Software Engineering Institute

Best Practices in Wireless Emergency Alerts

John D. McGregor
Joseph P. Elm
Elizabeth Trocki Stark, SRA International, Inc.
Jen Lavan, SRA International, Inc.
Rita Creel
Chris Alberts
Carol Woody
Robert Ellison
Tamara Marshall-Keim

February 2014

SPECIAL REPORT
CMU/SEI-2013-SR-015

CERT® Division, Software Solutions Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

DM-0000430

Table of Contents

List of Figures

List of Tables

Acknowledgments

We thank the following organizations for their help and feedback during data collection:

- Adams County 911, Colorado
- Alachua County Fire Rescue, Florida
- Altus Emergency Management Agency, Oklahoma
- Arvada Police Department, Colorado PUC 911 Task Force
- California Emergency Management Agency (Cal EMA)
- Cassidian Communications
- Cecil County Emergency Management Services, Maryland
- City of Pittsburgh Emergency Management & Homeland Security, Pennsylvania
- Colorado Office of Emergency Management
- Commonwealth Interoperability Coordinator's Office, Virginia
- Dane County Emergency Management, Wisconsin
- Emergency Management and Homeland Security, Lakewood, Colorado
- Fairfax County Office of Emergency Management, Virginia
- Harris County Office of Homeland Security and Emergency Management, Texas
- Hawaii State Civil Defense
- Jefferson County Emergency Communication Authority (JCECA), Colorado
- Johnson County Emergency Management Agency, Kansas
- Larimer Emergency Telephone Authority (LETA 911), Colorado
- Lexington-Fayette Urban County Government, Kentucky
- Maine Emergency Management Agency
- Metropolitan Washington Council of Governments, Washington, D.C.
- National Center for Missing & Exploited Children, Virginia
- National Oceanic and Atmospheric Administration/National Weather Service, Sterling, Virginia
- National Oceanic and Atmospheric Administration/National Weather Service, Colorado
- New York State Division of Homeland Security and Emergency Services
- Office of Emergency Management and Homeland Security, Pittsburgh, Pennsylvania
- Office of Environmental Health & Safety, Carnegie Mellon University, Pittsburgh, Pennsylvania
- Virginia Polytechnic Institute and State University, Blacksburg, Virginia
- Washington Military Department, Emergency Management Division, Washington
- Westminster Fire Department, Westminster, Colorado

Abstract

This report presents four best practices for the Wireless Emergency Alerts (WEA) program. These best practices were identified through interviews with emergency management agencies across the United States. The WEA "Go Live" Checklist identifies key steps that an emergency management agency should perform when implementing WEA in a local jurisdiction and provides guidance for completing each action. The WEA Training and Drilling Guide identifies the steps for preparing staff to use WEA and includes suggestions shared by alerting authorities that have implemented WEA. The WEA Governance Guide identifies steps for using or preparing to use WEA to ensure coordination between participating alerting agencies. The WEA Cybersecurity Risk Management (CSRM) Strategy describes a strategy that alert originators can use throughout WEA adoption, operations, and sustainment, as well as a set of governance activities for developing a plan to execute the CSRM. Because best practices will evolve as WEA matures and becomes more widely used, an appendix provides information on how a best practice–driven organization can search for best practices, adapt them to the local context, and adopt them for everyday use.

1 WEA Best Practices

In developing the sample best practices for the Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), contained in this report, the authors first performed research regarding the development and dissemination of best practices. Much of this research is summarized in the appendix. This research provided insights into best practice identification methods and guidance for the best practice documentation.

The four best practices contained herein were identified through interviews with emergency management agencies (EMAs) across the United States. Through these interviews, the researchers focused on attaining a clear understanding of the needs of the alert origination community and the challenges its members faced. Due to the infancy of the WEA service, many interviewees were not yet using WEA during the interview period throughout 2012 and early 2013. However, they were still able to provide relevant insights into WEA adoption and use based on previous experiences of adopting other systems and using other types of alerting systems. Through amalgamation of the inputs from the many interviewees, the researchers identified four topics for developing best practices:

1. WEA Go-Live Checklist
2. WEA Training and Drilling Guide
3. WEA Governance Guide
4. WEA Cybersecurity Risk Management Strategy

After identifying the best practices to address, the researchers developed the following guidelines to promote consistency:

1. Alert originators (AOs) are the primary audience for the WEA Best Practices. The WEA Best Practices must address their context, their needs, and their capabilities.
2. WEA Best Practices must be *relevant* to the audience. They must address a topic of interest and of value to the alert originating community.
3. WEA Best Practices must present information with *clarity*. They must be clearly written using terms, language, and style consistent with the audience.
4. WEA Best Practices must be *prescriptive*. They must provide clear recommendations for action.
5. WEA Best Practices must be *actionable*. Their recommendations must be executable within the EMA.
6. WEA Best Practices must be *concise*. They must be brief enough to retain the attention of the audience (10 pages at most). When appropriate, they may include a few relevant references for further elaboration; however, the fundamentals of the best practice must be conveyed within the body of the best practice itself.
7. WEA Best Practices must be *effective*. They must show a measurable improvement over alternative practices.

Based on these guidelines, the researchers further developed and documented the four best practices that seemed most important to AOs.

Due to the infancy of the WEA service at the time of this publication, the researchers could not fully evaluate the efficacy of the best practices through extensive field testing. Instead, the best practices were submitted to experts in the alerting community for review and comment. These reviewers included academics performing research in public alerting as well as public alerting practitioners.

Best practices are intended to be living documents. The four samples contained in this report are best practice "seeds" sown during the infancy of WEA. As WEA matures and becomes more widely used, AOs should review and revise these best practices as they gain knowledge and experience.

2 WEA "Go Live" Checklist

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), enables authorized public safety officials to send 90-character, geographically targeted alerts to the public via commercial mobile service providers (CMSPs) using the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN). The checklist in Table 1 identifies key steps that an emergency management agency should perform when implementing WEA in a local jurisdiction. Guidance for completing each action follows the checklist. The order of some of the steps may vary, depending on the organization's needs.

Table 1: WEA "Go Live" Checklist

Step	Action	Owner	Completion Date
1	Acquire IPAWS-compatible software1		
2	Establish memorandums of agreement with FEMA1		
3	Apply for IPAWS public alerting authority permissions1		
4	Complete IPAWS web-based training (IS-247)1		
5	Establish internal policies and standard operating procedures (SOPs) for WEA		
6	Train internal staff and other related personnel Train WEA operators using IPAWS web-based training (IS-247), proprietary materials based on your WEA SOPs, and your service provider's training materials Train other staff (e.g., dispatchers, 911 operators, public relations personnel) on the purpose and usage of WEA to prepare them for the impacts of WEA		
7	Coordinate plans for WEA deployment with emergency response agencies in your jurisdiction		
8	Coordinate plans for WEA deployment with emergency response agencies in adjacent jurisdictions and the state		
9	Complete internal testing of WEA operations		
10	Educate the public about WEA using state-generated materials (if available), press releases, media interviews, social media, your agency's website, presentations at town hall and civic group meetings, etc.		

WEA Go Live Guidance

1. Acquire IPAWS-Compatible Software[1]

Alert originators (AOs) initiate WEA messages by sending messages compliant with the Common Alerting Protocol (CAP) to IPAWS-OPEN using IPAWS-compatible software. Choose software and identify it in a memorandum of agreement (MOA) with FEMA (see Step 2). You may develop your own software or acquire it from a commercial supplier. A list of commercial vendors that have executed an MOA with FEMA for the purpose of gaining access to the IPAWS-OPEN Test Environment can be found at www.fema.gov/library/viewRecord.do?id=5670. Although FEMA neither endorses any specific products nor verifies the developer-submitted data, the list can serve as a starting point for you to identify commercial vendors that may have developed or may be in the process of developing IPAWS-compatible software that can issue WEA messages. If you are

1 The first four steps are required as part of FEMA's application process (see www.fema.gov/alerting-authorities).

acquiring your software from a commercial supplier, be sure to address issues such as security, testing, training, and sustainment in the choice of your supplier.

2. Establish Memorandums of Agreement (MOAs) with FEMA[1]

A Collaborative Operating Group (COG) is an organization that is responsible for coordinating emergency management or incident response activities and is authorized to issue emergency alerts. To create a COG, AOs must establish MOAs (the application is available at www.fema.gov/library/viewRecord.do?id=6019) with FEMA to gain access to IPAWS-OPEN and the Joint Interoperability Test Command (JITC), an instantiation of IPAWS-OPEN available for users to test and practice their alerting processes. After approval, FEMA will issue a COG ID and digital certificates that will enable users to securely access IPAWS-OPEN and the JITC Test Laboratory.

3. Apply for IPAWS Public Alerting Authority Permissions[1]

You must obtain approval to issue public alerts from a reviewer designated by your state.[2] FEMA will provide an Application for Public Alerting Authority and the contact information for your state reviewer after receiving your MOA. The application defines the types of alerts you intend to issue and the extent of your geographic warning area.

4. Complete IPAWS Web-Based Training (IS-247)[1]

One representative from your COG must satisfy FEMA's IPAWS training course "IS-247: Integrated Public Alert and Warning System (IPAWS)," available at http://training.fema.gov/EMIWeb/IS/is247a.asp. After your organization successfully completes Steps 1–4, FEMA will implement your COG's specific public alerting permissions in IPAWS-OPEN.

5. Establish Internal Policies and Standard Operating Procedures (SOPs) for WEA

You should create internal policies and SOPs for WEA that meet your alerting objectives and comply with the rules of behavior stipulated in your MOA. Among the topics that your SOPs should address are

- the types of alerts you will issue through WEA
- criteria for triggering an alert (e.g., severity, urgency, certainty)
- notification and approval processes for sending an alert
- geo-targeting capabilities of CMSPs that cover your area and how alerts display on their mobile devices[3]
- methods of creating alerts
  - automated alert assembly by IPAWS OPEN based on the fields contained in the CAP message from the AO

[2] State approval is not required for home rule states and federally recognized tribes. Coordination with state authorities is required within home rule states and is recommended for federally recognized tribes.

[3] See CTIA–The Wireless Association's WEA website, www.ctia.org/wea, for more information about CMSPs. Contact the CMSPs in your area to ascertain their geo-targeting capabilities.

  - free-form alerts using Commercial Mobile Alert Message text (CMAMtext)
  - for either method, templates that can assist you in creating understandable alerts quickly
- training and drilling procedures for staff who send or approve alerts (see Section 3)
- coordination with other agencies within your jurisdiction, as well as state agencies and neighboring jurisdictions
- security procedures to protect your systems from unauthorized use and to mitigate the effects of intrusions
- sustainment of your system, including system upgrades, periodic retraining, and periodic testing

You can find supporting information for many of these topics in the FEMA IS-247 course.

6. Train Internal Staff

Consider requiring all AOs in your organization to participate in FEMA's IS-247a training prior to issuing WEA messages. You can also develop WEA training materials and resources specific to your organization. Use these materials to educate AOs about your organization's WEA policies and SOPs. Solicit feedback from your AOs to evolve and improve these materials until they are comprehensive.

Prepare AOs to operate your organization's IPAWS-compatible software. If you have a vendor product, ask your software provider for instruction and training materials. If your organization developed the product in-house, your IT staff can help create a manual illustrated with screenshots to demonstrate its use. You can also create an illustrated manual to support the training materials furnished by your software provider. Post WEA training materials at the alert origination terminal for easy reference (see Section 3).

Also consider training for personnel other than those who issue alerts. Dispatchers, 911 operators, and public relations staff should have a basic knowledge of WEA to assist them in dealing with the public response to a WEA message.

7. Develop and Coordinate Plans for WEA Implementation with Emergency Response Agencies in Your Jurisdiction

Communicate with the primary emergency response agencies in your jurisdiction about your new WEA capabilities before you implement WEA. Include your Public Safety Answering Point (i.e., 911 call center) and other public-information call centers in your jurisdiction (e.g., 311 call center). This will prepare center operators to receive calls from the public about how to respond to an alert message.

Coordinate with other key offices and agencies in your jurisdiction, such as the mayor's office and fire, police, and emergency medical services. Describe your WEA capabilities, the types of events for which you will issue WEA messages, and how WEA messages may display on mobile devices. Discuss the possibilities of issuing WEA messages for these other agencies.

8. Coordinate Plans for WEA Implementation with Emergency Response Agencies in Adjacent Jurisdictions

Because WEA messages are disseminated via cell broadcast technology, your organization's local WEA messages may cross into other jurisdictions. Notify emergency response agencies in neighboring jurisdictions about your use of WEA so they know what to expect. You should also coordinate with your state's emergency management office, since they will also be issuing WEA messages.

Arrange a planning meeting about the types of incidents for which your organization, your local National Weather Service (NWS) office, neighboring jurisdictions, and your state will use WEA. Coordination helps prevent public confusion about conflicting WEA messages from two or more COGs.

Agree when to notify neighboring jurisdictions of WEA message dissemination, how to coordinate message templates, and how to coordinate alert message content during events that affect multiple jurisdictions. Such advance agreements can save time and frustration during an emergency (see Section 4).

9. Complete Internal Testing of WEA Operations

To ensure that your office and your staff are ready and able to issue WEA messages, you should test your WEA system and procedures. Federal regulations do not permit the issuance of WEA messages for test purposes by any authority other than FEMA, so you cannot perform end-to-end testing in which test alerts are disseminated all the way to the public. Instead, you should plan and perform testing internal to your organization, using the JITC Test Lab provided by FEMA. The Test Lab is an instantiation of IPAWS-OPEN in a configuration that is consistent with the production version of IPAWS-OPEN but is not connected to any CSMPs. As such, it duplicates the functions of IPAWS-OPEN, without the possibility of sending an actual alert to the public. Its purpose is to provide AOs with the ability to test their systems and practice their skills in an environment without the risk of inadvertently issuing a "practice" alert to the public.

Your testing activities should include the following:

- Practice your established operating procedures that define the activities your office will take when planning and sending a WEA message, including
  - exercising the process to decide to send a WEA message
  - exercising the WEA message approval process
  - exercising coordination activities with other organizations within your jurisdiction
  - exercising coordination activities with neighboring jurisdictions
- Practice accessing and using the software that you have chosen, including
  - establishing the correct message parameters (severity, urgency, etc.)
  - defining the correct geographic area
  - crafting a readable message within the 90-character constraints, if using the CMAMtext message generation option

  Perform this practice while connected to the JITC Test Lab, not IPAWS-OPEN.
- Verify your connections to IPAWS-OPEN. While it is not possible to fully verify your connection by sending a test message to IPAWS-OPEN, you can verify your ability to connect to

the IPAWS-OPEN production server through the use of IPAWS-OPEN administrative messages. Your alert software can generate a *getACK* request (ping) and, if there are no communication or authentication errors, IPAWS-OPEN will respond with a reply (pong).

10. Educate the Public About WEA

Conduct outreach to the public about WEA prior to deploying it. Outreach activities teach members of the public how to react when they receive WEA messages and may prevent people from opting out of WEA.

The IPAWS Program Management Office (PMO) has created public education products that are designed to ensure the American people understand the functions of the public alert and warning system and how to access, use, and respond to information from public safety officials. The PMO encourages public safety officials to take full advantage of these products and work, which include public service announcements specifically about WEA; a webpage (www.Ready.gov/alerts); and a 15-minute web-based training course, "IPAWS and the American People," which will be hosted by the Emergency Management Institute (EMI).

Find out if your state has created WEA materials that will suit your needs before you create your own. Often, the best and least expensive medium for conducting WEA outreach is the outlet that your organization already uses most to communicate with your constituents: press releases, TV and radio interviews, social media posts, website posts, and brief presentations at town hall and local civic group meetings.

Focus on creating audience-friendly materials and setting appropriate expectations about WEA. Address the questions people usually have about the service: What is it? Who issues WEA messages in my area? Will I have to pay to receive a WEA message? How is WEA different from subscriber-based Short Message Service alerts? What carriers and what mobile devices support WEA?

Include the date of WEA deployment in your jurisdiction, the types of events for which you will use WEA, areas where alerts will be issued, and how alerts display on mobile devices. You might also address privacy considerations, alerting frequency, and nighttime alerts. If your jurisdiction already receives NWS weather alerts or America's Missing: Broadcast Emergency Response alerts, research local media coverage and social media posts following alerts to learn how the public reacted and what questions they had.

Point the public to their CMSPs for further information about mobile device models that are WEA-compatible and what they need to do to receive WEA messages. Most large CMSPs provide some information about WEA, WEA-enabled mobile devices, and WEA opt-in/opt-out instructions on their websites (see www.ctia.org/wea).

Reinforce knowledge about your WEA capability whenever you conduct general alert-related or emergency event outreach with the public. This helps ensure that your constituents know what to do when they receive WEA messages.

Additional Resources

For more information concerning the activities of this checklist, see the following resources.

CTIA–The Wireless Association. *Wireless Emergency Alerts on Your Mobile Device*. http://www.ctia.org/consumer_info/safety/index.cfm/AID/12082 (2013).

Federal Emergency Management Agency. *Integrated Public Alert & Warning System. http://www.fema.gov/integrated-public-alert-warning-system (2013).*

Federal Emergency Management Agency. *Integrated Public Alert & Warning System Developer Webinar Archive*. http://www.fema.gov/calendar-events/integrated-public-alert-warning-system-developer-webinar-archive (2013).

Federal Communications Commission. *Wireless Emergency Alerts (WEA) Guide*. http://www.fcc.gov/guides/wireless-emergency-alerts-wea (2013).

Mileti, Denis S. & Sorenson, John H. *Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the Art Assessment.* Oak Ridge National Laboratory, 1990. http://emc.ed.ornl.gov/publications/PDF/CommunicationFinal.pdf

National Weather Service. *Wireless Emergency Alerts Capable: Weather Warnings on the Go*. http://www.nws.noaa.gov/com/weatherreadynation/wea.html (2013).

Public Outreach Examples Used by Alert Originators: [4]

- Baltimore, Maryland/Washington, DC, Region: http://www.erh.noaa.gov/lwx/WEA/WEA.php
- Calvert County, Maryland: http://www.co.cal.md.us/archives/51/CellAlerts062512.pdf
- Kansas City, Missouri: http://www.preparemetrokc.org/wea.asp
- New York, New York: http://www.nyc.gov/html/oem/html/pr/11_12_14_wirelessalert_test.shtml
- San Diego, California: http://www.sdcounty.ca.gov/Portal/News/2010/Aug/082410cmas.html
- Suffolk County, New York: http://www.suffolkcountyny.gov/Departments/FireRescueandEmergencyServices/OfficeofEmergencyManagement/ResolvetobeReady/GettingHelp.aspx

Software Engineering Institute. *Study of Integration Considerations for Wireless Emergency Alerts* (CMU/SEI-2013-SR-016). Software Engineering Institute, Carnegie Mellon University, 2013. http://techxferauth.sei.cmu.edu/library/asset-view.cfm?assetID=70063

[4] Some earlier publications use the term *CMAS* (Commercial Mobile Alert Service), an earlier designation for WEA.

3 WEA Training and Drilling Guide

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), enables authorized public safety officials to send geographically targeted text alerts to the public via commercial mobile service providers (CMSPs) using the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN).

This guide identifies the key steps that your agency should consider when preparing staff to use WEA. It is informed by training and drilling suggestions shared by IPAWS alerting authorities that have implemented WEA and focuses on establishing and improving your staff's knowledge and use of WEA. For the purposes of this document, the following definitions apply:

- **Training:** introducing staff to the value and capabilities of the WEA service, your agency's standard operating procedures (SOPs) for using WEA, and step-by-step instructions for using your agency's WEA message generation software to originate WEA messages
- **Drilling:** post-training activities focused on practicing, maintaining, and improving the WEA message origination knowledge and skills taught to your staff during training

Prepare for Training

As noted in the WEA Go Live Checklist (see Section 2), the initial steps of deploying WEA include establishing an alert generation capability (e.g., acquiring alerting software), receiving authorization to use WEA from FEMA, and establishing policies and SOPs within your agency. The following activities are prerequisites for developing training for your agency:

- authorization for WEA use received from FEMA
- installed and operational WEA (IPAWS-compatible) message generation capability
- familiarity with state-generated requirements, restrictions, and materials (if applicable)
- familiarity with FEMA's IS-247 training (required for at least one person in the agency to attain WEA authorization)
- WEA SOPs addressing the use of WEA established for your agency

Once these activities are complete, designate a training lead to create or acquire the training materials, assign the training delivery, identify all staff required to participate in the training, and oversee training management. Your existing WEA implementation lead may be the best person to serve as your training lead if he or she has the greatest familiarity with the prerequisites listed above.

Establish Goals for Training

The training lead, in coordination with agency leadership, should identify training baseline goals, which define the skills and knowledge that staff must acquire from training. Table 2 includes recommended minimum goals:[5]

Table 2: Goals and Objectives for WEA Training

Goals	Objectives
Understand the principles, benefits, and limitations of WEA	• Know the intents and purposes of WEA • Know the operating principles of WEA • Know the features and benefits of WEA • Know the limitations and constraints of WEA
Understand and be able to apply agency WEA SOPs	• Know when to send a WEA message • Know how to get approval to send a WEA message • Know how to determine the desired content of the WEA message, including secondary sources the public can access for more information • Know applicable security rules and practices
Possess the skills required to operate the WEA message generation software	• Know how to verify availability and operability of alert origination software • Know how to operate alert origination software to create and send an alert • Know how to verify submission of an alert

Identify Training Topics

FEMA's IS-247a online training course addresses several of the recommended goals. Consider requiring all training participants to complete this course. It provides a baseline understanding of IPAWS, including WEA. This baseline conserves training time to review the most essential elements of the course and focus on how your agency will apply the course information to your SOPs. It also enables participants to identify and address questions about IS-247 material together as a group on training day.

Training regarding your agency's SOPs is essential to ensure that staff members are confident in their understanding of your agency's intended use for WEA, as well as the capabilities and limitations of the system in your area. To accomplish these goals, design your training to address the following:

- **Your agency's alerting thresholds and how they align with FEMA's (IS-247) guidelines.** Address in depth the event types that your Collaborative Operating Group (COG) has permissions to issue alerts for per your Public Alerting Authority application, as well as general usage parameters or local emergency scenarios for which WEA use should be considered, as determined by your agency.
- **How WEA fits into your agency's alerting toolbox and interoperates with existing tools.** Address WEA's role in your overall communications plan for using multiple channels to inform the public.
- **Your agency's approval process for issuing a WEA message.** Include the decision tree for originating an alert, the specific approvers who authorize the alert, and time considerations or

[5] These goals address the operational aspects of WEA (e.g., alert authorization and alert generation). Separate training may be required for WEA administration to cover topics such as credential and certificate management, software updates, contingency plans in the event of failure or cyber attack, and so forth.

maximums for completing the process relative to the anticipation, onset, or conclusion of an emergency incident.

Training should also address alert dissemination factors, including carrier participation, geographic coverage, and alert display. Federal Communications Commission regulations do not mandate how WEA messages display on mobile devices; hence, different devices may display alerts in different formats. Training should include examples of WEA messages on several WEA-enabled devices to illustrate these differences. This will provide insights to staff about what is displayed to members of the public when they receive WEA messages. If possible, obtain the following information from the participating CMSPs operating within the jurisdictions:

- an approximate number of WEA-enabled mobile devices in the jurisdiction
- which carriers issue alerts at or below the county level
- where particular carriers' signals may be strong or weak

Share this information with the alert originators (AOs), as it may impact their decision to use WEA in particular circumstances. Educate staff about relevant border considerations for WEA (e.g., coordination with neighboring jurisdictions for emergencies that cross jurisdictional boundaries and bleed-over of alerts between neighboring jurisdictions).

Training must also address the operation of your agency's alert generation software. Staff should establish and exhibit proficiency in manipulating the WEA software and in developing and generating a WEA message. Staff should understand what types of WEA messages they will issue, cancel, or recall using the software and how to manipulate the software to do so.

Plan Training Management

Plan to provide training for all staff involved in WEA message generation, approval, and WEA software installation and maintenance. This will likely include your WEA message originators, executive staff with WEA message approval responsibilities, and IT staff who maintain your software. Including executive staff provides them with a well-rounded understanding of WEA capabilities, the alert origination process, and how approvals fit into this process. Including IT staff helps them understand the impact of any changes to your agency's WEA software or interface to the alert origination process.

Track efficacy and sufficiency of training against established WEA performance targets, and share the results with training participants. Targets should address factors such as alert origination speed, event confirmation requirements, and message content (e.g., data inclusions and accuracy, message clarity, voice, grammar, and spelling). Determine how these factors will be measured, which targets must be met on training day, and which targets can be met later during drilling.

Deliver Training

Several IPAWS public alerting authorities that have completed their own WEA training have indicated that a half-day training session is sufficient for meeting the recommended goals. They have also indicated that the training lead should create or compile the materials described in Table 3 in advance of training.

Table 3: Materials for WEA Training

WEA Training Manual	A comprehensive training manual that provides an overview of WEA and how your agency will use it; the manual should feature key IS-247 data that aligns with your agency's training goals, WEA SOPs, any WEA message templates, scenarios for using WEA, and relevant content from state-generated materials, if applicable.
WEA Software Guide	A step-by-step guide to using your WEA message origination software; the guide should include screenshots of each step of the process and align with the training manual's guidance.
WEA Reference Guide	A quick reference guide to be placed at alert origination terminals after training; during training, introduce staff to this resource, which should be a condensed hybrid of the training manual and software guide and feature essential SOPs, step-by-step instructions, and screenshots.

The ideal training session will focus on a combination of meeting the recommended goals and objectives as well as a practical application in the training session. Consider organizing your training session into five topics.

Topic 1 – WEA Basics: Focus the first section of training on developing an understanding of the principles, benefits, and limitations of WEA.

Topic 2 – WEA SOPs: Focus this section on presenting the concepts of your SOPs. Recognize that WEA messages are likely to trigger queries for additional information from the public; address how WEA fits into your agency's overall communication and emergency management strategies; and discuss governance issues regarding cross-jurisdiction coordination, roles, and responsibilities.

Topic 3 – Software Instruction: Focus this section on developing the skills required to create an alert. Use your WEA Software Guide to train participants on the use of your alert generation software to issue the alert types relevant to your WEA SOPs. Also address the creation and use of message templates (if applicable), cancellation of alerts, and update of alerts. Consider asking your software vendor representatives to assist in preparing and presenting this section if your agency acquired software to issue WEA messages.

Topic 4 – Practice: The fourth section should provide participants with the opportunity to reinforce, apply, and practice the knowledge and skills acquired during the first three portions of the training. Designing this section to incorporate tabletop exercises allows staff to become comfortable with applying your WEA guidelines and provides an opportunity to share questions, answers, and recommendations as a group. Allow participants to walk through the steps of vetting events that require a WEA message; generating alerts using the software and existing templates, if applicable; going through the approval chain; and even taking steps to cancel or update the alert. If practical, offer participants the opportunity to practice using your alert generation software (see the "Drilling" section of this guide). Note what is and is not working well, and use it to inform your drilling processes. Introduce your agency's WEA performance targets, and discuss the drilling process that you will use to assess and improve performance.

Topic 5 – Assessment and Evaluation: Assess the efficacy and impact of the training. Assess participants' baseline performance against the targets using one or more of these methods:

- **Assessment:** Participants complete a brief assessment at the beginning and end of the training session to determine their knowledge and proficiency of the material addressed.
- **Participant Feedback:** Participants provide their reactions and recommendations to the training through a brief feedback survey conducted at the end of the training.

Participants may also take a survey approximately one month after training to determine the results of the training in terms of organizational impact.

Additional Training Considerations

1. External resources, such as the Joint Interoperability Test Command (JITC) Test Laboratory, are available to help you train staff. Basic information about the test laboratory is provided in a Resources list at the end of this section. Consult with FEMA and your IPAWS-compatible software provider regarding this option.
2. Hands-on WEA training of multiple staff members is likely to produce many questions as well as some possible suggestions for improvements to training materials, SOPs, or related resources and processes. Task someone in the training room with capturing the main conversation points, questions and answers, action items, and suggested or agreed-upon improvements to resources and processes. After the training, share this data and resulting outcomes with the training participants.
3. The best time to establish future and ongoing WEA training requirements and processes is at the time you plan and execute your first WEA training, for example:
    - **Ongoing:** Consider identifying the owner, process, and time frame to train new staff members who join your agency in the future. You will need to train new staff eventually, so consider designing the training to be conducive to both live classroom training and self-study. For example, creating a video recording of the training session and providing it to new employees with the training materials may be more efficient than conducting follow-up classroom training sessions in the future.
    - **Annual:** Consider coupling the annual IT compliance requirement stipulated in your IPAWS memorandum of agreement with an annual training refresher to review any changes that your agency makes to WEA SOPs, software, or performance targets. Consider requiring staff to retake the IS-247 course to stay current on any recent changes to FEMA's guidance, parameters, and capabilities.

Drilling

WEA drilling activities should focus on maintaining, increasing, and verifying staff's knowledge and proficiency in using the skills acquired from training. Initiating ongoing drilling immediately after training can ensure that new knowledge stays fresh. In addition to maintaining skills, drilling also can identify opportunities for improvements to SOPs, WEA message templates, and other WEA assets.

Executive staff, together with your training lead, should determine the best staff resource to direct your agency's drilling activities. Once selected, your drilling lead should identify your agency's drilling participants, including all WEA message originators, alert approvers, and others directly engaged in issuing alerts. Keep IT staff informed of problems or suggested revisions that arise from drilling on the WEA software. Consider organizing the drilling process into three steps:

Step 1 – Plan: Starting with your agency's WEA performance targets, SOPs, alerting software usage instructions, training day assessment data, and training materials, develop a drilling plan. The plan should focus on assessing and improving performance as specified by your agency's

performance targets. Drilling may focus on improving factors such as authorization, origination, and connection:

- **WEA authorization process:** Practice using your SOPs by executing the process to approve an alert for a simulated emergency. Monitor the time between initial reporting of the emergency and the time when the issuance of an alert is authorized.
- **Alert origination process:** The drilling objective is to practice generating and submitting an alert request to IPAWS-OPEN. Your abilities to practice this task without incurring the risk of inadvertently issuing a public alert depend on the support provided by your alert origination software. Typically, alerting software is configured to communicate with IPAWS-OPEN. FEMA has entered into an agreement with JITC[6] to support the JITC Test Laboratory (JTL). The JTL is an alternative instantiation of IPAWS-OPEN available to AOs for testing and drilling. The JTL interacts with AOs in the same way that the IPAWS-OPEN production environment does; however, it does not disseminate alerts to the public through CMSPs.
  - Some alert origination software supports drilling and testing using the JTL. These systems enable you to direct your messages either to IPAWS-OPEN for actual alert generation or to the JTP for practice. The system clearly displays which mode is selected to mitigate the risk of inadvertently issuing an alert while in practice mode. When connected to the JTL, you can practice using the software to create CAP messages and send them to the JTL for evaluation and processing. This activity supports testing proficiency of both the alert creation process and alert generation software use.
  - Some alert origination software does *not* support drilling and testing using the JTL. While nearly all commercial software solutions can be retargeted to deliver messages to the JTL rather than IPAWS-OPEN, some require administrative privileges to do so. Furthermore, if the software does not provide a clear indication of its current target, operators could become confused and not know if they are connected to IPAWS-OPEN or the JTL. This creates a risk of inadvertent alert issuance during practice sessions.
    It may also be tempting to use your alerting software in its active mode (i.e., connected to IPAWS-OPEN) and simply stop the alert generation process before sending the message to IPAWS. This is unadvisable, again due to the risk of inadvertently issuing an alert during the practice session. If your software does not thoroughly support drilling using the JTL, you may have to practice alert generation offline (e.g., using desktop exercises and crafting messages on your computer using other applications such as text processors or email applications). Ask your software supplier for recommendations for drilling and practice.
- **IPAWS-OPEN connection:** Verify that you have an active connection to IPAWS-OPEN. Use your alert generation software to generate a *getACK* request (ping) and, if there are no communication or authentication errors, IPAWS-OPEN will respond with a reply (pong).

When practicing alert generation, factors to assess include speed, geo-targeting accuracy, and message accuracy. Simply measure speed as the time between the authorization to send an alert

[6] JITC is a division of the Defense Information Systems Agency within the U.S. Department of Defense. JITC maintains and operates an instantiation of the WEA service accessible by AOs for training and testing purposes.

and the time when the CAP message is ready to be sent to IPAWS-OPEN. Geo-targeting accuracy is a comparison between the targeted area for message delivery and the specified area contained in the CAP message. Evaluation of message accuracy depends on the process that your agency uses to generate the message.

In the default mode of operation, the AO provides data in the CAP fields defining Urgency, Severity, Certainty, Event Code, Expiration, and Response Type. IPAWS-OPEN automatically constructs the alert as a standard combination of phrases derived from these data inputs. In these cases, your agency does not control the structure of the message. See Table 4 for examples.

Table 4: IPAWS-OPEN Constructs Alerts from Cap Fields

CAP Field	Content	Alert Result
Urgency	"Immediate" or "Expected"	Required to issue a WEA message
Severity	"Extreme" or "Severe"	
Certainty	"Observed" or "Likely"	
Event Code	FRW	WEA Message "Fire Warning In this area Until 4:49 PM Evacuate now"
Event Category	Fire	
Expiration	2013-02-12T16:49:00-05:00	
Response Type	Evacuate	

However, some state authorities have granted a number of AOs the option to enter a free-form, 90-character message known as "CMAMtext."[7] In these cases, it is important that alert originators carefully craft an understandable and accurate message. Evaluate the resulting message for accuracy, clarity, voice, grammar, and spelling.

Step 2 – Drill: The rhythm and processes established for WEA drilling depend primarily on your staff's performance against established WEA performance targets. However, the frequency of actual alert issuance also plays a role. If you use WEA less frequently, you may need to perform more drilling to maintain needed proficiencies. Use the results of your drills to determine drill frequency. If WEA performance targets are not being met, more frequent or more comprehensive drills may be indicated. If WEA performance targets are being surpassed, less drilling may be needed.

Step 3 – Assess and Upgrade: Assess your WEA performance based on the data collected from your drills. If performance deficiencies are noted, examine your drills and drilling processes to identify needed improvements (e.g., more frequent drills, new drilling topics). To perform more comprehensive and productive assessments, collect feedback from the drill participants. Ask them for suggestions to improve both training and drilling. Identify opportunities for intersection with other drilling processes that your agency currently employs. For example, if you drill for Twitter or SMS-based alerts, consider incorporating WEA drilling into existing processes if it increases efficiency and still enables staff to meet WEA performance targets. Consider consulting the Homeland Security Exercise and Evaluation Program (HSEEP) for guidance if you plan to apply for grants to fund your activities.

[7] Check with FEMA to determine if your COG is authorized to use CMAMtext.

Conclusion

The WEA Training and Drilling Guide serves as a resource for establishing and building your staff's knowledge and use of WEA. We wish to thank the emergency management agencies that informed this guide with their own WEA training and drilling insights and activities.

Many additional resources exist to inform and supplement your agency's design and execution of WEA training and drilling processes. The following section suggests several such resources.

Additional Resources

Your agency may benefit from consulting more resources that provide guidance regarding the WEA implementation process, an environment and support for completing training and drilling activities, as well as standardized emergency management training and drilling instruction.

- The ***WEA "Go Live" Checklist*** identifies key steps that agencies should perform prior to implementing WEA. It provides high-level guidance for conducting each step of the implementation process as well as how training and drilling fit into this process. See Section 2.
- ***Wireless Emergency Alerts New York City Demonstration*** describes the adoption of WEA by the New York City Office of Emergency Management (NYC OEM). The document provides readers with some insights into how NYC OEM designed its own training and drilling practices as part WEA adoption. The document can be found at http://techxferauth.sei.cmu.edu/library/asset-view.cfm?assetID=70024.
- A special IPAWS test environment has been established at the **Joint Interoperability Test Command (JITC) Test Lab.** AOs and software developers may access the lab to test their systems offline in an environment that functions with alert origination software the same way that the IPAWS production environment does. The JITC lab offers simulated Emergency Alert System (EAS) alerting capabilities and the ability to test with WEA using a "toy cell" that can send WEA messages to WEA-enabled mobile devices located within the lab. During testing, the lab can be set up to restrict COGs to their current IPAWS permissions, or AOs can experiment with alerting outside their permissions on the IPAWS production site. Contact FEMA IPAWS directly for additional details regarding participation in the JITC Test Laboratory at ipaws@dhs.gov.
- The **Homeland Security Exercise and Evaluation Program (HSEEP)** is a capabilities- and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning. Local, state, and federal agencies often require training and drilling processes to be HSEEP compliant in order to qualify for grant funding. If your agency is considering applying for a grant to fund your WEA training or drilling activities, consult the HSEEP site early in your planning process: www.llis.dhs.gov/hseep.
- DHS has created a **Lessons Learned and Information Sharing (LLIS)** network to collect and disseminate best practices identified during exercises and actual incidents. Exercise planners are encouraged to share their lessons learned and best practices on this secure network. LLIS resources and information can be found at www.llis.dhs.gov.

4 WEA Governance Guide

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), is a national capability that enables authorized public safety officials to send geographically targeted text alerts to the public via commercial mobile service providers (CMSPs) using the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN).

The *WEA Governance Guide* identifies key steps that an emergency management agency (EMA) should consider when using or preparing to use WEA.

What is governance?

Governance is a framework of processes, organizational rules, communications protocols, and behavioral standards that enables 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. Each EMA that uses WEA will need to answer some fundamental questions about WEA governance:

Governance Issues

1. When should EMAs issue a WEA message?
2. Who is responsible for issuing a WEA message?
3. Who should EMAs consult or inform before they issue alerts?
4. How can EMAs communicate alerts effectively?

1. What circumstances warrant a WEA message?
2. Who is responsible for issuing an alert?
3. Who should the EMA consult and/or inform before issuing an alert?
4. How can the EMA communicate the alert effectively?

Why is WEA governance necessary?

Effective alerting requires the dissemination of clear, unambiguous information to the intended members of the public. WEA governance is necessary to ensure coordination between participating alerting agencies to satisfy this requirement. As more and more alerting agencies adopt WEA, governance becomes more critical for several reasons:

1. Emergencies do not respect jurisdictional boundaries. Many emergencies span multiple jurisdictions, or they may originate in one jurisdiction but have impacts in neighboring jurisdictions.
2. Currently, WEA geotargeting resolution is equivalent to the broadcast range of cell towers in the jurisdiction. This means that an alert for a specified area may "bleed over" into surrounding areas, reaching recipients who are within range of the cell tower but outside of the specified alert area.
3. Overlapping jurisdictions—such as counties within a state and municipalities within a county—are common in the United States and complicate the process of public alerting. Even within a single jurisdiction, multiple agencies such as the municipal police department, fire

department, county EMA, and National Weather Service (NWS) all may have authority to issue public alerts, including WEA messages.

These factors contribute to the challenge of getting the right message to the right people at the right time. Effective governance reduces the likelihood that the public will receive irrelevant, contradictory, or redundant alerts.

What circumstances warrant a WEA message?

Per FEMA guidelines, an event must meet three specific criteria before an EMA should issue a WEA message.

1. Urgency: The event urgency must be classified as either *immediate*, requiring immediate responsive action, or *expected*, requiring responsive action within one hour.
2. Severity: The severity of the event must be classified as either *extreme*, posing an extraordinary threat to life of property, or *severe*, posing a significant threat to life or property.
3. Certainty: The certainty of the event must be classified as either *observed*, determined to have occurred or to be ongoing, or *likely*, determined to have a probability of occurrence of 50% or greater.

These criteria set the minimum threshold for the issuance of an alert. However, EMAs may wish to consider additional factors in the process of deciding to issue an alert. These factors, among others, may be relevant to the decision:

- Geographic location and geographic breadth of the event: How does the area affected by the event relate to the area that will receive the alert?
- Time of day: Should the EMA consider the time of day when the alert is issued?
- Number of recent WEA messages issued: Is there a possibility that the public will experience "alert fatigue" due to recent alerting activities?
- Complexity of the required response: Can the EMA clearly communicate the response required of the public within the constraints of the WEA message?

EMAs should consider various scenarios addressing these and other issues and develop guidelines and policies for when to issue a WEA message.

Who is responsible for issuing an alert?

Multiple agencies (e.g., federal, state, county, municipal) may be authorized and equipped to issue alerts in an area. When an emergency occurs, EMAs have no time to waste on deciding who has responsibility to issue the alert. All concerned agencies should determine responsibility in advance and agree to clear rules of engagement. Some of this determination is done when the EMA applies for alerting authority, which defines the geographic extent of the authority and the types of alerts authorized. But in some cases, further delineation is needed. EMAs may employ various methods for defining these rules of engagement.

In many cases, EMAs can use the type of event to designate the appropriate alerting agency. For example, responsibility for alerts involving fire or explosion (i.e., alerts issued with the Fire Warning [FRW] event code) may be assigned to the local fire department. Alerts involving police matters (i.e., alerts issued with the Law Enforcement Warning [LEW] or Civil Danger Warning

[CDW] event codes) may be the responsibility of the local police department. Weather-related alerts may be designated as the responsibility of the NWS.

Geographical jurisdiction is another factor influencing responsibility. Agencies using WEA will have an alerting jurisdiction defined in their memorandum of agreement (MOA) with FEMA. The MOA permits them to issue alerts only within this jurisdiction. Hence, they should not issue alerts for events that are not relevant to the defined jurisdiction. In cases where an event (e.g., a wild-fire) spans multiple jurisdictions, it may be necessary for multiple agencies to issue alerts, each intended for its own specific jurisdiction. In these cases, coordination of alerts is imperative to ensure clear, consistent, non-contradictory messages. This is particularly important in the face of message bleedover between jurisdictions, where the public in one jurisdiction may see alerts from neighboring jurisdictions (see Figure 1). The WEA service provides an internal COG-to-COG communication capability that can support this communication.

Regardless of how agencies choose to divide alerting responsibilities within their regions, it is imperative that they agree on and codify this division before circumstances warrant a WEA mes-sage.

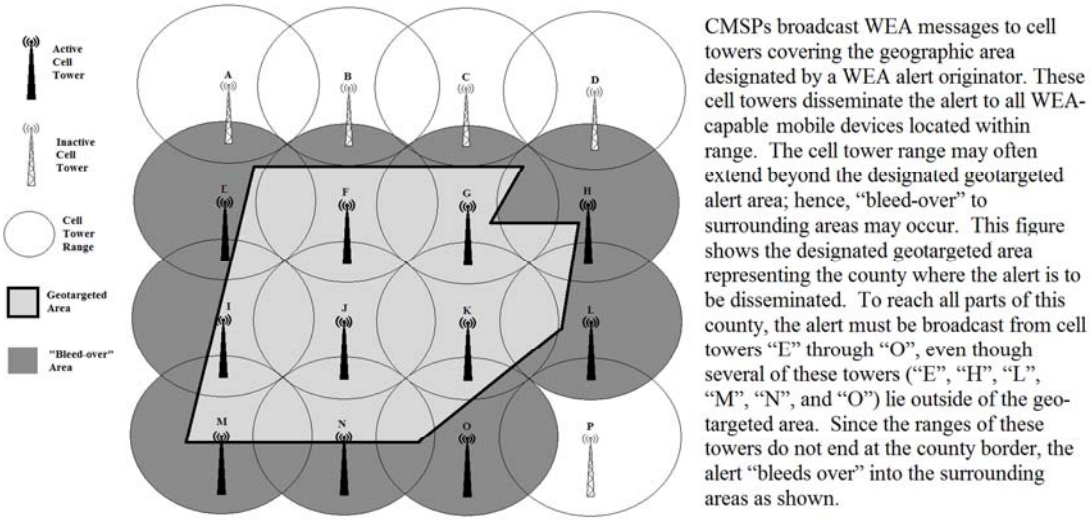

Figure 1: WEA Message Bleedover

Who should EMAs consult or inform before issuing an alert?

Even with defined responsibilities between AOs in a region, interagency communication during the alerting process remains essential. When an agency issues or plans to issue an alert, it should notify surrounding or overlapping jurisdictions of the alert and the events prompting it. This ena-bles agencies in neighboring jurisdictions to decide whether or not to propagate the alert so that related alerting activities can be coordinated and consistent. Notification also makes neighboring agencies aware of alerts that might bleed over into their jurisdictions. This knowledge enables them to prepare for public inquiries that may come to their offices.

When issuing a WEA message, an agency should also address alternative information sources available to the public. The limited size (90 characters) of a WEA message precludes the possibil-

ity of including detailed information in the alert. EMAs should use other communication mechanisms (e.g., the EMA's Facebook page, Twitter account, or website) to supplement the alert information. Thus, it is important for the AO to notify the personnel and departments within the EMA who hold responsibility for these channels that an alert has been issued.

How can EMAs communicate alerts effectively?

Formal or informal agreements among AOs in a region can improve alerting effectiveness. Many events will not affect an entire county; however, at this time WEA standards do not require CMSPs to geotarget any area smaller than a county. Therefore, to issue an alert for a localized event, an EMA may have to alert the entire county.[8] As county residents receive alerts that are not relevant to them, over time this could result in alert fatigue, as the recipients become desensitized to the alerts. While it is not currently possible to change this geotargeting resolution, it is possible to mitigate the effects of irrelevant alerting through the content of the alerts.

As shown in Table 5, the default WEA alert format offers little specificity of the geographic area description within the text of the alert. WEA offers an alternative message composition method called CMAMtext,[9] which provides AOs with more flexibility to create alerts. In these cases, it is possible to be more specific (within the 90-character message limit) regarding the area affected by the event. So, even though the alert may still be distributed to the entire county, the alert content now makes clear who should respond.

Table 5: Alert Message Formats

Default WEA Format	**Alternative CMAMtext Message Content**	
Fire Warning **In this area** Until 4:49 PM Evacuate now Pgh Fire Dept	Fire Warning **in ZIP 12345** Until 4:49 PM Evacuate now Pgh Fire Dept	Fire Warning Until 4:49 PM Evacuate **MAIN ST. from 1ST to 3RD AVE** now Pgh Fire Dept

Language is another factor influencing alert content. Many geographic areas have significant non-English-speaking populations. For these areas, AOs may desire to issue alerts in alternative languages. Again, AOs cannot do this using the default WEA message formats but can use another language with the CMAMtext alternative.

Agreements among AOs in the region regarding alerting protocols and consideration of language issues will help maximize the effectiveness of alerting.

When should EMAs address governance?

Regardless of where you are in the process of adopting WEA, the best time to sow the seeds for effective WEA governance is *now*. Reach out to

- all alerting agencies within your jurisdiction (municipality and county)

[8] While many CSMPs are voluntarily prioritizing alert dissemination to polygon-defined geographic areas, alerting authorities must prepare for county-wide alert dissemination, as some CSMPs may choose to map a polygon definition into county FIPS codes.

[9] Some state authorities have granted a number of AOs the option to enter a free-form, 90-character message known as "CMAMtext." Check with FEMA to determine if your COG is authorized to use CMAMtext.

- neighboring county emergency managers
- your state-level alerting officials and/or state emergency management agency
- your local NWS office

These conversations can help you understand WEA use or plans for use in your immediate geographic area. They can also serve to inform your decision to adopt WEA and support defining the scope of your alerting authority when completing FEMA's Application for IPAWS Public Alerting Authority.[10] For example, within a single county, one may find both municipal-level and county-level emergency managers who wish to apply for IPAWS alerting authority. Alerting for all weather-related emergencies may be reserved for the local NWS office, and America's Missing: Broadcast Emergency Response alerting may be reserved for a designated state emergency management agency. Should your governance conversations lead to a similar determination, contact the FEMA IPAWS office for recommendations on the best approach to address this particular scenario.

How can EMAs establish effective governance?

A clear governance process and formalized governance structure provide a unified approach across multiple jurisdictions and disciplines that can aid the effectiveness, efficiency, and overall support of WEA. Establishing a regional governing body is helpful in addressing the key challenges of WEA. Such a governing body provides the framework in which stakeholders can collaborate and make decisions that reflect a common objective. The suggested process for establishing a WEA-related governance entity is presented below.

Step 1: Identify a *champion and key players to participate.* The collaborative approach to governance calls for identification of the key participants from all jurisdictions and disciplines that have a stake in WEA-related issues. This approach helps assure balanced representation. Ultimately, decisions about who should be included will reflect local political, geographic, and fiscal considerations. However, the optimal governance approach should strive for balance among a variety of organizations such as those involved in local and regional emergency management, firefighting, and law enforcement.

Step 2: Establish and validate a governance process and plan. The key players will need to develop a process and a plan to identify goals and address issues. To define the best governance structure, the right people and leaders must be identified, involved, and committed to working toward consensus and optimal solutions that affect the entire region, not only their respective agencies.

Step 3: Develop a governance charter. A charter defines the conditions under which a body is organized and defines its rights and privileges. Defining a governance charter will help determine relationships and roles and help members understand how their roles fit into the overall effort.

Step 4: Conduct regular meetings to identify and address issues. Once the representatives have established the formal governing body, they should determine the frequency of regular

[10] The *WEA "Go Live" Guide* provides a high-level overview of 10 recommended steps that you should perform prior to implementing WEA in your jurisdiction (see Section 2).

meetings. The WEA-related issues that members have identified will drive the purpose, outcomes, and agenda for each meeting. These meetings can serve as a forum for sharing processes, policies, and experiences among member agencies.

Step 5: Implement decisions. Outcomes from regular meetings of the governing body will include achieving consensus regarding WEA-related issues. Once the governing body has made a decision, it will identify both actions and action owners to drive toward accomplishment. The governing body must communicate all decisions to the affected stakeholders in a timely fashion.

What is an appropriate governance structure?

Based on the evaluation of governance models used in several different localities and states, we have found that successful governance models employ three groups and have provisions for administrative support. This three-tiered governance model encourages partnerships with other relevant organizations.

1. *An oversight body* or *executive committee*, composed of key representatives with funding authority, should be vested with final decision-making authority. Ideally, one appointed representative and one alternate from each participating jurisdiction or agency take part. The charter should specify how often the executive committee meets; meeting quarterly is the recommended minimum.
2. Leadership will benefit from *a committee* that includes an equal number of representatives from each participating jurisdiction or agency. The committee should meet regularly. The group can work with the executive committee to prioritize implementation tasks and develop a roadmap for the future or a project plan.
3. Temporary, narrowly chartered *action teams* should be formed for specific tasks, such as conducting research and collecting data. These action teams would have no voting powers and would disband upon the completion of the chartered tasks.

Additional Governance Principles and Considerations

Some key guiding principles for setting up a governance structure can help to promote the highest degree of collaboration, effectiveness, and efficiency:

1. *Work from the bottom up.* A successful governing body relies heavily on local and state public safety practitioners for input and guidance as it works to define and implement processes.
2. *Seek the strongest possible sponsorship.* Strong sponsorship, at the highest possible levels, helps ensure that the governance structure has the necessary authority to govern.
3. *Establish and articulate a shared understanding of goals.* A shared vision is the foundation of any effective undertaking, while common goals provide momentum to move forward and maintain commitment to the group.
4. *Promote shared decision making, while maintaining accountability.* Strong leadership and clearly defined roles and responsibilities are essential to achieving an effective balance.
5. *Promote transparency*. The membership, operations, charter, and actions of the governing body must be clearly articulated and understood, not only within the entity itself but also among the greater alert and warning community. As responsibilities within each governance structure may shift, clarity and transparency will help smooth the path forward.

6. *Promote sustainability.* The governing body should build succession planning and membership rotation into the governance structure.
7. *Stay flexible.* Working processes, roles, and responsibilities are likely to evolve over time. As the needs and goals of the group shift, so will the attendant roles. Be prepared to revisit policies and procedures periodically to ensure effectiveness and relevance.
8. *Actively and continually engage stakeholders.* The governance structure should represent the full range of interests to ensure that solutions are responsive to community needs and incorporate diverse perspectives. As the interests may shift, the active engagement of diverse stakeholders with an investment in the issue is also paramount.

Conclusion

The *WEA Governance Guide* serves as a resource for establishing consensus on the rules of engagement among alerting authorities in your geographic region. Such consensus will promote effective use of WEA and avoid irrelevant, contradictory, or redundant alerts.

5 WEA Cybersecurity Risk Management Strategy

The Wireless Emergency Alerts (WEA) service depends on information technology (IT)—computer systems and networks—to convey potentially life-saving information to the public in a timely manner. However, like other cyber-enabled services, the WEA service is susceptible to risks that may enable an attacker to disseminate unauthorized alerts or to delay, modify, or destroy valid alerts. Successful attacks on the alerting process may result in property destruction, financial loss, infrastructure disruption, injury, or death. Such attacks may damage WEA credibility to the extent that users ignore future alerts or disable alerting on their mobile devices.

To assure that their WEA capability is robust and resilient against cyber attacks, alert originators need an effective strategy for managing cybersecurity risks that considers the following questions:

1. What is the WEA alerting process; that is, what assets—such as procedures, personnel, and technologies—will alert originators use to create and disseminate messages?
2. What vulnerabilities exist—in alerting procedures, personnel, IT policies, and systems—that increase the susceptibility of the WEA capability to an attack?
3. Which of these vulnerabilities introduce critical cybersecurity risks, as determined by the potential impact and the probability that the risks will be realized?
4. How can alert originators mitigate the risks associated with critical vulnerabilities?

This guide presents a cybersecurity risk management (CSRM) strategy that alert originators can use to assess and manage cybersecurity risks throughout WEA adoption, operations, and sustainment. The strategy, illustrated in Figure 2, consists of four stages that address the questions above: Prepare for cybersecurity analysis of the WEA alerting process, identify cyber threats and vulnerabilities, assess and prioritize cybersecurity risks, and mitigate cybersecurity risks. Alert originators should repeat the activities of each stage as needed to address changes in the WEA alerting process, for example, in operational procedures, technology, the cyber-threat environment, and staff roles and responsibilities. The strategy is directed, planned, and executed through the alert originator's governance structure, organizational processes, and operational mechanisms.

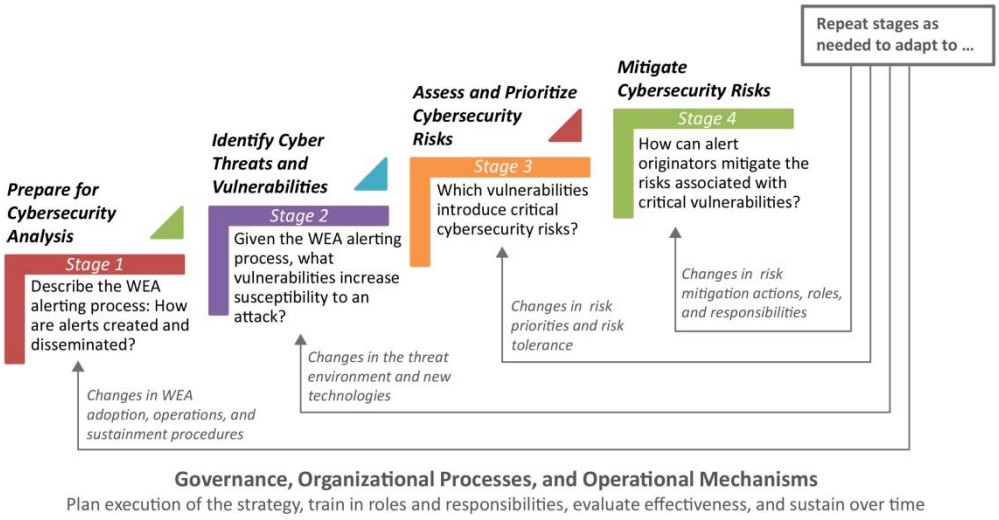

Figure 2: A Four-Stage CSRM Strategy for the WEA Service

Stage 1: Prepare for Cybersecurity Analysis

Question: What is the WEA alerting process; that is, what assets—such as procedures, personnel, and technologies—will alert originators use to create and disseminate messages?

In responding to this question, alert originators describe the step-by-step process that they use to generate and disseminate an alert. Table 6 shows a sample result.

Table 6: Example of Alerting Process Steps

Step	Example Step Description
1	First responder contacts local alerting authority with information about an event that qualifies for a WEA message.
2	Local alerting authority (person) determines call or email is legitimate.
3	Local alerting authority instructs alert origination system (AOS) operator to issue an alert using information provided by first responder (the alerting authority and AOS operator may be the same person).
4	AOS operator attempts to log on to access the WEA service.
5	AOS logon activates auditing of the operator's session.
6	AOS operator enters alert, cancel, or update message.
7	AOS converts message to Common Alerting Protocol (CAP)-compliant format required by Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN).
8	Two authorized persons sign CAP-compliant message.
9	AOS transmits message to IPAWS-OPEN.
n	…

Recommended participants in developing the process description include AOS operations personnel and IT staff. The final process description will reflect the alert originator's environment in sufficient detail to expose the assets (technology, personnel, facilities, and information) used in each step, enabling a targeted, thorough analysis of cyber threats and vulnerabilities.

Stage 2: Identify Cyber Threats and Vulnerabilities

Question: What vulnerabilities exist—in alerting procedures, personnel, IT policies, and systems—that increase susceptibility of the WEA capability to an attack?

In Stage 2, alert originators analyze the step-by-step alerting process documented in Stage 1, listing the assets needed to execute each step. Next, they examine the technology assets, policies surrounding their use, and interfaces with other systems to expose threats and vulnerabilities that would enable a cyber attack. A *threat* is any circumstance, event, object, or human with a potential to negatively impact organizational operations or otherwise cause harm; a *vulnerability* is a weakness in design, implementation, operational procedures, or controls that makes an organization susceptible to exploitation by a threat [CNSS 2010, NIST 2013].

Table 7 illustrates the process of identifying cyber threats and vulnerabilities for a single step in the alerting process. This example uses the STRIDE threat classification scheme: spoofing (S), tampering with data (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privilege (E) [Microsoft 2005, Howard 2006].

Table 7: Example of Threat and Vulnerability Analysis

Step	Example Step Description	Example Assets	Example Threats*	Vulnerabilities
4	AOS operator attempts to log on to access the WEA service.	• One person • Server (authentication) • Username and password database • Logon procedure • Logon application • Communications between software, server, and AOS	**S** Unidentified individual attempts to log on using alert originator credentials **T** Attacker modifies logon database **R** AOS operator denies having logged on **I** Logon data captured by key logger or packet sniffer **D** AOS operator's account inaccessible or servers down **E** Super-user privileges granted in error	• Unprotected passwords • Unprotected databases • Audit logging not enabled or audit files not protected • Unauthorized applications on alerting system • Alerting system accessible through public-facing networks

* S: spoofing; T: tampering; R: repudiation; I: information disclosure; D: denial of service; E: elevation of privilege.

In addition to analyzing the alerting process, the alert originator should review policies governing the use of assets and permissible interconnections between these assets. Such policies are often incompletely specified or unevenly implemented, leading to vulnerabilities that make the assets easy prey for an attacker. For example, if a website that provides emergency information to the public is not isolated from critical assets used in alerting, an attack on the website could compromise the alerting system. As another example, failure to change default passwords on equipment can expose an organization to attack. Figure 3 illustrates examples of some common attack methods used by adversaries and the vulnerabilities that enable them.

Figure 3: Attack Methods and Enabling Vulnerabilities

Participants in threat and vulnerability identification include operations, IT, and facilities personnel as well as cybersecurity experts with a solid understanding of typical attack methods and vulnerabilities. An alert originator may either draw on internal resources for cybersecurity expertise or seek assistance from external consultants.

Stage 3: Assess and Prioritize Cybersecurity Risks

Question: Which of these vulnerabilities introduce critical cybersecurity risks, as determined by the potential impact and the probability that the risks will be realized?

Because of IT and network complexity, the rapid pace of change in software and hardware technology, and organizational resource constraints, it is impossible to find and eliminate all vulnerabilities in a service such as WEA. Therefore, it is essential to determine which vulnerabilities introduce the greatest levels of risk.

In Stage 3, the alert originator, working with internal or external cybersecurity experts, analyzes threats and vulnerabilities identified in Stage 2, transforms them into distinct statements of risk, and evaluates the risks in terms of the *probability* that they will enable a successful attack and the *impact* of that attack on their ability to create and disseminate alerts. This process helps alert originators determine the most critical vulnerabilities, so they can prioritize mitigation actions and resources accordingly, focusing the most attention on risks that have a potential impact too great to ignore. Figure 4 illustrates the relationship between threats, vulnerabilities, and consequences; risk probability and impact; and risk exposure.

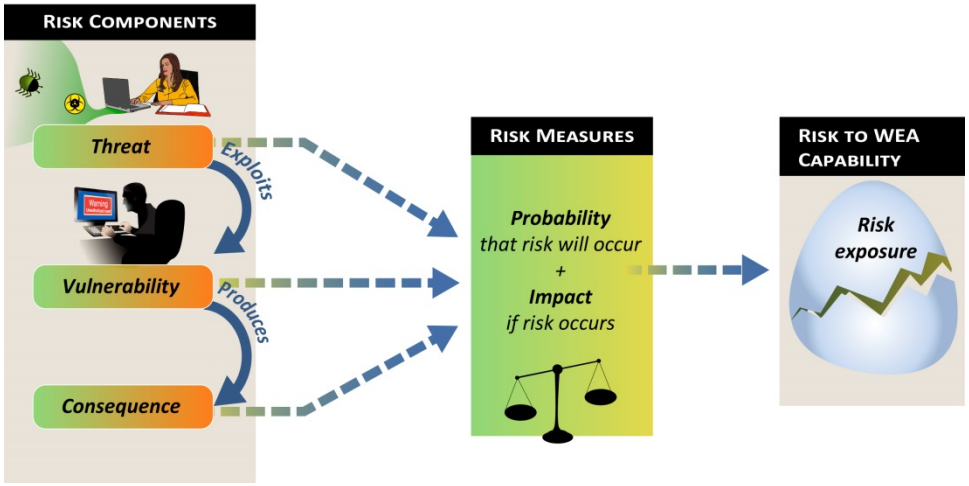

Figure 4: Deriving Critical Cybersecurity Risks from Threats and Vulnerabilities

For example, several steps in the alerting process may be susceptible to failure due to a denial-of-service threat (D in the STRIDE classification) caused by malicious code: An operator may be locked out when attempting to access the system; the software that processes alert inputs may be corrupted; or a server running the software or user validation code may be unavailable. Vulnerabilities that enable a denial-of-service attack include IT resources that are not adequately isolated from unauthorized access, failure to protect account information and credentials, and allowing the unrestricted use of external media, such as universal serial bus (USB) flash drives. Consequences include any negative effects that may result when a threat successfully exploits a vulnerability.

From this information, the alert originator can articulate the risk as follows: *If malicious code (installed due to a vulnerability) prevents an operator from entering an alert into the AOS (denial-of-service threat), then health, safety, legal, financial, and productivity effects could result (types of consequences—the alert originator would replace these with specific consequences).*

Next, the alert originator assesses the probability that this risk will be realized and the impact if it is. For this example, the terms *low*, *moderate*, and *high* characterize both probability and impact. If the current set of precautions is appropriate, this risk will have a low probability of occurrence, but in a lax security environment, this risk's probability will be moderate or perhaps even high. Similarly, if malicious code is installed, the impact will be low if the organization has alternative means for disseminating alerts, and moderate to high if not. Since this type of risk applies to several steps in the alerting process, it makes sense to identify the appropriate precautions, or mitigation actions, that will reduce the associated vulnerabilities and nullify future threats.

Stage 4: Select and Execute Risk-Mitigation Actions

Question: How can alert originators mitigate the risks associated with critical vulnerabilities?

Once cybersecurity risks are identified and prioritized, the alert originator selects mitigation actions and assigns roles and responsibilities for implementing them. To increase effectiveness and efficiency, the alert originator should look for common mitigation actions that apply to multiple risks. Figure 5 shows examples of such mitigation actions.

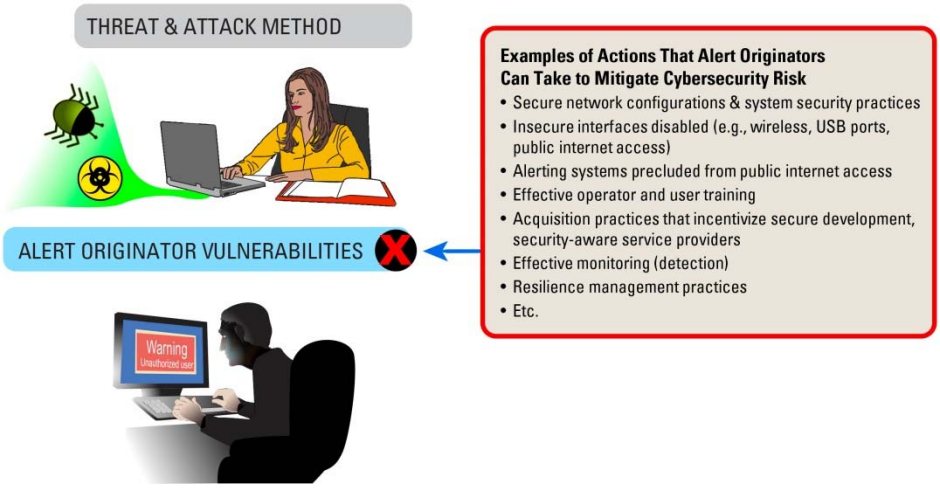

Figure 5: Example Cybersecurity Risk-Mitigation Actions

Once mitigation actions are chosen, it is necessary to respond to the following questions:

- Who in the alert originator's organization is responsible for each risk-mitigation action?
- When in the life cycle (adoption, operations, and sustainment) should the alert originator perform risk mitigation and management tasks?
- How should the alert originator structure and manage tasks and interactions with a WEA-capability vendor or service provider to ensure secure and resilient operations?

The answers to these questions will help clarify roles and responsibilities and enable the alert originator to develop a plan to both implement the selected risk-mitigation actions and execute the CSRM strategy. Table 8 contains a sample list of top-level planning activities, along with the role(s) that might be responsible for each. The role names that organizations use may differ from the generic role names used in the table. Alert originators should substitute the roles used by their organization and assign responsibilities accordingly.

Table 8: CSRM Planning Activities and Assignments

Activity	Activity Goal	Role Assigned to
1	Define organizational security requirements.	Executive manager (decision maker), assisted by others as needed
2	Complete mandated IPAWS-OPEN training and any additional competency training needed for WEA preparation.	Operations manager and others as appropriate
3	Select the organizational security requirements to assign to • acquired technology and services • operational staff • development staff	Technology acquisition and contracting staff, operations manager, and development staff
4	Identify remaining unaddressed security requirements, and define how to address them.	Executive manager, assisted by others as needed
5	Prepare for cybersecurity analysis (Stage 1 of the CSRM strategy). Additional activities such as training for selected vendor tools may be necessary first.	Technology acquisition and contracting staff, operations manager, and development staff representative
6	Validate the procedures described in Activity 5 with candidate technology and service providers, operational users, and development staff.	Technology acquisition and contracting staff, operations manager, and development staff
7	Identify cyber threats and vulnerabilities (Stage 2 of the CSRM strategy).	Technology acquisition and contracting staff, operations manager, development staff, and security analysts (internal or contracted)
8	Review the identified threats and vulnerabilities with the vendor (if appropriate) and the executive manager.	Technology acquisition and contracting staff, operations manager, and development staff
9	Assess and prioritize cybersecurity risks (Stage 3 of the CSRM strategy).	Technology acquisition and contracting staff, operations manager, development staff representative, and security analysts
10	Review and augment the organizational security requirements defined in Activity 1 to ensure that they address the cybersecurity risks prioritized for mitigation in Activity 9. Update the results of Activity 3 accordingly.	Technology acquisition and contracting staff, operations manager, and development staff
11	Construct a timeline of tasks to address all assigned cybersecurity requirements.	Technology acquisition and contracting staff, operations manager, and development staff representative
12	Review the timeline with executive management to ensure that it accommodates other organizational priorities.	Executive manager, assisted by others as needed
13	Schedule and conduct periodic reviews to ensure that tasks are completed according to the timeline and to adapt security requirements and tasks to changes in operational procedures, technology, threats, or staff roles and responsibilities.	Executive manager, assisted by others as needed
14	Construct an operational security risk management plan to ensure that cybersecurity risks are continuously evaluated and addressed once the WEA capability is deployed.	Operations manager
15	Review the operational security plan for completeness, and assign responsibility for monitoring cybersecurity activities and tasks.	Executive manager, assisted by others as needed
16	Schedule and conduct periodic reviews of the operational security plan and its implementation to ensure that cybersecurity risks and issues are being addressed.	Executive manager, operations manager, and other participants as needed

Participants in selecting risk-mitigation actions include WEA-capability vendors, technical security analysts, and alert originator managers and staff. While WEA-capability vendors and technical security analysts can assist in identifying appropriate mitigation actions, alert originator participation is critical because the choice of risk-mitigation actions will affect cost, usability, and organizational policies.

Governance, Organizational Processes, and Operational Mechanisms

The four-stage CSRM strategy requires effective planning, monitoring, and sustainment to ensure that it is effective and adapted over time to address new threats, technology upgrades, and changes in staff and operational procedures. These planning, monitoring, and sustainment activities are accomplished through organizational governance, processes, and operational mechanisms. The National Institute of Standards and Technology (NIST) Risk Management Framework, illustrated in Figure 6, depicts this structure [NIST 2011]. Governance functions at the top of the organization to fund, approve, and guide; processes define the ongoing activities of the organization to ensure consistency, accuracy, and repeatability; and operations forms the context within which processes are executed, supplying tools, technology, communications, and connectivity.

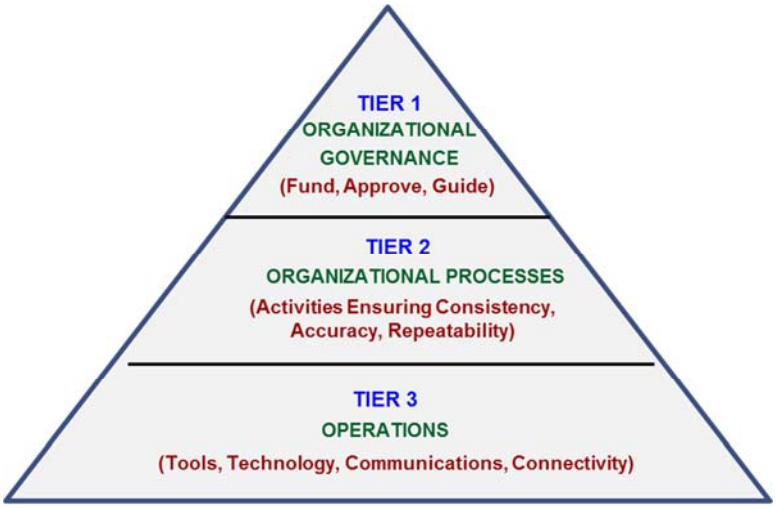

Figure 6: Risk Management Framework [Derived from NIST 2011, p. 9]

For the WEA CSRM strategy, the *governance tier* of the Risk Management Framework funds, approves, and guides planning, execution, and sustainment of the strategy. The *organizational processes tier* documents the plan and schedule for CSRM activities such as those shown in Table 8, verifies implementation, and evaluates effectiveness. The *operations tier* executes the plan, applying the methods and tools identified for each stage in the CSRM strategy (e.g., procedure documentation, STRIDE analysis, and cybersecurity risk assessment).

Conclusion

The alert originator has an important role in managing cybersecurity risks to the WEA capability. Whether the capability resides in-house or is delivered as a service, the alert originator is responsible for understanding threats, ensuring that vulnerabilities are identified, and mitigating risks so that alerts are sent with proper authorization, accurately, and on time, every time. The four-stage WEA CSRM strategy—supported by governance, organizational processes, and operational mechanisms—provides an approach that alert originators can apply to meet this responsibility in their organizations' environments. For more information on the CSRM strategy and its governance, see the report *WEA Cybersecurity Risk Management Strategy for Alert Originators* [SEI 2013b].

Key Terms

alert originator An organization that uses the WEA service to alert the public of emergency situations.

authentication The actions taken to verify that a user is authorized to perform a task. For example, an alerting system might authenticate by checking operators' credentials before allowing them to generate an alert.

credentials Proof of authority. Examples include user names, passwords, key fobs, and badges.

cybersecurity The ability to protect or defend computer systems and networks from attack.

denial of service An attack method that attempts to prevent legitimate users from accessing a network resource. For example, an attacker may target a website and, if successful, prevent users from accessing its content.

Additional Resources

Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley, 2003.

Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

Committee on National Security Systems (CNSSI). *CNSSI Instruction No. 4009 National Information Assurance Glossary*. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (2010).

Federal Emergency Management Agency. *Commercial Mobile Alert System (CMAS) Concept of Operations (CONOPS)* (Version 1.0). FEMA, November 2009. http://www.fema.gov/pdf/emergency/ipaws/ipaws_cap_mg.pdf

Howard, Michael & Lipner, Steve. *The Security Development Life Cycle*. Microsoft Press, 2006.

International Telecommunication Union. *ITU-T X.1205 Series X: Data Networks, Open System Communications and Security—Telecommunication Security: Overview of Cybersecurity*. ITU, 2008.

Microsoft Corporation. *The STRIDE Threat Model*. http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx (2006).

National Institute of Standards and Technology. *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST Special Publication (SP) 800-39). NIST, U.S. Department of Commerce, 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

National Institute of Standards and Technology, Computer Security Division, Information Technology Lab. *Glossary of Key Information Security Terms, NISTIR 7298 Revision 2*. NIST, U.S. Department of Commerce, 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Software Engineering Institute. *Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators* (CMU/SEI-2013-SR-018). Software Engineering Institute, Carnegie Mellon University, 2013. http://techxferauth.sei.cmu.edu/library/assetview.cfm?assetID=70071

Appendix Methods in Best Practices

In public alerting, some agencies have reduced the pressure on emergency alert personnel during an emergency by developing and maintaining a database of predefined alert messages that can be easily tailored for emergency events. The predefined messages reduce the time needed to compose a new message in the midst of a stressful situation. This practice has proven to be effective and can therefore qualify as a best practice. Sharing such a best practice among alerting agencies can lead to improved public safety outcomes.

A *best practice* is a method or technique that has consistently shown results superior to those achieved with other means and that, through experience and research, has proven to reliably lead to a desired result [BusinessDictionary 2013]. The University of Kansas Community Toolbox describes best practices as "those methods or programs that have been found to be successful in accomplishing their goals, and that can be used, or adapted for use, in your circumstances" [Rabinowitz 2013].

A best practice framework is a set of best practices defined at a high level of abstraction that summarizes the experiences of a great many people. There are a number of best practice frameworks, such as Six Sigma for quality assurance [Pyzdek 2001] and the Balanced Score Card for performance management [Martinsons 1999]. A best practice–driven organization searches for best practices or best practice frameworks, adapts them to the local context, and adopts them for everyday use. IzReal.eu describes a process for adopting a best practice to a local context that is designed for use by citizens with minimal process training. This process includes the following steps [IzReal.eu 2012]:

- **Searching** – There are numerous publications in every domain of endeavor that describe best practices in that domain. Before adopting a new practice, thoroughly search for existing best practices to save time and gain the insights of others into the task for which a best practice is sought.
- **Evaluating** – Evaluate each candidate best practice to determine whether it is feasible to carry out the activities of the practice given the constraints in the local context.
- **Validating** – Validate each selected best practice through a controlled pilot use of the practice.
- **Transferring** – Communicate the validated best practice to the personnel who will integrate the best practice into their operating procedures.
- **Reviewing** – Periodically review and update all practices to determine that they are still effective and the best that exist.
- **Routinizing** – Rehearse the practices sufficiently for performing them to become routine.

We explore each of these steps more deeply in the following sections.

A The Value of Best Practices

The value of a best practice is the positive difference in outcome that results from using that specific practice as opposed to the outcomes of using other ways of accomplishing the same task.

Value is measured in terms of the types of outcomes expected. For example, a practice that reduces property damage from a storm could be valued in terms of the dollars in property damage saved compared to the level of damage in past events of similar magnitude and intensity. A practice that reduces the likelihood of loss of life can be valued through actuarial processes but also has value for which there is no accounting. While quantitative evidence of the value of a best practice is always desirable, in some cases it is not easily attainable. In the absence of quantitative evidence, practices may still be classified as "best" based on qualitative measures.

Many new practices are modifications of existing practices; therefore, the creators of the new practice should be able to point to the specific changes they have made to the old practice and reason about the impact of those changes on the value of the practice. Changes to best practices result from process improvement activities within an organization or process improvement efforts in an industry. For example, the World Institute for Nuclear Security is an international organization devoted solely to the development, exchange, and promulgation of nuclear security best practices collected from numerous process improvement efforts. Other organizations in other industries have similar charges, including the Federal Emergency Management Agency (FEMA), which published an *Emergency Alert System Best Practices Guide* [FEMA 2013a]. This guide is based on input from the Emergency Alert System community.

Valuable practices often reflect an interaction across organizations. Within an industry, several related organizations having similar end goals but different foci may join forces. For example, the American Rental Association has partnered with the Association of Equipment Manufacturers, the International Powered Access Federation, and the Scaffold & Access Industry Association to produce a document, *Statement of Best Practices for Workplace Risk Assessment and Aerial Work Platform Selection*, which explains how to rent and use heavy equipment [ARA 2013]. The International Association of Fire Fighters, AFL-CIO, and CLC in cooperation with FEMA, the Department of Justice, and the National Institute of Justice produced *Best Practices for Emergency Vehicle and Roadway Operations Safety in the Emergency Services*, which presents a large number of case studies of mutual interest [IAFF 2010].

Best practice descriptions often have a history of use and describe multiple implementations. The history of use provides potential adopters with examples where the practice has been most valuable and where it has not been as useful. The multiple implementations can help illustrate how an organization might adapt a standard definition to fit special local needs. *Best Practices for Emergency Vehicle and Roadway Operations Safety in the Emergency Services* illustrates the best practices with examples from multiple states and types of vehicles.

The World Health Organization (WHO) has identified a number of characteristics of a valuable best practice [WHO 2008]. Table 9 lists a few of the relevant characteristics from the WHO's *Guide for Documenting and Sharing "Best Practices."*

Table 9: Characteristics of a Valuable Best Practice [WHO 2008]

Effectiveness	This is a fundamental criterion implicit in the definition. The practice must work and achieve measurable results.
Efficiency	The proposed practice must produce results with a reasonable level of resources and time.
Relevance	The proposed practice must address the activities needed for the practice.
Ethical soundness	The practice must respect the current rules of ethics for dealing with the content of the practice.
Sustainability	The proposed practice must be implementable over a long period of time without any massive injection of additional resources.
Possibility of duplication	The proposed practice, as carried out, must be replicable elsewhere.
Involvement of partnerships	The proposed practice should involve satisfactory collaboration between several stake-holders.

The definition of a best practice should include three important characteristics:

1. a comparative process
2. an action
3. a linkage between the action and some outcome or goal

The comparative process allows an organization to compare the candidate practice to other known practices either internal or external to the organization. The primary means of comparison is by the value produced by each practice. Other criteria might include the resources consumed to produce that value or the time frame within which the value is produced.

The action is the application of the techniques defined in the best practice. The description must be sufficiently clear that others with a reasonable background can replicate the practice. The actions may also help an organization understand the level of resources needed. The action can be represented in either a natural language or a constructed language such as a workflow language.

There is a causal relationship between the actions carried out for the practice and the expected outcomes. The definition of the practice should make this as clear as possible so that anyone who modifies the practice will understand the consequences of omitting certain actions. We explore this linkage in more depth in Section B.

The Toyota Production System (TPS) is an example of a corporate commitment to best practices [Kato 2010] that demonstrates the comparative process, action, and linkage between action and outcome. The Toyota Kaizen process is used to continually improve processes through the results of many small experiments. Each employee is empowered to design and conduct these experiments and to alter the process if the experiment is successful. At any given moment, Toyota is using the best practices that its employees have managed to design through the Kaizen approach. These best practices work because employees have already tested them in production.

Best practices should not be confused with industry or government standards. Best practices are more responsive than formal standards to the need for changes in processes and technologies. Defining a best practice begins with an existing practice and proceeds through testing some incremental change, as in a TPS experiment. A practice definition should not have to pass through a long approval process if there is sufficient evidence of its efficacy.

Standards, on the other hand, are products of dialog among professionals and often represent the compromises required to reach agreement among diverse elements of a profession. Standards are useful for interactions among researchers, organizations, and others, but standards sometimes represent the future expectations of the group rather than tested and proven techniques. The long approval process for most international standards prevents them from being very agile. A best practice is a proven process that can be replaced more rapidly than a standard.

The Common Object Request Broker Architecture (CORBA) illustrates an interesting distinction between best practices and standards. The Object Management Group (OMG) developed the CORBA standard with the intent of changing the way that software designers and developers construct software and write code. Unfortunately, implementation weaknesses as well as the process by which the CORBA standard was created led to a significant decline in its use and adoption. A computer science professor at the University of California–Berkeley describes one of the lessons learned from this decline as follows:

> *Standardize existing best practices, rather than trying to "innovate" in the standard; otherwise you risk everything-but-the-kitchen-sink feature creep of unproven approaches. [Fox 2008]*

Standards often represent a theoretical process that is a blend of activities, each of which has worked in some situation but not necessarily together with others as a unit. A best practice may blend activities, but the practice in its entirety has proved successful.

A.1 The Importance of Context

Best practices are not universally applicable. They are particularly applicable in specific situations, but they may be contraindicated in other situations. Constraints, cultures, and assumptions define the boundaries within which a practice is "best." There may be legal or regulatory constraints that prohibit the use of a certain practice in some locales. Resource constraints may make certain practices impractical for a community lacking the specific resource: water, trained professionals, or money. Technology constraints may also play a role: using emergency notification services such as Reverse 911 that will take 30 minutes to reach an audience of 20,000 people is not a best practice if a tornado has already been seen nearby.

Cultural issues are usually implicit in the domain that will apply the practice. Capturing those issues in the best practice description will help personnel to remember them when evaluating a practice for use. For example, rescue helicopter pilots will view weather restrictions differently from commuter helicopter pilots.

The attributes of the practice contribute to determining the appropriateness of a practice in a specific context. For example, the reading level of the process description must match the abilities of the employees who will perform the practice. Or a practice might assume that evacuees are mobile and self-sufficient, which will not be the case in the evacuation of a skilled-care nursing home.

The definition of a best practice should give the information needed to determine those situations to which the best practice applies. The writer of a best practice should be as explicit as the situation allows. If a person must have specific certifications, a required number of years of experience, or knowledge of a second language, the practice description must include this information.

Any method for applying best practices should include a step in which the practice is compared to the environment in which it will be used. Any conflict with a constraint should be identified and noted, and a relevant authority should either accept the risk or consider a different practice. A simple risk analysis can identify possible consequences of applying the practice.

A.2 Results to Expect from Using Best Practices

Best practices correctly applied and used in the appropriate context should produce best-in-class results. The results should be better than what the organization has been experiencing and what others in similar circumstances experience. Failing to correctly apply the practice or violating a contextual constraint will at least reduce the impact of the results and may result in catastrophic outcomes.

The value expected from deploying best practices should at a minimum be greater than the amount of resources required to apply the practice. If the organization takes a value engineering approach, then all aspects of the project have an assigned value [DoD 2011]. It can then base decisions on the expected value generated by an action and evaluate how closely the applied practice comes to generating the expected value.

Do not necessarily expect perfect results or even as good a result as others have achieved when deploying a best practice. Constraints, culture, and previously unrecognized assumptions influence the effectiveness of a practice, and one organization may not be able to use a practice as effectively as another organization due to limitations on resources or other constraints.

B Outcomes Theory

Emergency management agencies (EMAs) should evaluate best practices to include in emergency procedures on the ultimate outcome as well as immediate results.[11] The outcome of applying a best practice is often more far reaching than the immediate observed results. Using sirens to broadcast a warning of a tornado on the ground has the immediate result of people moving to shelters, but the outcome of this action is a reduction in deaths and injuries. The siren warning causes people to know there is danger and to seek shelter. The shelter protects the people, with the outcome of reductions in deaths and injuries. An outcome is the end result of a causal chain with multiple intermediate results between the initial intervention and the last event in the causal chain.

In the field of emergency alerting, the intervention is the issuance of a message that gets the attention of a target audience. The expected result can be stated as an output from the intervention in terms of how many people are alerted by the intervention. The result could be stated as an outcome of the intervention in which there is no loss of life or serious injury.

An outcome is the result of an action, not the action itself. In our case, the action is an intervention into a situation by applying a best practice. Outcomes theory defines techniques for establishing and documenting causality. We intend for our intervention to produce a desired outcome, but we do not always have direct control over the outcome. There may be multiple factors that influence the outcome. For example, loud thunder and winds may prevent some people from hearing an emergency siren.

[11] A *result* is the direct, causally related effect of applying a certain action. An *outcome* is a result, but it is a long-term change that may be less directly related to a single specific action.

An outcome is also not the output from an action. There is a causal relationship between the action and the outcome, while there is a direct functional relationship between the action and its outputs. An *output* in emergency alerting might be the number of telephone calls that the Reverse 911 system made in an hour. An intermediate *result* in the causal chain might be that a higher percentage of people took mitigating steps before the weather event struck, with the ultimate *outcome* being fewer deaths and injuries.

B.1 Specifying Desired Outcomes

There are several theories of outcomes, and most of them specify outcomes as causal chains using diagramming techniques such as results maps, logic models, program logics, intervention logics, means–ends diagrams, logframes, theories of change, program theories, outcomes hierarchies, and strategy maps [Duignan 2010]. These diagrams provide a flow of activities leading to the planned-for outcome. Figure 7 shows an example flow.

The diagram begins with a state of the system and then shows actions that are believed to be causally linked to a specific set of outcomes. The set of actions represents a theory of what will cause the intended outcome. The causal network is hypothesized during planning and verified over time with experience.

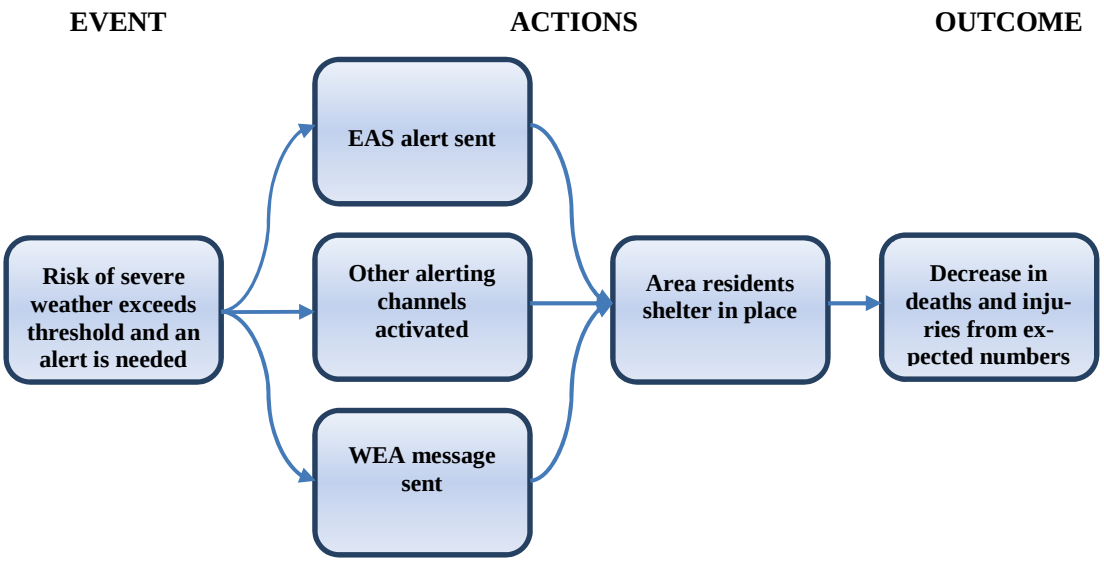

Figure 7: Causal Diagram

The Easy Outcomes method defines a method for modeling the causal relationships among actions [Duignan 2006]. Table 10 shows the 10 steps in the method for defining, using, and evaluating outcomes. In Step 2, outcomes are specified and then, in Step 3, the activities that lead to those outcomes. This is a reasonable way to plan—beginning with the desired outcomes and then, once the causal network is established, identifying the required actions. The method also calls for several forms of validation. Finally, the model is used to explain the chain of cause and effect to others.

Table 10: Steps in the Easy Outcomes Method [Adapted from Duignan 2006]

1. Plan your Easy Outcomes work.
2. Build an outcomes model, and check the evidence for it.
3. Map your activities and priorities onto the model.
4. Identify indicators that measure outcomes.
5. Identify evaluation questions and evaluation projects.
6. Identify possible economic evaluation.
7. Decide on piloting or full roll-out outcome evaluation.
8. Identify evaluation management issues.
9. Select outcomes-focused contracting arrangements.
10. Use your model for reporting back.

B.2 Planning to Evaluate Outcomes

Planning for emergency response is a continuous process. After each incident, an EMA assesses the current practice and plans for changes to the practice. It then validates the changes and prepares for the next incident. The National Preparedness Cycle defined by FEMA's National Incident Management System (NIMS) specifies a comprehensive process [FEMA 2013e]. This iterative approach to planning is shown in Figure 8. The process includes a comprehensive assessment of the activities and outcomes for the best practice. The detailed steps include

- Plan
- Organize / Equip
- Train
- Exercise
- Evaluate / Improve

Figure 8: The Planning Process [Adapted from FEMA 2013e]

Quantitative measures such as number of people who hear a siren or number of telephones rung are easier to estimate than the number of deaths that have been prevented, but the broader outcome is the more important societal goal and a more meaningful measure of success. The IBM Center for the Business of Government report *Moving Toward Outcome-Oriented Performance Measurement Systems* provides a set of recommendations for adopting an outcomes approach to measurement in the public sector [Callahan 2009]. Two of these apply to outcomes in general:

1. Actionable indicators are more important than measures and plans [Callahan 2009].
   Outcomes should provide direction for further action. Time should be spent defining meaningful outcomes as opposed to numerous measures.
2. Select the most important indicators and avoid developing a cumbersome system [Callahan 2009].
   Managers like data. Given the option, they will define numerous measures under the assumption that adding an item to be collected is small overhead. Before they realize it, there are too many, and too much effort is expended managing the collection and analysis of data.

B.3 Problems Evaluating Outcomes

Executing the actions defined in the best practice should produce the anticipated outcomes. One problem with this simple statement is that sometimes the expected results may not be observable for a period of time after the actions are completed. It is usually simple and quick to measure the outputs from the actions, but these are seldom as important as the higher level outcomes.

A second problem is that the organization performing the best practice often is not in control of the outcomes. At best it may be able to influence them. The natural reaction is to use outputs that are more predictable for evaluating the efforts of the organization. This may result in seemingly better reviews for the organization at the expense of the long-term improvement of the organization and its environment.

C How to Identify Best Practices

There are three primary ways to identify a best practice [Veselý 2011]. One approach is to establish a causal relationship between the inputs and outputs of the practice. The second approach is to select a panel of area experts and have them reach consensus on the acceptable practice. The third approach is to instrument the current processes in the organization, tweak those processes, and determine which combinations produce the best results.

C.1 Causal Analysis

Building a causal model captures the activities that define the best practice in a web of cause and effect, such as shown in Figure 8. By backtracking through the model to determine which interventions resulted in favorable outcomes, the analyst can identify best practices. Causal models can be built using statistical inference and can support reasoning about whether a causal model represents reality. For example, Traynor used statistically based reasoning to show that SMS-based emergency alert systems might under certain circumstances not meet their target goals for dissemination time [Traynor 2012]. This is a useful technique for researchers, but practitioners typically do not have access to sufficient data to build such models.

C.2 Authoritative Sources

Some domains may lack the formal foundation necessary for a causal analysis. The knowledge resides in the seasoned professionals who carry out the practices. In that case, a panel of professionals, assembled under the authority of a professional society or government entity, can define the practices. Researchers have performed studies on what constitutes a domain expert and what competencies those experts must have to carry out activities in their domains, such as Bass has shown for the software architecture domain [Bass 2008]. Persons with these competencies are

particularly suitable for identifying best practices. Instead of a panel, a survey instrument sent to a selected audience may be substituted [Griffin 1997].

Research in a domain is often a source of best practices [LIFE 2013]. The research must be correct, and this should be verified through the review process of a conference or journal or by a group of experienced professionals. The Partnership for Public Warning, which has now dissolved, was a public/private partnership of professionals with experience in emergency alerting. They collected information on emergency alerting and have a repository of publications that capture lessons learned by many authorities in the field of emergency alerting [PPW 2008].

C.3 What Works in Your Context

A number of self-improvement techniques can lead to the identification of best practices [Herron 2005]. Frameworks such as the Carnegie Mellon Software Engineering Institute (SEI) CMMI for software development provide a basis for determining what should be measured, what constitutes a noteworthy level of each attribute, and alternative activities that could be designed [Ahern 2001].

Benchmarking is "the process of identifying, understanding, and adapting outstanding practices from organizations anywhere in the world to help an organization improve its performance" [Kumar 1999]. The benchmarking allows the best practice to be supported by available data. Benchmarking is an effective technique when applied internally to an organization because the organization will undertake benchmarking in the same context in which it will deploy the benchmarked best practice.

Benchmarking is used to evaluate practices with techniques such as

- strategy-based benchmarking
- technical efficiency-based practices
- national competitiveness benchmarking

C.4 Piloting

The deployment of a best practice is often sufficiently expensive that conducting a pilot experiment to evaluate the effectiveness and efficiency of the practice prior to committing to a full-scale adoption is a useful investment [NARA 2006]. Several activities are generic enough to form an abstract framework for piloting a best practice experiment. Frameworks such as Six Sigma provide a context for planning and executing a pilot study [Yang 2003].

The pilot must be sufficiently broad to give realistic results but still be cost effective. Techniques such as running scenarios with the practice before conducting the pilot often remove many easy-to-find problems. This results in a more effective pilot whose results will not be distorted by early and obvious mistakes.

D How to Disseminate Best Practices

Communication of knowledge through the dissemination of research findings is a key mechanism for the growth and development of a discipline [Lewando-Hundt 2004]. Determine those who need the information, and then find where they go for information. The best practices must be documented with the target audience in mind and then disseminated in ways that bring the prac-

tices to the attention of the appropriate people. In keeping with the earlier observation that practices evolve, the practice descriptions should be easily modified and cheaply disseminated.

D.1 Documentation Methods and Characteristics

The documentation of best practices must be clear, correct, and descriptive. The language level of the documentation must be appropriate to the level of the users. The writing should convey accurate information using correct grammar. The descriptions must contain enough detail to allow readers to replicate the practice.

When an organization will maintain a large number of best practices, using a standard template will assist both the writer and the reader. The template will guide the writer to include all necessary information. The template will also establish an ordering so that readers can quickly find the specific information that interests them.

D.2 Distribution Methods

Publication in traditional venues such as conferences and journals is appropriate if the intended audience is other researchers, but the language of research is often inaccessible to practitioners. Appropriate venues should be selected for each target audience, and appropriate wording should be used in each venue. These days there is a spectrum of distribution methods from which to choose. Most professional people have mobile devices, and many jobs involve desktop personal computers or tablet-like devices. All of these can access web portals with information provided in visual and audio forms.

Websites can range from simple lists of pointers to documents that just make the information available, or they can be quite elaborate and help users find the information they need through sophisticated query facilities. When the site becomes complex, an architecture is necessary to ensure that the content is valid and accessible [UN 2001]. Wikis, blogs [Wimberly 2013], and other widely available media are useful for distributing best practice information.

The Eclipse Process Framework is a method-engineering environment that supports the OMG Software Process Engineering Metamodel (SPEM) for process description [Eclipse 2013, OMG 2008]. The practices are developed by first using the modular structure of SPEM to define individual roles, tools, processes, and work products. A specific method is then specified, and a website is automatically generated.

E How to Adopt Best Practices

Best practices are often introduced as part of process improvement efforts or technology introduction efforts. These initiatives may be triggered by an event such as a project gone bad or part of continuous process monitoring and evaluation. One approach to structuring the adoption of a best practice is the IDEAL model, developed by the SEI [McFeeley 1996]. The IDEAL model follows the steps of initiating, diagnosing, establishing, acting, and learning as shown in Figure 9. This model supports an iterative adoption process.

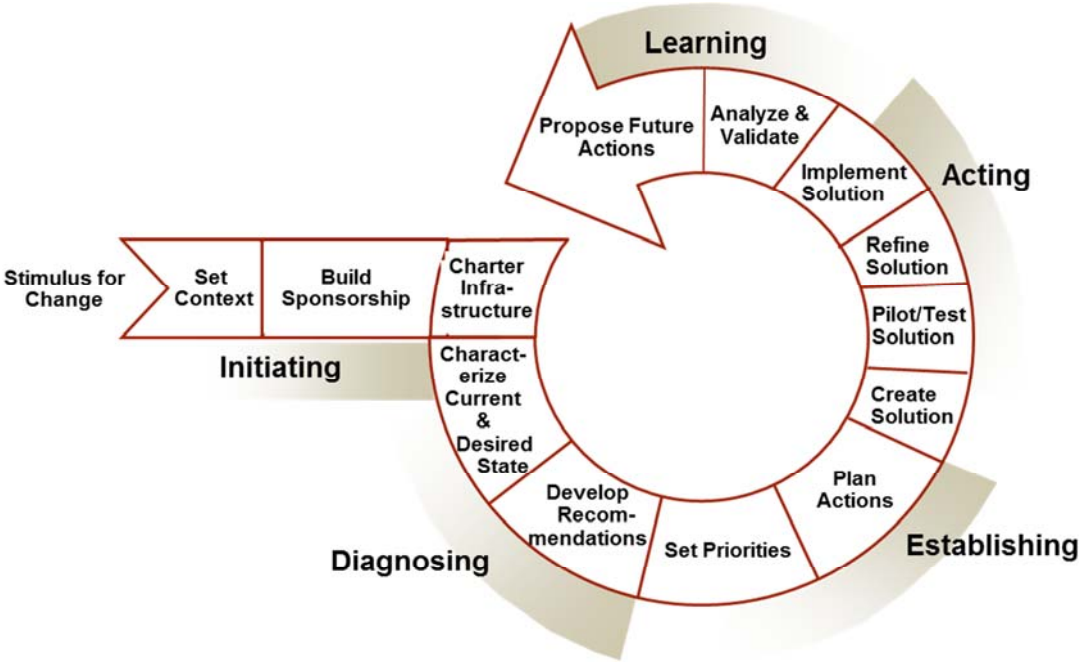

Figure 9: IDEAL Model [Adapted from McFeeley 1996]

The IDEAL model can be integrated with many process improvement techniques that are much more specifically targeted to an organization's context. For example, Izreal.eu describes a process for adopting a best practice that includes the steps searching, evaluating, validating, transferring, reviewing, and routinizing [IzReal.eu 2012]. The steps from that process, which we describe in detail in this section, would be inserted into the Acting section of the IDEAL model shown in Figure 9.

E.1 Searching

EMAs can discover candidate best practices in many ways. They should begin by searching existing collections of best practices for appropriate practices. Professional organizations and government agencies are excellent sources. FEMA has published numerous best practice guides, including *An Emergency Alert System Best Practices Guide* [FEMA 2013a]. The organization should also consider its own current practices as candidate best practices. In some situations, an organization may issue a general "call for practices," similar to a conference's call for papers, to seek input from the audience of the call.

E.2 Evaluating

An organization should evaluate each identified practice against its intended use. "Adapt and then adopt" is the approach recommended for the set of best practices in the Information Technology Infrastructure Library [Burrin 2007]. Once the organization has found or created an appropriate practice, it must adapt the practice to the local context. As it adapts the practice, the organization must accommodate any local constraints in the definition of the practice or perform an analysis to justify violated constraints (in Section F, we discuss evaluating and improving practices in more detail).

E.3 Validating

EMAs must validate the appropriateness of a best practice for the local context. Does the practice work in the local context? This includes considering the availability of resources that the candidate practice requires. A pilot project in which a small group uses the practice during a simulated emergency can assist in identifying steps that the organization needs to modify before full deployment.

E.4 Transferring

The group that defines the best practice must transfer it to the groups that will deploy the process. This transfer may not be as easy as expected, even within the same organization. Research has shown that the "stickiness"—that is, the difficulty in transferring—is due to an inability of the target audience to absorb the information, perhaps because of their previous level of education; causal ambiguity, such as the impossibility of knowing all the factors that lead to success; and an arduous relationship between the source and the recipient, as with transfers to offices in other time zones or that use different languages [Szulanski 1996]. Each challenge requires its own solution:

- Inability to absorb – Write the practice at a more appropriate reading level for the target audience; modularize the practice description to reduce complexity.
- Causal ambiguity – Create a superset of actions for the practice in order to be certain that it includes all required components.
- Arduous relationship – Explain the best practice in a video that the users can download and view at their convenience; assign a self-guided exercise using the best practice and then evaluate the results asynchronously.

E.5 Reviewing

An organization should review a newly deployed practice more often than a mature one. The review should be structured to identify previously unrecognized dependencies and constraints. For example, the state of Minnesota conducts a best practices review annually, targeting a different facet of local government operations with each review [Otto 2012]. The method used includes surveys, interviews, and document searches. Audits in recent years have included the 911 service and fire services.

E.6 Routinizing

By modifying the practice to more tightly integrate with existing practices and organizational culture, an organization can make the practice part of routine operations. Communities of Practice assist with routinizing because this step involves organizational learning as well as individual learning [Borzillo 2007]. A Community of Practice can institutionalize a practice by looking across all of the organizational units represented in its membership. It may find that it needs to reword the practice description and actions to reflect local terminology. It may need to adjust time factors to reflect local geographic constraints or distribution of participants in practice activities. Ultimately the goal is to create a Learning Organization so that the organization can routinize new best practices more easily.

F Evaluation and Continuous Improvement

The evaluation of best practices ranges from informal postmortems [Collier 1996] to benchmarking [Griffin 1997] to statistical experiments [Chilingerian 1995]. Evaluation activities address the major objectives for the practice and should be designed at the same time as the practice activities. The evaluation activities described in this section are part of the IDEAL cycle and hence are iteratively applied.

F.1 Continuous Evaluation of Best Practices

Evaluation itself has best practices, and one of those is to integrate the evaluation into standard operating procedures to achieve continuous feedback. To ensure accurate and prompt feedback, an organization should automate as much of the process as possible. Consider automating options to generate log files or record and play back functions that capture actual operations. Web-based tools should provide the opportunity for pop-up surveys that capture input from employees and end users.

The organization should also plan for how to direct feedback to the group responsible for the appropriate practice. Follow-up should ensure that the group has carefully considered the feedback and made changes to the practice if the feedback indicates that they are needed.

F.2 Continuous Improvement of Best Practices

For an organization to benefit from continuous improvement, it must be a learning organization [Garvin 2000]. Employees must feel free to question existing practices, make suggestions, and develop new materials to help others learn. Capturing best practices using smartphones or inexpensive video cameras allows an organization to propagate changes in practices quickly and cost effectively. This enables communication through the organization.

A key element in continuous improvement is to intervene as early as possible. While addressing the feedback received during evaluation activities, an organization can use causal analysis to identify root causes of problems. The team responding to the feedback for a specific practice can address each root cause and propose changes to the practice as soon as it obtains sufficient feedback.

Improving a practice follows a process much like a software development process. The evaluation activities define the new requirements for the practice. The practice must be redesigned to meet the new requirements. The new practice must be prototyped, tried, and then implemented. A learning organization can quickly deploy a practice and then iteratively improve it.

G Maintaining Best Practices

Maintaining an organization at a best practice level of operation requires two major activities. The organization must continually evaluate and modify the practices it uses to ensure that they really are the best. The organization must also ensure that personnel comply with the current versions of the practices.

G.1 Revising

Practices that are out of date and no longer “best” are at least a source of customer dissatisfaction and may even be a source of liability. A regular revision rhythm will help make the revision pro-

cess successful. Personnel can plan activities such as all-hands meetings and create personal development plans, and other activities can be matched to the rhythm. The revision rhythm should match the dominant external or internal forces. For example, governmental organizations have major rhythms around new budgets for October 1, changes in tax laws on January 1, and other new laws going into effect on July 1.

The continuous evaluation and continuous improvement activities discussed in this section are essential for revising the best practices. The feedback from these activities gives input for revision. Once an organization receives the feedback, it must modify the practice to address the issues identified in the feedback.

G.2 Training

Training is directly connected to the best practices and to revisions. A regular rhythm of practice revisions can translate into a regular training schedule. Managers and operational personnel can expect to update themselves on the new practice definitions and perhaps to attend formal training after each scheduled release.

Organizations can track training through personal training plans for all personnel. Each role in the organization has a list of practices for which a person holding that role must be trained. Training records simply capture what training personnel should have, given their roles; when they have taken or are scheduled to take the training; and how often they must be retrained.

In some cases, the revisions to best practices may be sufficiently simple that a reading of the revised practice or just the revision notes is sufficient for personnel to comply with the changes. E-training provides the advantage of asynchronous training and lets personnel fit training into those moments when other business is manageable [Lesh 2001].

G.3 Contributing

The personnel contributing the best practices and those using them have different perspectives on the practices applied by the organization, and both are valuable. The users will provide comments and will identify their priorities. The contributors will create the revisions and the accompanying training material.

References

URLs are valid as of the publication date of this document.

[Ahern 2001]
Ahern, Dennis M.; Clouse, Aaron; & Turner, Richard. *CMMI Distilled: A Practical Introduction to Integrated Process Improvement*. Addison-Wesley, 2001.

[Alberts 2003]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley, 2003.

[ARA 2013]
American Rental Association, Association of Equipment Manufacturers, International Powered Access Federation, & Scaffold and Access Industry Association. *Industry Groups Issue Statement of Best Practices for Workplace Risk Assessment and AWP Equipment Selection*. Rental Equipment Register, 2013. http://rermag.com/headline-news/industry-groups-issue-statement-best-practices-workplace-risk-assessment-and-awp-equip

[Bass 2008]
Bass, Len; Clements, Paul; Kazman, Rick; & Klein, Mark. *Models for Evaluating and Improving Architecture Competence* (CMU/SEI-2008-TR-006). Software Engineering Institute, Carnegie Mellon University, 2008. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8673

[Borzillo 2007]
Borzillo, Stefano. *Communities of Practice to Actively Manage Best Practices*. Springer, 2007.

[Burrin 2007]
Burrin, Nelly; Regev, Gil; & Wegmann, Alain. "Adapt and Adopt: An Experiment in Making Best Practices Adequate in an Organization." Presented at the 19th International Conference on Advanced Information Systems Engineering, Trondheim, Norway, June 2007. http://lams.epfl.ch/conference/bpmds07/program/Burrin_36.pdf

[BusinessDictionary 2013]
BusinessDictionary.com. "Best Practice." WebFinance, Inc., 2013. http://www.businessdictionary.com/definition/best-practice.html

[Callahan 2009]
Callahan, Kathe & Kloby, Kathryn. *Moving Toward Outcome-Oriented Performance Measurement Systems*. IBM Center for the Business of Government, 2009. http://www.businessofgovernment.org/report/moving-toward-outcome-oriented-performance-measurement-systems

[Caralli 2011]
Caralli, Richard A.; Allen, Julia H.; & White, David W. CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience. Addison-Wesley, 2011.

[Chilingerian 1995]
Chilingerian, Jon A. "Evaluating Physician Efficiency in Hospitals: A Multivariate Analysis of Best Practices." *European Journal of Operational Research 80*, 3 (February 1995): 548–574.

[CNSS 2010]
Committee on National Security Systems. *CNSSI Instruction No. 4009 National Information Assurance Glossary*. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (2010).

[Collier 1996]
Collier, B.; DeMarco, Tom; & Fearey, P. "A Defined Process for Project Post Mortem Review." *IEEE Software 13*, 4 (July 1996): 65–72.

[CTIA 2013]
CTIA–The Wireless Association. *Wireless Emergency Alerts on Your Mobile Device*. http://www.ctia.org/consumer_info/safety/index.cfm/AID/12082 (2013).

[DHS 2013a]
Department of Homeland Security. *Homeland Security Exercise and Evaluation (HSEEP) Program*. https://www.llis.dhs.gov/hseep (2013).

[DHS 2013b]
Department of Homeland Security. *Lessons Learned Information Sharing (LLIS.gov)*. https://www.llis.dhs.gov (2013).

[DoD 2011]
Office of Deputy Assistant Secretary of Defense Systems Engineering. V*alue Engineering: A Guidebook of Best Practices and Tools* (SD-24). Department of Defense, 2011.

[Duignan 2006]
Duignan, Paul. *Guidelines for Drawing Good Outcomes Models*. Easy Outcomes, 2006. http://www.easyoutcomes.org/guidelines/outcomesguidelines.html

[Duignan 2010]
Duignan, Paul. *What Are Outcomes Models (Program Logic Models)?* Outcomes Theory Knowledge Base, 2010. https://outcomestheory.wordpress.com/article/what-are-outcomes-models-program-logic-2m7zd68aaz774-22

[Eclipse 2013]
Eclipse Foundation. *Eclipse Process Framework Project (EPF)*. http://www.eclipse.org/epf (2013).

[FEMA 2009]
Federal Emergency Management Agency. *Commercial Mobile Alert System (CMAS) Concept of Operations (CONOPS)* (Version 1.0). FEMA, November 2009. http://www.fema.gov/pdf/emergency/ipaws/ipaws_cap_mg.pdf

[FEMA 2013a]
Federal Emergency Management Agency. *An Emergency Alert System Best Practices Guide* (Version 1.0). FEMA, 2013. http://www.fema.gov/pdf/emergency/ipaws/eas_best_practices_guide.pdf

[FEMA 2013b]
Federal Emergency Management Agency. *Integrated Public Alert & Warning System*. http://www.fema.gov/integrated-public-alert-warning-system (2013).

[FEMA 2013c]
Federal Emergency Management Agency. *Integrated Public Alert & Warning System Developer Webinar Archive*. http://www.fema.gov/calendar-events/integrated-public-alert-warning-system-developer-webinar-archive (2013).

[FEMA 2013d]
Federal Communications Commission. *Wireless Emergency Alerts (WEA) Guide*. http://www.fcc.gov/guides/wireless-emergency-alerts-wea (2013).

[FEMA 2013e]
Federal Emergency Management Agency. *National Preparedness Cycle*. FEMA, 2013. http://www.fema.gov/national-preparedness-cycle

[Fox 2008]
Fox, Armando. *On the Decline of CORBA*. http://www.armandofox.com/geek/2008/09/on-the-decline-of-corba (2008).

[Garvin 2000]
Garvin, David A. *Learning in Action: A Guide to Putting the Learning Organization to Work*. Harvard Business School Press, 2000.

[Griffin 1997]
Griffin, Abbie. "PDMA Research on New Product Development Practices: Updating Trends and Benchmarking Best Practices." *Journal of Product Innovation Management 14*, 6 (1997): 429–458.

[Herron 2005]
Herron, David & Garmus, David. "Identifying Your Organization's Best Practices." *CrossTalk 18*, 6 (June 2005): 22–25. http://www.crosstalkonline.org/storage/issue-archives/2005/200506/200506-Herron.pdf

[Howard 2006]
Howard, Michael & Lipner, Steve. *The Security Development Life Cycle*. Microsoft Press, 2006.

[IAFF 2010]
International Association of Fire Fighters. *Best Practices for Emergency Vehicle and Roadway Operations Safety in the Emergency Services*. IAFF, 2010. http://www.iaff.org/hs/evsp/Best%20Practices.pdf

[ITU 2008]
International Telecommunication Union. ITU-T X.1205 Series X: Data Networks, Open System Communications and Security—Telecommunication Security: Overview of Cybersecurity. ITU, 2008.

[IzReaL.eu 2012]
IzReaL.eu. *Adopting Best Practices.* Alcula Group U.A.B., 2012. http://izreal.eu/2012/10/31/adopting-best-practices

[Kato 2010]
Kato, Isao & Smalley, Art. *Toyota Kaizen Methods: Six Steps to Improvement*. Productivity Press, 2010.

[Kumar 1999]
Kumar, A.; Motwani, J.; Douglas, C.; & Das, N. "A Quality Competitiveness Index for Benchmarking." *Benchmarking: An International Journal 6*, 1 (1999): 12–21.

[Lesh 2001]
Lesh, Steven G. "Evidence-Based Asynchronous Learning Best Practices." Presented at the Seventh Sloan-C International Conference on Online Learning. Orlando, FL, Nov. 2001. http://sloanconsortium.org/conference/proceedings/2001/ppt/01_lesh.ppt

[Lewando-Hundt 2004]
Lewando-Hundt, G. & Zaroo, S. A. "Evaluating the Dissemination of Health Promotion Research," 163–176. *Evaluating Health Promotion: Practice and Methods*, 2nd ed. Edited by M. Thorogood & Y. Yolande Coombes. Oxford University Press, 2004.

[LIFE 2013]
LIFE Programme. *Best Practice – A Method for Dissemination and Implementation of Project Results*. European Commission, 2013. http://ec.europa.eu/environment/life/publications/lifepublications/generalpublications/documents/bestpractice.pdf

[Martinsons 1999]
Martinsons, Maris; Davison, Robert; & Tse, Dennis. "The Balanced Scorecard: A Foundation for the Strategic Management of Information Systems." *Decision Support Systems 25*, 1 (February 1999): 71–88.

[McFeeley 1996]
McFeeley, Bob. *IDEAL: A User's Guide for Software Process Improvement* (CMU/SEI-96-HB-001). Software Engineering Institute, Carnegie Mellon University, 1996. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=12449

[Microsoft 2005]
Microsoft Corporation. *The STRIDE Threat Model*. http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx (2006).

[Mileti 1990]
Mileti, Denis S. & Sorenson, John H. *Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the Art Assessment.* Oak Ridge National Laboratory, 1990. http://emc.ed.ornl.gov/publications/PDF/CommunicationFinal.pdf

[NARA 2006]
National Archives and Records Administration. *Recommended Practice: Developing and Implementing an Enterprise-wide Electronic Records Management (ERM) Proof of Concept Pilot.* http://www.archives.gov/records-mgmt/policy/pilot-guidance.html (2006).

[NIST 2011]
National Institute of Standards and Technology. *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST Special Publication (SP) 800-39). NIST, U.S. Department of Commerce, 2011.
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[NIST 2013]
National Institute of Standards and Technology, Computer Security Division, Information Technology Lab. *Glossary of Key Information Security Terms, NISTIR 7298 Revision 2.* NIST, U.S. Department of Commerce, 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[NWS 2013]
National Weather Service. *Wireless Emergency Alerts Capable: Weather Warnings on the Go.* http://www.nws.noaa.gov/com/weatherreadynation/wea.html (2013).

[OMG 2008]
Object Management Group. *Software & Systems Process Engineering Metamodel Specification (SPEM)* (Version 2.0). http://www.omg.org/spec/SPEM/2.0 (2008).

[Otto 2012]
Otto, Rebecca. *Best Practices Reviews*. Minnesota Office of the State Auditor, 2012. http://www.osa.state.mn.us/default.aspx?page=bestPracticesReviews

[PPW 2008]
Partnership for Public Warning. http://www.partnershipforpublicwarning.org (2008).

[Pyzdek, Thomas 2001]
Pyzdek, Thomas. *The Six Sigma Handbook: A Complete Guide for Green Belts, Black Belts, and Managers at All Levels*. McGraw-Hill, 2001.

[Rabinowitz 2013]
Rabinowitz, Phil & the Community Toolbox. *Promoting the Adoption and Use of Best Practices.* Work Group for Community Health and Development at the University of Kansas, 2013. http://ctb.ku.edu/en/tablecontents/MainSection19.6.aspx

[SEI 2013a]
Software Engineering Institute. *Study of Integration Considerations for Wireless Emergency Alerts* (CMU/SEI-2013-SR-016). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70063

[SEI 2013b]
Software Engineering Institute. *Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators* (CMU/SEI-2013-SR-018). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70071

[Szulanski 1996]
Szulanski, Gabriel. "Exploring Internal Stickiness: Impediments to the Transfer of Best Practice Within the Firm." *Strategic Management Journal 17* (1996): 27–43.

[Trocki Stark 2013]
Trocki Stark, E.; Lavan, J.; Frankel, M.; Marshall-Keim, T.; & Elm, J. *Wireless Emergency Alerts: New York City Demonstration* (CMU/SEI-2012-SR-016). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=70024

[Traynor 2012]
Traynor, P. "Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services." *IEEE Transactions on Mobile Computing 11*, 6 (June 2012): 983–994.

[UN 2001]
United Nations Statistical Commission & Economic Commission for Europe. *Best Practices in Designing Websites for Dissemination of Statistics*. United Nations, 2001. http://www.unece.org/fileadmin/DAM/stats/publications/websitebestpractice.pdf

[Veselý 2011]
Veselý, Arnošt. "Theory and Methodology of Best Practice Research: A Critical Review of the Current State." *Central European Journal of Public Policy 5*, 2 (December 2011): 98–117.

[WHO 2008]
World Health Organization. *Guide for Documenting and Sharing "Best Practices" in Health Programmes*. WHO, 2008.

[Wimberly 2013]
Wimberly, Rick. "Boston Bombing Shows How Wireless Emergency Alerts Can Work with Other Media." *Emergency Management*. http://www.emergencymgmt.com/emergency-blogs/alerts/Boston-Bombing-Shows-How-042313.html (2013).

[Yang 2003]
Yang, Kai & El-Haik, Basem. *Design for Six Sigma: A Roadmap for Product Development*. McGraw-Hill, 2003.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Best Practices in Wireless Emergency Alerts	FA8721-05-C-0003

6. AUTHOR(S)

John D. McGregor, Joseph P. Elm, Elizabeth Trocki Stark, SRA International, Inc., Jen Lavan, SRA International, Inc., Rita Creel, Chris Alberts, Carol Woody, Robert Ellison, Tamara Marshall-Keim

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-SR-015

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report presents four best practices for the Wireless Emergency Alerts (WEA) program. These best practices were identified through interviews with emergency management agencies across the United States. The WEA "Go Live" Checklist identifies key steps that an emergency management agency should perform when implementing WEA in a local jurisdiction and provides guidance for completing each action. The WEA Training and Drilling Guide identifies the steps for preparing staff to use WEA and includes suggestions shared by alerting authorities that have implemented WEA. The WEA Governance Guide identifies steps for using or preparing to use WEA to ensure coordination between participating alerting agencies. The WEA Cybersecurity Risk Management (CSRM) Strategy describes a strategy that alert originators can use throughout WEA adoption, operations, and sustainment, as well as a set of governance activities for developing a plan to execute the CSRM. Because best practices will evolve as WEA matures and becomes more widely used, an appendix provides information on how a best practice–driven organization can search for best practices, adapt them to the local context, and adopt them for everyday use.

14. SUBJECT TERMS	15. NUMBER OF PAGES
best practices, Commercial Mobile Alert Service, CMAS, cybersecurity, emergency alerting, governance, software acquisition, software integration, Wireless Emergency Alerts, WEA	64

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL