time).[63,64] Furthermore, messages should be easy to understand, free of mistakes, and based on the most current information available. AOs should coordinate with PIOs as soon as possible to best ensure synchronized public-facing communications. Still, this coordination should not delay AWN issuances for rapid-onset incidents that may pose an imminent threat. Refer to FEMA's PrepTalk: Modernizing Public Warning Messages for further information regarding actionable messaging as well as Chapter 1 (pp. 18-44) of the National Academy of Sciences, Engineering, and Medicine's *Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions*[65] for more information regarding public response to AWNs.

Account for the Public's Perception of Risk: AWN messages should be authoritative and confident. Still, AOs must often issue AWNs under uncertain circumstances, as damages may incur before a threat can be verified. So to ensure the timely taking of protective actions, AWNs should be issued early and message content geared towards the uncertainty of an incident (e.g., specifying an incident as "reported" and providing revised information as needed).[66] Additionally, people rarely act on a single message alone,[67] so delivering messages through multiple channels increases public attention and audience reach, confirms message importance and authority, and encourages the taking of protective actions. Moreover, to gain recognition, AWNs should be issued from a trusted source.

Maintain Transparency: AWNs should be transparent and honest. AOs should not withhold information out of fear for causing panic, as this only serves to inspire distrust, and forces people to seek information from other less reliable sources. AOs should also work to confirm hazardous situations and "policies should clearly identify what level of certainty is needed (e.g., confirmation from X independent sources, eyes on the scene) before issuing an [AWN] message."[68] Still, AOs "should use their best judgment but err on the side of public safety" when deciding whether to issue an alert or warning that has the potential to turn out to be a false alarm, or when dealing with conflicting or uncertain information about a threat. "Incomplete or imperfect information is not a valid reason to delay or avoid issuing an [AWN]."[69] "When in doubt, warn."[70]

Avoid Causing "Alert Fatigue": Irrelevant messaging fatigues the public and causes recipients to discount or unsubscribe for further AWNs.[71] As such, wide reaching AWNs should be disseminated wisely and

[61] National Academies of Sciences, Engineering, and Medicine, "Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions," 2018.

[62] D. Mileti, "PrepTalks: Modernizing Public Warning Messaging," *FEMA*, February 13, 2018.

[63] D. Mileti and J. Sorensen, "A Guide to Public Alerts and Warnings for Dam and Levee Emergencies," *U.S. Army Corps of Engineers Risk Management Center*, June 5, 2015.

[64] National Advisory Council, "Modernizing the Nation's Public Alert and Warning System," *FEMA*, February 15, 2019.

[65] National Academies of Sciences, Engineering, and Medicine, "Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions," 2018.

[66] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.

[67] National Research Council, "Public Response to Alerts and Warnings Using Social Media," *The National Academies Press*: 5-6, 2013.

[68] DHS S&T, "Wireless Emergency Alerts: New York City Demonstration Lessons Learned Report," February 2013.

[69] California Governor's Office of Emergency Services, "California Sate Warning Plan," December, 2016.

[70] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.

[71] J. Trainor, D. Nagele, B. Philips, and B. Scott, "Tornadoes, Social Science, and the False Alarm Effect," *American Metrological Society*, October 21, 2015.

issued for imminent rapid onset, short detection to impact hazards, that threaten life, health, public safety, security, or property, and require immediate action,[72] thereby maintaining future public receptiveness to AWNs for hazards that pose a significant threat.

Geotargeting—disseminating AWNs based on recipient location—is important to ensure that those not at risk do not receive inapplicable messages. With this said, AOs should be mindful that some hazards may impact locations of interest to these individuals, like the location of a family member or home, and might rapidly spread into unwarned areas. So, targeting should include people (and their devices), who are at risk from a hazard, or who care about people and property at risk from a hazard, and issued across areas where potential for the hazard to spread exists. If there is concern that people who are safe could think that they are unsafe, the AWN message should address these individuals—for example, a message could state "people who live in other parts of the city will not experience flooding," and then also explain why these areas are safe.[73,74]

Additionally, alert origination operators need to sort through a large amount of potential threat information (disseminated internally within a public safety entity for situational awareness) to determine each messages validity, the actual threat posed, and any follow-up actions to take, or AWNs to issue to the public. As such, too many illegitimate or minor threat messages can cause internal "alert fatigue." To address this issue, AOs should work to reduce the number of messages requiring an operator's attention, to prevent operators from overlooking hazards that pose a real or serious threat.[75]

10 Monitor and Correct Misinformation

Real-time evaluation of public response patterns, checking for misinformation, and correction of ineffective or false messaging ensures correct and accurate information flow as well as a desired public response.

Monitor: AOs should work with PIOs to monitor information and the public's response to AWNs—verifying AWNs reach their intended recipients and that recipients are taking the correct protective actions, listening for incorrect information, assessing situational changes, and subsequently providing updates accordingly. Assessing application data analytics and social media traffic can aid AOs in this process. Refer to the DHS S&T's Social Media Working Group for Emergency Services and Disaster Management documents for more information about incorporating social media into AWN processes.

Correct: In the event of misinformation, AWN corrections should be issued swiftly, and over the same system(s) used for the initial dissemination. Other available AWN systems should be utilized to reinforce these retractions, amendments, or updates, to ensure messages are received across multiple platforms, and increase the likelihood of receipt.[76] AOs should explain the reasons behind any changes.[77] AOs may also consider including a website link within messages, so AWN recipients can easily access up-to-date incident information, and consider issuing an "all clear" notice once a threat has subsided.

[72] D. Mileti, "PrepTalks: Modernizing Public Warning Messaging," *FEMA*, February 13, 2018.

[73] National Academies of Sciences, Engineering, and Medicine, "Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions," 2018.

[74] D. Mileti and J. Sorensen, "Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment," *FEMA*, August 1990.

[75] G. Masters, "Crying Wolf: Combating Cybersecurity Alert Fatigue," *SC Magazine*, June 9, 2017.

[76] FCC, "Report and Recommendations Hawaii Emergency Management Agency January 13, 2018 False Alert," April 10, 2018.

[77] National Research Council, "Public Response to Alerts and Warnings Using Social Media," *The National Academies Press*: 5-6, 2013.

CONCLUSION

To better protect the nation and maintain an informed public during crises, AOs should coordinate with all partners and stakeholders to prioritize the establishment, maintenance, and improvement of AWN oversight and systems. Security safeguards and resiliency practices—addressing both human errors and technical issues—protect this critical emergency ecosystem. AWN structures must incorporate the diverse backgrounds and risk perceptions of the whole community into messaging considerations to ensure that actionable messages reach all effected groups in a timely fashion. While operators and systems responsible for messaging sometimes experience setbacks, officials must work to capture and integrate lessons observed into operations to better ensure the public's safety and preserve their trust in emergency management institutions.

Appendix A: Acronyms

AO	Alert Originator
AWN	Alert, Warning, and Notification
CISA	Cybersecurity and Infrastructure Security Agency
CSRM	Cybersecurity Risk Management
CSEPP	Chemical Stockpile Emergency Preparedness Program
DHS	Department of Homeland Security
EAS	Emergency Alert System
ECC	Emergency Communications Center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
IAEM	International Association of Emergency Managers
IC	Incident Commander
IPAWS	Integrated Public Alert and Warning System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCSWIC	National Council of Statewide Interoperability Coordinators
NEMA	National Emergency Management Association
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OPEN	Open Platform for Emergency Networks
PIO	Public Information Officer
PSAP	Public Safety Answering Point
PSCC	Public Safety Communication Center
S&T	Science and Technology Directorate
SLTT	State, Local, Tribal, and Territorial
SOP	Standard Operating Procedure
WEA	Wireless Emergency Alert

Appendix B: Disclaimer of Liability

The *Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings, & Notifications* document (hereinafter the "document") is provided by the Department of Homeland Security (DHS) and is intended to provide guidance, and does not contain or infer any official requirements, policies, or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents.

As a condition of the use of the document, the recipient agrees that in no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected to the document or the use of information from the document for any purpose.

DHS does not endorse any commercial product or service referenced in the document, either explicitly or implicitly. Any reference herein to any specific commercial products, processes, or services does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or DHS.

The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or DHS and shall not be used for advertising or product endorsement purposes. Alert, warning, and notification (AWN) systems and government rules and regulations (at all levels of government) regularly change; it is the responsibility of the reader to ensure they remain informed and up-to-date of any changes to AWN systems, as well as government rules and regulations.