Software Engineering Institute

Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators

The WEA Project Team

March 2014

SPECIAL REPORT
CMU/SEI-2013-SR-018

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-0000879

Table of Contents

List of Figures

List of Tables

Executive Summary

The Wireless Emergency Alerts (WEA) Research, Development, Testing, and Evaluation (RDT&E) program, formerly known as the Commercial Mobile Alert Service (CMAS) RDT&E program, is a collaborative partnership that includes the cellular industry, the Federal Communications Commission, the Federal Emergency Management Agency, and the Department of Homeland Security Science and Technology Directorate (DHS S&T). The Carnegie Mellon Software Engineering Institute supported DHS S&T by developing a cybersecurity risk management (CSRM) strategy to assure accurate, timely dissemination of alerts despite attempted or successful attacks on the cyber infrastructure that supports the WEA service.

The goal of the CSRM strategy documented in this report is to enable alert originators to identify and manage cyber threats and vulnerabilities that may affect their ability to send WEA messages. The primary audience for this report includes alert originators who plan to adopt the WEA capability. In addition, for DHS S&T, the report provides a framework for cybersecurity risk management that can be tailored and applied across the WEA alerting pipeline.[1]

The CSRM strategy describes the alert originator role in the context of the end-to-end WEA alerting pipeline, which includes four elements: alert originators, the Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN), commercial mobile service providers (CMSPs), and alert recipients. The strategy is a set of activities, in four stages, implemented to increase confidence in an organization's ability to accomplish its mission in the presence of cyber threats and vulnerabilities. The WEA CSRM strategy focuses on threats to the operational system, an assessment of the level of risk presented by these threats, and risk-mitigation actions to reduce vulnerabilities and increase resilience in the face of these threats.

In Stage 1, Prepare for Cybersecurity Analysis, an organization identifies the elements of the WEA alerting pipeline and the system's life-cycle phases (adoption, operations, and sustainment) to consider in the cybersecurity analysis, describes the operational environment, and documents WEA mission threads that illustrate a system's behavior in responding to an incident or executing a mission. A generic operational mission thread for the WEA capability traces the alerting process from initiation of an alert by a first responder to dissemination to intended recipients.

In Stage 2, Conduct Cybersecurity Analysis, an organization examines the mission thread to identify operational steps and assets that might be vulnerable to cyber threats. Each step in the mission thread is analyzed to identify assets that are critical to the mission thread as well as potential threats and vulnerabilities that may make the assets susceptible to attack. The CSRM strategy uses the STRIDE Threat Model, developed by Microsoft, to identify threats [Microsoft 2005, Howard 2006]. STRIDE includes six categories of threats (its name is formed from the first letters of the category names): spoofing, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. Examples illustrate a STRIDE analysis of the generic mission

[1] The *CMAS Alerting Pipeline Taxonomy* describes in detail a hierarchical classification that encompasses the following four elements of the alerting pipeline: alert originator, IPAWS, CMSPs, and alert recipients [SEI 2012a].

thread as well as an approach that alert originators can use to tailor the mission thread and cybersecurity analysis to fit their particular environments.

In Stage 3, Assess and Prioritize Cybersecurity Risks, an organization assesses the identified threats and vulnerabilities to determine the level of risk presented to WEA operations. The organization then evaluates risks in terms of their likelihood of occurrence and potential impact on operations. Alerting organizations cannot act against all threats or identify and remove all vulnerabilities. Therefore, they should give the most serious risks, those with the potential to disrupt operations, the highest priority when allocating risk-mitigation resources. Examples of risk assessment, prioritization, and mitigation requirements are provided for four risks.

In Stage 4, Mitigate Cybersecurity Risks Throughout the Life Cycle, an organization uses the results of its cybersecurity analysis and risk assessments to define a set of cybersecurity roles and to assign cybersecurity risk-mitigation actions that match the roles within the organization. In this stage, an organization also determines when in the life cycle to perform the mitigation actions.

An organization will need to plan for the activities described in the CSRM strategy and integrate them into existing organizational processes. This report provides guidance for developing and sustaining a risk management plan that encompasses the CSRM strategy and governance activities and processes specific to the alert originator's organization. This guidance leverages the significant body of cybersecurity best practices that exist, as applicable to alert originators.

The report also includes supplemental materials to provide more information about the research approach and the specific methods that alert originators can apply in executing the CSRM strategy. Appendix A reports observations from interviews with stakeholders and vendors about their current security practices and plans for adopting and using the WEA service. Appendix B explains the mission thread analysis methodology and includes complete examples. Appendix C lists common software weaknesses that lead to exploitable vulnerabilities. Appendix D provides the cybersecurity risk analysis methodology along with complete examples. Appendix E contains a list of decisions that alert originators might make about WEA adoption, operations, and sustainment that affect cybersecurity risk. Appendix F describes cybersecurity tasks for alert originators during WEA adoption. And Appendix G includes sample CSRM planning activities that alerting organizations can tailor to meet their WEA cybersecurity risk management needs.

Stakeholders operating within each element of the alerting pipeline have responsibilities for assuring secure, resilient operations. Although this report focuses on a strategy for cybersecurity risk management from the perspective of alert originators, an organization within any element of the pipeline could tailor and apply this strategy to its own environment. And while alert originators do not have control over the entire pipeline, they need to understand the issues that may unfold throughout the pipeline so that they can respond appropriately. This strategy should be a useful aid to assuring cyber-resilient operations of the WEA capability and of future alerting and emergency management technologies.

Abstract

The Wireless Emergency Alerts (WEA) service depends on computer systems and networks to convey potentially life-saving information to the public in a timely manner. However, like other cyber-enabled services, it is susceptible to risks that may enable attackers to disseminate unauthorized alerts or to delay, modify, or destroy valid alerts. Successful attacks may result in property destruction, financial loss, injury, or death and may damage WEA credibility to the extent that users ignore future alerts or disable alerting. This report describes a four-stage cybersecurity risk management (CSRM) 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. In Stage 1, alert originators document mission threads, describing the process for generating WEA messages. In Stage 2, they examine the mission threads to identify threats and vulnerabilities. In Stage 3, they use the identified threats and vulnerabilities to assess and prioritize risks according to their likely impact on WEA operations. Finally, in Stage 4, they use the results of risk assessment to define cybersecurity roles and assign risk-mitigation actions. The four stages are repeated periodically and as procedures, threats, technology, and staff assignments change.

1 Introduction

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), is a collaborative partnership that includes the cellular industry, the Federal Communications Commission (FCC), the Federal Emergency Management Agency (FEMA), and the Department of Homeland Security Science and Technology Directorate (DHS S&T). The Carnegie Mellon® Software Engineering Institute (SEI) supported DHS S&T by developing an integration strategy and associated artifacts to facilitate the successful deployment, operations, and sustainment of the WEA capability, with a special focus on the needs of alert originators [FEMA 2012a].

The WEA capability provides a valuable service, disseminating emergency alerts to users of capable mobile devices if they are located in or travel to an affected geographic area. However, like other cyber-enabled services, WEA is subject to cyber threats that may prevent its use or damage the credibility of the service it provides. Attackers may attempt to delay, destroy, or modify alerts, or even to insert false alerts, actions that may pose a significant risk to the public. Non-adversarial sources of failure also exist, for example, design flaws, user errors, or acts of nature that compromise operations.

1.1 The WEA Alerting Pipeline and Cybersecurity Risk

The end-to-end WEA alerting pipeline consists of four major elements that implement the alerting process. These elements are shown in Figure 1.

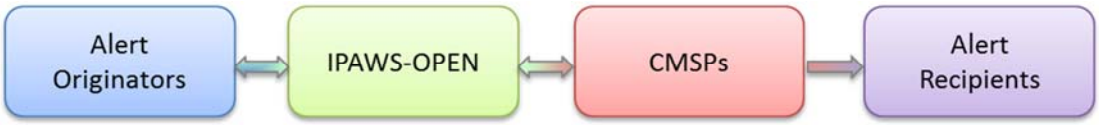


Figure 1: The Four Elements of the WEA Alerting Pipeline

The *alert originators* element consists of the people, information, technology, and facilities that initiate and create an alert, define a target distribution area, and convert the alert information into the Common Alerting Protocol (CAP) format accepted by the Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN) element. The alert originators element also includes alert origination service providers (AOSPs). An AOSP, which may be internal or external to the emergency manager's organization, provides the interface to the IPAWS-OPEN element. The *IPAWS-OPEN* element receives, validates, authenticates, and routes various types of alerts to the appropriate disseminator, such as WEA, the Emergency Alert System (EAS), or the National Oceanic and Atmospheric Administration. For WEA, IPAWS-OPEN translates CAP messages into Commercial Mobile Alert for C Interface (CMAC) format and transmits them to the commercial mobile service providers (CMSPs) element. The *CMSPs* element broadcasts alerts to *alert recipients*, the WEA-capable mobile devices located in the targeted alert area.

WEA alerting pipeline elements are implemented using mechanisms that are subject to cyber threats and vulnerabilities. Networks (wireless and wired), anticipated use of web interfaces by

AOSPs, and other technology choices will enable many organizations to integrate the WEA capability into their existing suites of emergency management services. At the same time, these technologies introduce risks that organizations must acknowledge and manage. For example, alert originators may wish to initiate alerts from a variety of devices, including mobile devices as well as devices physically located within emergency operations centers (EOCs). How will the alert origination system (AOS) authenticate their identities without fail? If authentication erroneously fails, how will alert originators transmit urgent WEA messages? If a part of the IPAWS or CMSP infrastructure is compromised, will the alert originator have an alternative dissemination path? When users of WEA-capable mobile devices receive alerts, how will they know that the alert is authentic and not spoofed? How can an organization mitigate the risk that cyber threats and vulnerabilities will disrupt the alerting process?

1.2 About the Cybersecurity Risk Management Strategy

As described above, cybersecurity risks span the WEA pipeline. While the cybersecurity risk management (CSRM) strategy described in this report can be applied to all pipeline elements, the examples and information provided focus on the alert originator element, the first line of defense against cyber threats to the WEA capability. The CSRM strategy will enable alert originators to identify and manage cyber threats and vulnerabilities that may affect their ability to send WEA messages. The end goal is to assure accurate, timely dissemination of alerts to intended recipients despite attempted attacks on the cyber infrastructure that supports the WEA service.

The CSRM strategy includes four stages: prepare for cybersecurity analysis, identify cyber threats and vulnerabilities, assess and prioritize cybersecurity risks, and mitigate cybersecurity risks. In developing the strategy, the SEI analyzed information from interviews with emergency management stakeholders (summarized in Appendix A) to determine common practices, concerns, and needs; reviewed publicly available information about WEA architecture and requirements; and studied existing practices for cyber resilience. This report builds on these information sources to create a CSRM strategy tailored for application to the alert originator's environment.

1.3 About This Report

1.3.1 Intended Audience

The primary audience for this report includes alert originators who plan to adopt the WEA capability. For alert originators, the CSRM strategy creates awareness of the cybersecurity risks to the WEA service and provides an approach they can use to manage risks specific to their own operational environments. In addition, for DHS S&T, the CSRM strategy provides a framework for understanding and managing cybersecurity risks across the elements of the end-to-end WEA alerting pipeline, including alert originators, IPAWS-OPEN, CMSPs, and alert recipients. Understanding common threats and vulnerabilities and the steps that organizations can take to manage risks will enhance the cyber resilience of WEA operations.

This report assumes that most alert originators, especially those within smaller organizational units, are focused primarily on operations and may not be equipped to assess cybersecurity risk or determine how to manage it without technical assistance. We refer to alert originators throughout the report because they are ultimately responsible for the cybersecurity of their WEA services, even if they outsource the cybersecurity analysis. We also use role names such as "executive

manager" and "personnel manager" to refer to different roles within the alert-originating organization. We recognize that different organizations use different role names, so alert originators should determine what roles in their organization correspond and replace our role names with their own.

1.3.2 Relationship to Other Reports

This report, *WEA CSRM Strategy for Alert Originators*, is the third product of the SEI effort in support of WEA, following two other reports, the *Commercial Mobile Alert Service Alerting Pipeline Taxonomy* and the *Commercial Mobile Alert Service Scenarios* [SEI 2012a, 2012b]. The CSRM strategy used the taxonomy report to define the four elements of the WEA alerting pipeline. And the CSRM strategy used information from the scenarios report to develop operational mission threads that alert originators can adapt and analyze to identify cybersecurity threats and vulnerabilities in their environments. The fourth product of the SEI effort in support of WEA is the *Study of Integration Strategy Considerations for Wireless Emergency Alerts* [SEI 2013], which includes the WEA CSRM strategy in its recommendations for alert originators who are building or buying a WEA solution and integrating it into their alerting toolbox. Finally, *Best Practices in Wireless Emergency Alerts* [McGregor 2013] summarizes best practices in four WEA-related topics, including the CSRM strategy.

1.3.3 Organization of This Report

Section 2 provides an overview of the four-stage WEA CSRM strategy. Sections 3–6 describe each stage in depth, including specific examples of methods applicable to each stage and how to apply them. Section 3 introduces a *mission thread*, a set of steps describing the WEA environmental context and alert-generation process. Section 4 demonstrates use of the mission thread to identify critical WEA assets, common cyber threats to these assets, and vulnerabilities that make the assets susceptible to threats. Section 5 analyzes and prioritizes the risks arising from identified threats and vulnerabilities. Section 6 defines mitigation roles and responsibilities for these risks.

Successful application of the CSRM strategy requires comprehensive planning and monitoring execution to ensure effectiveness. Section 7 introduces guidelines for building and sustaining a plan for executing the CSRM strategy. Finally, Section 8 provides a brief conclusion and suggested next steps. The report also includes several supporting appendixes, an acronym list, a glossary of key terms and concepts, and a reference list.

2 WEA Cybersecurity Risk Management Strategy Overview

Figure 2 illustrates the four-stage CSRM strategy detailed in Sections 3–6. Each stage builds on work done in the previous stage and is repeated as needed in response to changes that impact the work of that stage.

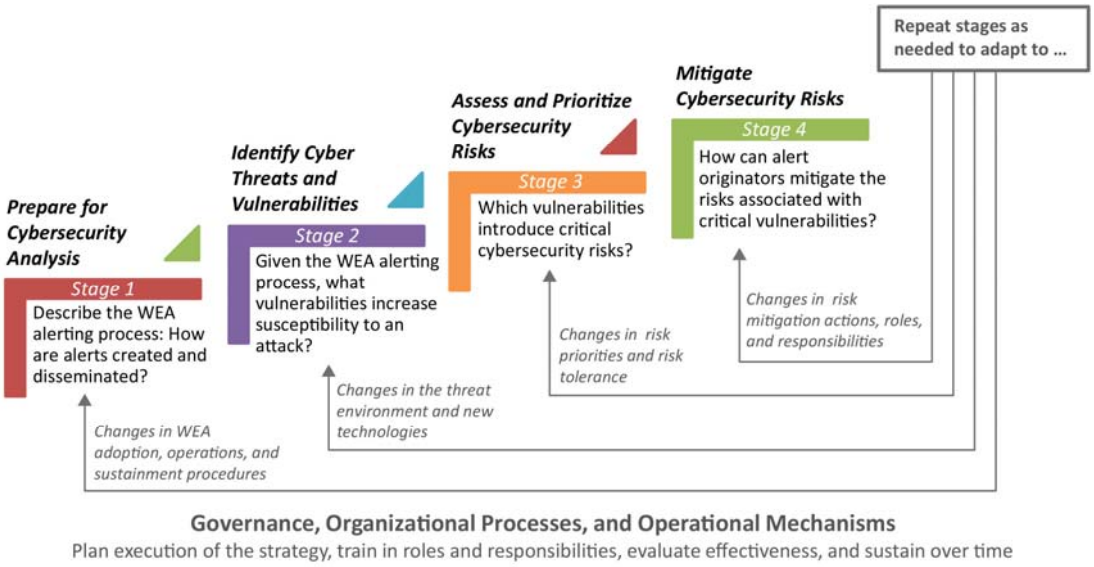


Figure 2: Four-Stage CSRM Strategy

Stage 1: Prepare for Cybersecurity Analysis

In Stage 1, alert originators prepare for cybersecurity analysis by developing a complete description of the WEA alerting process for their environments that they can analyze. This description, called a *mission thread*, includes participants in the alerting process, assumptions about the environment, and the end-to-end set of steps executed in generating alerts.

Stage 2: Identify Cyber Threats and Vulnerabilities

In Stage 2, alert originators analyze the mission thread steps documented in Stage 1 to identify cyber threats to the alerting process and vulnerabilities that make the alerting capability susceptible to an attack. First, for each step, they list the assets—information, people, technologies, and facilities—that are critical to the mission thread. Next, they identify potential threats in each mission step along with the vulnerabilities that may make the WEA capability susceptible to attack. Many methods exist for this type of threat and vulnerability identification. This report uses the STRIDE Threat Model as an example [Microsoft 2005, Howard 2006]. STRIDE includes six categories of threats and derives its name from the first letter in each category: spoofing, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. Qualified security analysts should assist in threat and vulnerability identification.

Stage 3: Assess and Prioritize Cybersecurity Risks

It is not possible to act against all threats or to identify and remove all vulnerabilities. Therefore, when allocating risk-mitigation resources, an organization should assign highest priority to the most serious risks, those with the potential to disrupt operations. In Stage 3, qualified security analysts review the threats and vulnerabilities identified in Stage 2 and articulate the associated risks. They assess and prioritize these risks in terms of their likelihood of occurrence and impact on operations if the risks are realized.

This prioritized list of risks provides a basis for identifying and prioritizing software, hardware, and procedural security risk-mitigation requirements. Another source of risk-mitigation requirements for alert originators is the set of rules of behavior documented in the Memorandum of Agreement (MOA) with IPAWS-OPEN that the alert originator executes with FEMA. These rules of behavior specify expected security practices that also mitigate risk.

Specifically for WEA, a number of documents exist that contain security requirements or recommended security practices. However, because WEA is a complex, collaborative effort, no single authoritative source for security requirements exists that reflects the current operational realities for all elements in the alerting pipeline. Although alert originators do not control all elements in the pipeline, they should consider how compromises to the other elements could affect their own ability to disseminate alerts, and they should identify risk-mitigation requirements accordingly.

Stage 4: Mitigate Cybersecurity Risks

In Stage 4, the alert originator assigns the cybersecurity risk-mitigation responsibilities identified in Stage 3 to roles within the alert-originating organization. Roles include, for example, executive manager (i.e., the central decision-making role for the alert originator's organization), operations manager, information technology (IT) staff, system administrator, and operator.

Plan and Sustain WEA Cybersecurity Risk Management

For the CSRM strategy to be effective, the alert originator should develop a plan for its use and sustainment. The plan should be communicated through the appropriate organizational channels, for example, information sessions, policies and procedures, and training for those assigned specific roles and responsibilities. As alert originators execute the strategy, they should evaluate its effectiveness and identify and implement needed adjustments.

Sustaining and refreshing the CSRM strategy are critically important activities. Threats and attack methods continually evolve, and technology upgrades and changes in procedures and staff may introduce new vulnerabilities throughout the alerting pipeline. Therefore, it is necessary to repeat Stage 1 to revise the mission thread when operational procedures change, Stage 2 to reevaluate threats and vulnerabilities based on the revised mission thread, Stage 3 to update the risk assessment, and Stage 4 to update risk-mitigation roles and responsibilities. This continuous approach to risk management will assure that the strategy accounts for evolving sources of cybersecurity risk.

3 Prepare for Cybersecurity Analysis

Alert originators prepare for cybersecurity analysis by defining the scope of the analysis, including the life-cycle phase, assets, environment, and procedures to be analyzed. They should document this information in a structured format that facilitates analysis. One such format is called a *mission thread*. A mission thread is a set of steps taken to respond to an incident or execute a mission. A mission thread description for alerting includes the EMA's environment, a diagram illustrating the environmental context, and the organizational assets and actors involved in the steps. Defined at a high level from the perspective of an operator or user, mission threads are useful for exploring the behaviors, interactions, and properties (including security) of systems such as the cooperating systems that deliver the WEA service. This section develops a WEA mission thread for use in cybersecurity analysis.

3.1 Select the Life-Cycle Phase for Analysis

Effective cybersecurity risk management requires consideration throughout the life cycle. Three life-cycle phases are relevant to WEA cybersecurity analysis: adoption, operations, and sustainment.

Table 1 describes activities central to each phase.

Table 1: Life-Cycle Phases for WEA Implementation and Use

Life-Cycle Phase	Concerned with Activities to …
Adoption	**Acquire or develop the capability to send WEA messages.** This could include developing a system from scratch, procuring a product or service, or modifying a legacy system to incorporate the WEA capability. These activities include FEMA procedures that a prospective alert originator must agree to follow to become eligible; technical processes of analyzing and defining requirements and preparing technical inputs to acquisition; acquisition analysis and procurement decision making; development monitoring and risk management; acceptance testing; planning all aspects of deployment; and deploying the system and conducting initial checkout.
Operations	**Carry out the operational mission,** that is, generate and disseminate an imminent threat, America's Missing: Broadcasting Emergency Response (AMBER) alert, or presidential alert. These mission steps span the end-to-end WEA alerting pipeline.
Sustainment	**Sustain the WEA capability,** including tasks such as adding users, upgrading hardware or software, employing a heartbeat monitor to ensure that the system is functional, performing emergency maintenance, participating in an end-to-end test, restoring service following an outage, and managing security incidents. Some of these tasks, such as end-to-end tests, span the entire alerting pipeline while others, such as adding a user, may not.

The example mission thread in this section focuses on the operations perspective, but the alert originator may use the same approach to develop mission threads for the adoption and sustainment life-cycle phases. This mission thread was developed through the following process:

- Analyze operational scenarios from the *CMAS Concept of Operations* [FEMA 2009] and information from interviews with alert originators.
- Create example operational mission threads based on these scenarios for each of the three types of alerts—imminent threat, AMBER, and presidential.
- Create a single, generalized WEA mission thread for risk analysis based on the examples produced for the three alert types.

3.2 Identify Assets: Elements and Components of the WEA Service

To identify the assets relevant to cybersecurity analysis, the alert originator starts with the elements and components of the WEA service and their interfaces [CMSAAC 2007; FEMA 2009, 2010, 2011, 2012a, 2012b]. Figure 3 illustrates the terminology used in referring to these elements and components in this report. The WEA alerting pipeline consists of four elements: alert originators, IPAWS-OPEN, CMSPs, and alert recipients. Each pipeline element consists of two or more components. Of primary concern to alert originators is successful completion of their operational missions. The mission thread in this section describes actions of the various components as well as interactions between components needed to complete the operational mission.

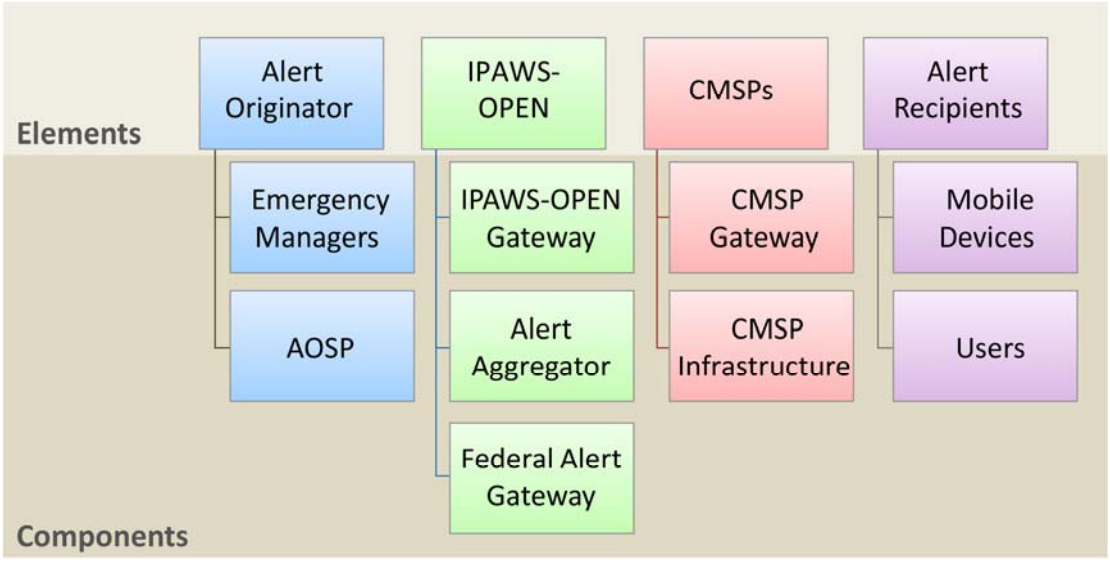


Figure 3: Elements and Components for Security Analysis of WEA Alerting Pipeline

3.3 Describe Environmental Context for the Operational Mission Thread

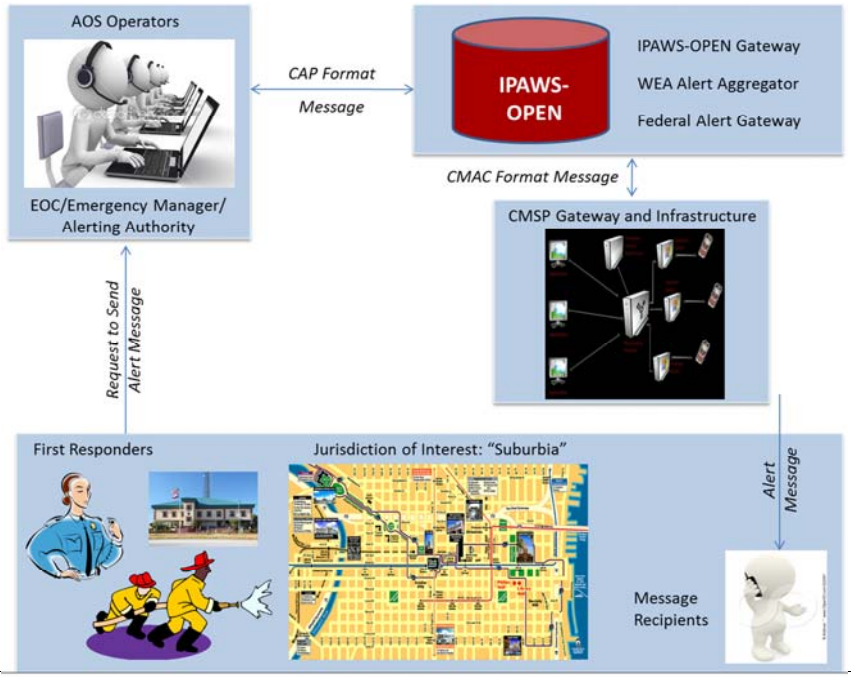
Table 2 provides an example mission thread description. Each row in the table describes an aspect of the mission thread:

- *name* – name of the mission thread
- *vignette* (summary description) – the environment before the event occurs
- *nodes and actors (assets)* – people, equipment, and facilities in the environment that may respond to or be affected by the event and one another (For the WEA mission threads, nodes and actors represent WEA elements and components.)
- *assumptions* – conditions related to the environment and characteristics of the nodes and actors that are assumed to be true at the start of the mission thread
- *environmental context diagram* – graphical representation of the environment

Alert originators should document a mission thread description for each operational mission thread that they plan to develop.

Table 2: Description for the Generic WEA Operational Mission Thread

Name	Generic Mission Thread for Emergency Alert
Vignette (Summary Description)	The city of "Suburbia" has a population of 45,000 people and covers a total area of 75 square miles. The city staffs and maintains its own fire, police, and other emergency operations facilities, including two police stations, two fire stations, and two EOCs, one staffed 24x7 and the other a hot backup. First responders attempt to provide immediate assistance in response to accidents, emergencies, and potentially dangerous situations. The city has integrated into the EOCs the ability to generate and communicate WEA messages by interfacing with the IPAWS-OPEN Gateway using an AOS. EOC staff includes qualified and authorized AOS operators. The WEA capability has been operational since May 2012, and mobile device users have successfully received mobile alerts.
Nodes and Actors (Assets)	First responders, alerting authority, AOS, AOS operators, IPAWS-OPEN Gateway, WEA Alert Aggregator, Federal Alert Gateway, CMSP Gateway, CMSP Infrastructure, mobile device users
Assumptions	**Situational** • No imminent threats have yet been identified in the region. • Today is a normal weekday, and first responders have reported to work at fire and police stations; local and regional EOC personnel have reported to work. **Organizational (staffing and procedures)** • First responders are authorized within the jurisdiction to request origination of WEA messages. • AOS operators who are responsible for issuing public alerts and warnings on behalf of their jurisdiction are authorized, are capable (trained and knowledgeable), and possess the credentials to use the WEA service. • At least two AOS operators are present to electronically sign alert messages. • An AOS systems administrator has established an account for the AOS operator and enabled audit logging. • An IPAWS systems administrator has enabled access by the AOS and enabled audit logging on applicable IPAWS components. **Technological** • The AOS has a fully operational and available WEA capability that is able to communicate with IPAWS. • IPAWS is fully operational and available to accept, process, and transmit alert messages; it consists of the IPAWS-OPEN Gateway, WEA Alert Aggregator, and Federal Alert Gateway. • The CMSP Gateway and Infrastructure are fully operational and available to accept and broadcast WEA messages. • Mobile devices are WEA-capable devices and in a state to receive alerts with adequate CMSP signal.

Environmental Context Diagram	

3.4 Document WEA Operational Mission Steps

Table 3 documents the generic mission steps that will be analyzed to identify cyber threats and vulnerabilities that may be present in the nominal alert-generation process. These mission steps were derived from the specific mission threads documented in Appendix B. The specific mission threads in the appendix also include a column indicating the clock time at which each mission step occurs. For simplicity, the generic mission thread omits the clock time since the time is not relevant to the security analysis to be performed.[2]

Table 3: Generic WEA Operational Mission Thread for Security Analysis (Nominal Path)

Mission Step	Generic Mission Step Description
1	First responder contacts local alerting authority via an approved device (cell phone, email, radio, etc.) to state that criteria are met for using the WEA service to issue, cancel, or update an alert and provides information for message.
2	Local alerting authority (person) determines that call or email is legitimate.
3	Local alerting authority instructs AOS operator to issue, cancel, or update an alert using information provided by first responder.[3]
4	AOS operator attempts to log on to the AOS.
5	AOS logon process activates auditing of the operator's session.
6	AOS operator enters alert, cancel, or update message with status of "actual."[4]
7	AOS converts message to CAP-compliant format.

[2] Mission threads are used to analyze a variety of quality attributes in addition to security. Timing is relevant for some of these, for example, performance, but is not required in this report's demonstration of security analysis.

[3] In some cases, the alerting authority and the AOS operator may be the same person.

[4] Other status values include "test" and "system" [FEMA 2010].

Mission Step	Generic Mission Step Description
8	CAP-compliant message is signed by two people.
9	AOS transmits message to the IPAWS-OPEN Gateway.
10	IPAWS-OPEN Gateway verifies[5] message and returns status message to AOS.
11	AOS operator reads status message and responds as needed.
12	IPAWS-OPEN Gateway sends message to WEA Alert Aggregator.
13	WEA Alert Aggregator verifies message and returns status to IPAWS-OPEN Gateway.
14	IPAWS-OPEN Gateway processes status and responds as needed.
15	WEA Alert Aggregator performs additional message processing.
16	WEA Alert Aggregator transmits alert to Federal Alert Gateway.
17	Federal Alert Gateway verifies message and returns status to WEA Alert Aggregator.
18	WEA Alert Aggregator processes status and responds as needed.
19	Federal Alert Gateway converts message to CMAC format.
20	Federal Alert Gateway transmits message to CMSP Gateway.
21	CMSP Gateway returns status to Federal Alert Gateway.
22	Federal Alert Gateway processes status and responds as needed.
23	CMSP Gateway sends message to CMSP Infrastructure.
24	CMSP Infrastructure sends message to mobile devices in the designated area(s).
25	Mobile device users (recipients) receive the message.

Figure 4 is a conceptual picture of the WEA alerting pipeline that illustrates where in the pipeline each mission step occurs. The next section describes a method for analyzing the mission thread steps to identify cyber threats and vulnerabilities.

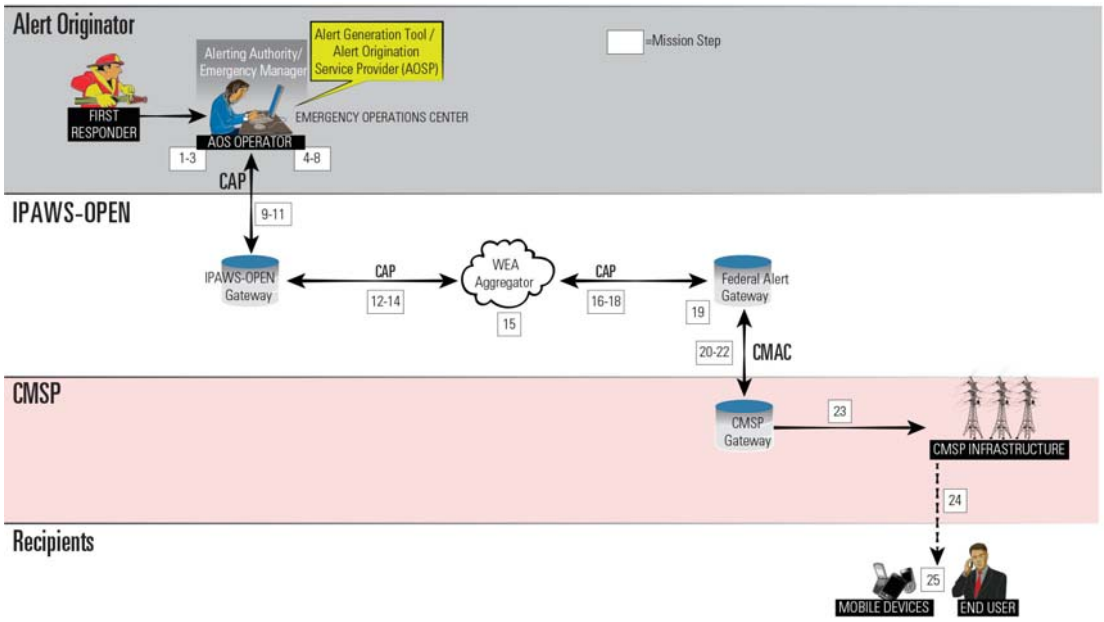


Figure 4: WEA Mission Steps Mapped to WEA Pipeline

[5] In this table, message verification includes authenticating the message and ensuring that it is correctly formatted.

4 Conduct Cybersecurity Analysis

Most approaches to cybersecurity analysis require in-depth technical knowledge of the system of interest. Yet many organizations needing to perform a top-level threat-and-vulnerability analysis, including many alert originators, do not possess sufficient expertise to use these methods. In contrast, the STRIDE Threat Model, developed by Microsoft, can be applied at various levels of granularity to identify threats and vulnerabilities for mission-critical capabilities such as emergency alerting [Microsoft 2005, Howard 2006].[6] For example, alert originators can apply it to mission thread steps to identify top-level areas of concern for cybersecurity. As needed, they can engage security analysts from other organizational units or from outside the organization to conduct more detailed analyses.

STRIDE considers the following six categories of threats[7] and derives its name from the first letter in each category:

- spoofing
- tampering with data
- repudiation
- information disclosure
- denial of service
- elevation of privilege

The STRIDE categories provide reasonable coverage of security considerations and have been applied in a broad range of environments.

Table 4 lists the Microsoft definitions for these categories along with some notes for applying the categories to WEA.

Table 4: STRIDE Threat Taxonomy Definitions and WEA Usage Notes

STRIDE Category	**Microsoft Definition** ***[adapted from Howard 2006]***	**WEA Usage Notes**
(S) Spoofing	Attacker posing as another entity, such as a user posing as another individual or a server posing as another server	Spoofing includes unauthorized access and use of authentication information as well as deliberate sending of misinformation.
(T) Tampering with data	Malicious modification of data or code, where the data or code may be at rest or in transit	*See Definition column.*

[6] With its extensive customer base, Microsoft has long been a favored target for cyber attacks. Since the early 2000s, the company has worked to develop and introduce security practices and tools to reduce vulnerabilities in its delivered products, thereby reducing the success rate of cyber attacks. Most notably, Microsoft has developed and implemented as policy the Security Development Lifecycle (SDL), which is supported by techniques and tools such as STRIDE and others [Howard 2006].

[7] Microsoft refers to these as "threat" categories while others consider them categories of attack or risk. In the literature, a threat is most often defined as the actor or agent that is the source of an attack or risk [McGraw 2006, Allen 2008, CNSSI 2010], and that is how the *CMAS Concept of Operations* defines threat [FEMA 2009, pp. 21–22]. The word *threat* has also been more broadly defined as a situation that provides the conditions for an attack, consisting of a source (actor or agent), asset, motive, access, and undesirable outcome [Alberts 2003, Caralli 2011].

STRIDE Category	Microsoft Definition *[adapted from Howard 2006]*	WEA Usage Notes
(R) Repudiation	Attacker (human) denying to have performed an action that other parties can neither confirm nor contradict (Nonrepudiation is a system's ability to counter repudiation threats, e.g., through digital signatures that can be traced to an individual.)	WEA applications need to establish sufficient proof of user actions so that denial is not viable.
(I) Information disclosure	Exposure of information to individuals who are not supposed to have access to it	Since the content of WEA messages is intended to be public, the alert messages themselves do not need to be protected from disclosure. However, account information, authentication data, and system identification data must be protected.
(D) Denial of service	Attacks that deny or degrade access to a critical service to valid users, for example, by making servers temporarily unavailable or unusable	*See Definition column.*
(E) Elevation of privilege	Accidental or intentional condition in which a user gains system access and privileges that he or she is not supposed to have (e.g., a user taking advantage of a coding bug to gain administrative privileges) (Elevation of privilege may also apply to software applications, e.g., code that executes in a web browser with a level of permissions that enables it to launch an attack.)	*See Definition column.*

4.1 Identify Cyber Threats and Vulnerabilities Using STRIDE

To identify cyber threats and vulnerabilities, the alert originator can apply STRIDE to a mission thread as follows: For each step in the mission thread, an alert originator lists the assets used that could be compromised, posing a risk to mission success. Security analysts then examine the steps to identify threats that may be present and vulnerabilities that would render the assets susceptible to these threats.

4.1.1 Example: Apply STRIDE to the Generic Mission Thread

Table 5 illustrates application of the STRIDE method to the generic WEA mission thread. The columns in the table contain the following information:

- *mission step* – step number from the generic WEA mission thread presented in Table 3
- *mission step description* – description of the step
- *assets* – critical assets used in the step that are relevant to the STRIDE analysis
- *STRIDE threat identification examples* – specific threats to these assets, tagged with the appropriate category letter (S, T, R, I, D, and E)
- *example vulnerabilities* – common vulnerabilities that would make the assets susceptible to one or more of the threats identified in the STRIDE Threat Identification Examples column

The example vulnerabilities are drawn from the *CWE/SANS Top 25 Most Dangerous Software Errors*, a list of the most common software weaknesses that can lead to exploitable security vul-

nerabilities [SANS 2011]. This list is produced through collaboration among the SANS Institute, MITRE Corporation, and top software security experts and is regularly updated. Another source is the Open Web Application Security Project (OWASP) Top Ten Project–The Top Ten Web Application Security Risks [OWASP 2013].

The Example Vulnerabilities column in Table 5 provides information that the AOSP needs to consider during design, development, and operations of systems that the alert originator uses to interface with IPAWS. The *CWE/SANS Top 25* uses three high-level categories of weaknesses [SANS 2011]:

- Insecure Interaction Between Components: weaknesses related to insecure transmission or receipt of data between separate assets of the system, where assets can be technology items, people, processes, or facilities
- Risky Resource Management: weaknesses related to improper management and use of key system resources, for example, code and data
- Porous Defenses: weaknesses related to improper use of, or failure to use, defensive techniques

Appendix C provides more information on the weaknesses identified in the Example Vulnerabilities column.

Table 5: Security Analysis for Generic WEA Operational Mission Thread (Nominal Path)
(Shaded steps occur outside the alert originator element, i.e., in the IPAWS-OPEN, CMSP, or alert recipient elements.)

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
1	First responder contacts local alerting authority via an approved device (cell phone, email, radio, etc.) to state that criteria are met for using the WEA service to issue, cancel, or update an alert and provides information for alert message.	• Two people • Communication devices • Procedures and criteria	S: Fake first responder T: Data altered in transit I: Disclosure of authentication information D: Communications devices not operational	• Insecure Interaction Between Components • Porous Defenses – Missing encryption of sensitive data (authentication information) – Use of a broken or risky cryptographic algorithm
2	Local alerting authority (person) determines call or email is legitimate.	• One person • Authentication info	S: Connect to the wrong person T: Tampering with info used to authenticate first responder E: Insider threat or man in the middle	• Porous Defenses – Reliance on untrusted inputs
3	Local alerting authority instructs AOS operator to issue, cancel, or update an alert using information provided by first responder.	• Two people • Communication devices • Procedures and criteria	S: Fake alerting authority or AOS operator T: Tampering with data provided D: Communications are down	• Insecure Interaction Between Components
4	AOS operator attempts to log on to the AOS.	• One person • Server (valid accounts and authentication information) • Logon procedure • Logon application • Communications between logon software, server, and AOS	S: Unidentified individual attempts to log on with AOS operator's information R: AOS operator denies logon I: Capture of logon info using key logger or packet sniffer D: AOS operator's account not registered or servers are down E: Successful logon by unidentified individual	• Risky Resource Management – Inclusion of functionality from untrusted control sphere • Porous Defenses – Improper restriction of excessive authentication attempts – Authorization bypass through user-controlled key

[8] S: spoofing; T: tampering with data; R: repudiation; I: information disclosure; D: denial of service; E: elevation of privilege.

[9] See Appendix C for more information.

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
5	AOS logon activates auditing of the operator's session.	• Auditing application • Auditing procedure • Communications from accounts to auditing application • Local or remote storage	T: Logged entries deleted or modified I: Logged entries contain credential data and are leaked D: Log full or server unavailable	• Insecure Interaction Between Components – Audit files not well protected • Porous Defenses – Hard-coded credentials
6	AOS operator enters alert, cancel, or update message with status of "actual."[10]	• One person • Alert scripts • Procedures for building scripts, geotargeting, etc. • Graphical user interface (GUI) application • Communications between GUI application and alert-generation software (including server and application)	T: Formatting errors produce incorrect message, or man-in-the-middle attacker changes alert data before sending it D: Scripts not available or scripts corrupted E: Malicious insider gains access to privileges, allowing him or her to tamper with alerts	• Risky Resource Management – Uncontrolled format string • Insecure Interaction Between Components – Origin validation error • Porous Defenses – Improper restriction of logon attempts – Authorization bypass
7	AOS converts message to CAP-compliant format.	• Conversion application	T: Data is changed between the AOS and the server D: The server is down	• Risky Resource Management – Inclusion of functionality from untrusted control sphere
8	CAP-compliant message is signed by two people.	• Signature entry application • Signature validation application • Public–private key pair for every user	S: Digital signature is falsified R: User claims not to have signed D: Server goes down so keys cannot be distributed, or keys have expired and message cannot be sent	• Porous Defenses – Hard-coded credentials – Use of a broken or risky cryptographic algorithm
9	AOS transmits message to the IPAWS-OPEN Gateway.	• Application that securely connects to IPAWS • Information used to authenticate AOS and IPAWS	S: Falsified AOS CAP message or IPAWS-OPEN Gateway attacked and site is redirected T: Data within message is modified I: Message is not encrypted and credentials are visible D: IPAWS-OPEN Gateway is down	• Insecure Interaction Between Components – Cross-site request forgery – Uniform Resource Locator (URL) redirection to untrusted site

[10] Other status values include "test" and "system."

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
10	IPAWS-OPEN Gateway verifies[11] message and returns status message to AOS.	• Authentication information • Message validation scripts	S: Connect to malicious authentication tools or digital signature is falsified I: Authentication information is leaked	• Porous Defenses – Incorrect authorization ▪ Cookie-storing credentials
11	AOS operator reads status message and responds as needed.	• One person • Application that securely connects to IPAWS • Authentication information	S: Falsified CAP message T: Data within message is modified R: AOS operator repudiates message sent in Step 8 D: IPAWS-OPEN Gateway is down	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing authorization in Step 8
12	IPAWS-OPEN Gateway sends message to WEA Alert Aggregator.	• Application that securely connects to WEA Alert Aggregator • Authentication information	S: Falsified CAP message or WEA Alert Aggregator attacked and alert message redirected to another site T: Data within message is modified I: Message not encrypted and credentials are visible D: WEA Alert Aggregator is down	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Hard-coded credentials – Missing encryption of sensitive data
13	WEA Alert Aggregator verifies message and returns status to IPAWS-OPEN Gateway.	• Authentication information • Message validation scripts	S: Digital signature is falsified I: Authentication information is leaked	• Porous Defenses – Use of hard-coded credentials

[11] In this table, message verification includes authenticating the message and ensuring that it is in the correct format.

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
14	IPAWS-OPEN Gateway processes status and responds as needed.	• Application that securely connects to WEA Alert Aggregator • Authentication information	S: Falsified CAP message T: Data within message is modified I: Message not encrypted and credentials are visible	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data
15	WEA Alert Aggregator performs additional message processing.	• Messaging processing application	D: WEA Alert Aggregator is down E: Malicious insider gains access to privileges, allowing him or her to tamper with conversion application	• Risky Resource Management – Inclusion of functionality from untrusted control sphere – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data • Improper restriction of logon attempts – Authorization bypass
16	WEA Alert Aggregator transmits alert to Federal Alert Gateway.	• Application that securely connects to Federal Alert Gateway • Authentication information	S: Falsified CAP message T: Data within message is modified I: Message not encrypted and credentials are visible D: Federal Alert Gateway is down	• Insecure Interaction Between Components – Origin validation error • Porous Defenses – Missing encryption of sensitive data
17	Federal Alert Gateway verifies message and returns status to WEA Alert Aggregator.	• Authentication information • Message validation scripts	S: Digital signature is falsified I: Authentication information is leaked	• Porous Defenses – Use of hard-coded credentials

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
18	WEA Alert Aggregator processes status and responds as needed.	• Application that securely connects to Federal Alert Gateway • Authentication information	S: Falsified CAP message T: Data within the message is modified I: Message not encrypted and credentials are visible D: Federal Alert Gateway is down	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data
19	Federal Alert Gateway converts message to CMAC format.	• Message conversion application	D: Federal Alert Gateway is down E: Malicious insider gains access to privileges, allowing him or her to tamper with conversion application	• Risky Resource Management – Inclusion of functionality from untrusted control sphere – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data • Improper restriction of logon attempts – Authorization bypass
20	Federal Alert Gateway transmits message to CMSP Gateway.	• Application that securely connects to CMSP Gateway • Authentication information	S: Falsified CMAC message T: Data within message is modified I: Message not encrypted and credentials are visible D: CMSP Gateway is down	• Insecure Interaction Between Components – Direct requests • Porous Defenses – Missing encryption of sensitive data
21	CMSP Gateway returns status to Federal Alert Gateway.	• Application that securely connects to Federal Alert Gateway • Authentication information	S: Falsified CAP message T: Data within the message is modified I: Message not encrypted and credentials are visible D: Federal Alert Gateway is down	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data

Mission Step	Mission Step Description	Assets	STRIDE[8] Threat Identification Examples	Example Vulnerabilities[9]
22	Federal Alert Gateway processes status and responds as needed.	• Application that securely connects to CMSP Gateway • Authentication information	S: Falsified CMAC message T: Data within the message is modified I: Message not encrypted and credentials are visible D: CMSP Gateway is down	• Insecure Interaction Between Components – URL redirection to untrusted site • Risky Resource Management – Buffer overflow – Uncontrolled format string • Porous Defenses – Missing encryption of sensitive data
23	CMSP Gateway sends message to CMSP Infrastructure.	• CMSP Gateway • Cell towers in the geotargeted area	S: Falsified message T: Data within message is modified D: CMSP Infrastructure is down, or CMSP Gateway is down	• Insecure Interaction Between Components – URL redirection to untrusted site
24	CMSP Infrastructure sends message to mobile devices in the designated area(s).	• Cell towers in the geotargeted area	S: Falsified message T: Data within the message is modified	• Insecure Interaction Between Components
25	Mobile device users (recipients) receive the message.	• WEA-ready device	S: Falsified message received T, D: Feature of mobile device that processes message is disabled	• Insecure Interaction Between Components

4.2 Explore Mission Thread Variations

The generic operational mission thread analyzed in Section 4.1.1 provides a starting point for security analysis. To expand its usefulness to a given organization, alert originators should tailor the mission thread to reflect key implementation choices, known risks, and operational realities of the organization. This section identifies some possible variations that an organization could apply to the generic mission thread. Alert originators would tailor the mission thread steps to reflect selected variations and revisit the STRIDE analysis for the changed mission steps.

Three types of common variations and the corresponding STRIDE analyses are exemplified below: implementation choices that may affect security, cyber threats of interest, and operational limitations and procedural issues.

Variations based on implementation choices that may affect security:

- Adoption (acquisition and development) choices:
  - Web based: The AOSP's software is entirely web based and is accessible from anywhere by authorized alert originators.
  - Installed software: The AOSP's software is installed on each alert originator's computer.
  - Provided software and hardware system: The AOSP provides the alert originator with dedicated hardware running the software necessary to communicate with IPAWS.
  - Software developed internally for access to IPAWS: The alert originator's organization has developed and maintains its own software to interface with IPAWS.
- Heartbeat: The AOSP's software implements a periodic "ping" to the IPAWS-OPEN Gateway to ensure continued access to the WEA service.
- One set of credentials per shift: Every shift has a single set of valid credentials instead of credentials for each AOS operator, and any AOS operator working the shift can send a CAP message to IPAWS (this variation is analyzed in Section 4.2.1).

Variations based on specific cyber threats of interest:

- Spoofing: A CAP message is sent from an unauthorized source with stolen credentials.
- Tampering with data: An attacker captures an unencrypted CAP message as it is transmitted between components, modifies the data, and sends it forward on the right path.
- Information disclosure:
  - An attacker captures unencrypted credentials as they are transmitted between components.
  - An attacker gains access to unencrypted log files that have stored authentication information.
- URL redirection: An alert originator clicks a link to download the latest version of software but is redirected to a malicious site that installs malware (e.g., a virus, Trojan, worm, or key logger).
- Authentication attempts not restricted: An attacker uses a brute-force method to obtain an alert originator's password, enabling the attacker to log in at will.

- Hard-coded credentials: An attacker gains access to static (hard-coded) credentials such as those stored on a flash drive.
- Trusted connection compromised:
  - An AOSP site is compromised and malicious code is propagated to an originator through a software update.
  - An employee inserts a compromised device, such as a Universal Serial Bus (USB) flash drive, into a port, compromising the AOS.

Variations based on operational limitations and procedural issues:

- Authorization failure: An alert originator's credentials have expired and have not been renewed, causing IPAWS to reject an alert message.
- Countersign failure: There is either only one certified alert originator on duty or there is only one set of credentials per shift, so a CAP message cannot be countersigned and is rejected by IPAWS.[12]

4.2.1 Example: Impact of a Mission Thread Variation on STRIDE Analysis

This example illustrates the impact of a single operational variation on the STRIDE analysis. Alert originators will have site-specific limitations and may make site-specific implementation and procedural choices that affect security. As a result, they will need to tailor one or more steps in the generic mission thread to make the STRIDE analysis fully applicable to their needs. This tailoring will change what occurs in the selected step(s) and may affect the assets, threats, and vulnerabilities associated with the step(s).

In this example, a site has chosen to implement a single AOS account per shift (which may include multiple AOS operators), rather than requiring an account for each AOS operator. This implementation choice will affect Step 8 in the generic mission thread. Table 6 shows Step 8 exactly as it appeared in the generic case in Table 5.

Table 6: Mission Step 8: Generic

Mission Step	Mission Step Description	Assets	STRIDE Threat Identification Examples	Example Vulnerabilities
8	CAP-compliant message is signed by two people.	• Signature entry application • Signature validation application • Public–private key pair for every user	S: Digital signature is falsified R: User claims not to have signed D: Server goes down so keys cannot be distributed, or keys have expired and message cannot be sent	• Porous Defenses - Hard-coded credentials - Use of a broken or risky cryptographic algorithm

It is a recommended practice to require separate accounts for each AOS operator and to have CAP-compliant messages signed by two distinct operators. However, some alert-originating organizations require only a single account per shift, which may include multiple operators. There-

[12] Currently, a countersignature is not required but is a recommended practice. However, this may become a requirement in the future.

fore, instead of associating a digital signature with each authorized alert originator, some alert-originating organizations associate a single digital signature with each shift of personnel.

Table 7 illustrates how an alert originator might choose to adjust Step 8 to reflect the operational environment and the impact that the adjustments would have on the STRIDE analysis. As an example, from a security standpoint if there is only one account (and one digital signature) available per shift, with multiple AOS operators using the account, this practice affects the threat of repudiation. Changes to the analysis of the generic mission thread are indicated in red italicized type. Note that the assets vary only slightly. There is now a public–private key pair for each shift instead of for each user. As a result, the STRIDE analysis changes for repudiation-related threats. The alert-originating organization cannot trace the message back to a single user because no digital record proves which operator sent the message, only that it was sent during a particular shift. Therefore, if an alert originator wants to deny (repudiate) sending a message, there is no audit trail available to counter that denial.

Table 7: Mission Step 8: Site-Specific Tailoring

Mission Step	Mission Step Description	Assets	STRIDE Threat Identification Examples	Example Vulnerabilities
8	CAP-compliant message is signed *by a single user ID that is unique to a shift time and not to an individual.*	• Signature entry application • Signature validation application • Public–private key pair for every *shift*	S: Digital signature is falsified R: User claims not to have signed *(All users on shift can repudiate messages with a very high success rate, since no digital proof exists to tie actions to an individual.)* D: Server goes down so keys cannot be distributed, or keys have expired and message cannot be sent	• Porous Defenses – Hard-coded credentials – Use of a broken or risky cryptographic algorithm *Risky Resource Management* – *Single digital signature for multiple users*

With this operational variation, an additional vulnerability exists for Step 8 because the alert-originating organization cannot hold any individual user accountable for messages sent by the AOS.

5 Assess and Prioritize Cybersecurity Risks

This section illustrates how the alert originator can use threats and vulnerabilities identified through the STRIDE method (see Section 4) to document, assess, and prioritize cybersecurity risks to the WEA operational mission. Alert originators analyze each risk to determine its probability of occurrence and impact on the WEA service if the risk is realized. Then, they use this information to prioritize the risks and determine which they need to control. This provides a basis for implementing software, hardware, and procedural security risk-mitigation requirements.

Appendix D describes the cybersecurity risk analysis method that is applied in this section to document and analyze cybersecurity risks for the WEA service and provides a complete set of data for each risk scenario. This section summarizes the results of applying the method, focusing on risks to alert originators. Figure 5 illustrates how risks can be derived from the threats and vulnerabilities identified in Section 4. As previously defined, the threat is the actor or agent that is the source of an attack. A vulnerability is a weakness in the system or the procedures used to implement and sustain it. A threat without a vulnerability, or a vulnerability without a threat, does not pose risk. The combination of the threat and the vulnerability creates risk.

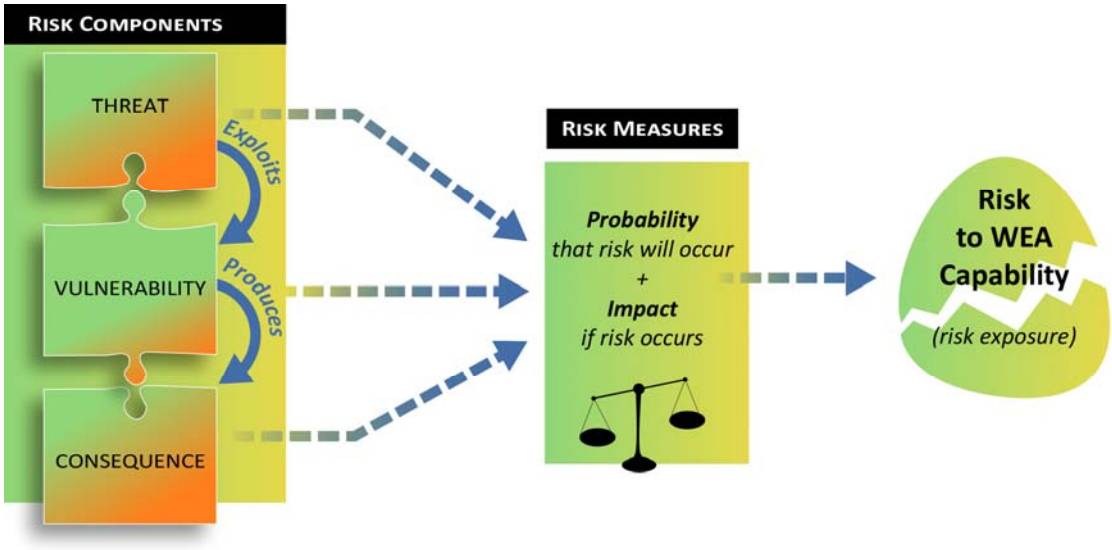


Figure 5: Relationship of Risks to Threats and Vulnerabilities

5.1 Document and Assess Cybersecurity Risks

We selected four risks for assessment based on the cyber threats and vulnerabilities identified through the STRIDE analysis (Table 5):

- Risk 1: Maliciously Sent CAP-Compliant Message (Table 5, Steps 6, 8, and 9)
- Risk 2: Denial of Service from Malicious Code (Table 5, Steps 4–7)
- Risk 3: Insider Spoofing Colleague's Identity (Table 5, Steps 1–4, 8, and 9)
- Risk 4: Unavailable Communication Channel (Table 5, Step 9)

These risks provide a broad cross section of the types of issues likely to affect the WEA service. The underlying threats that trigger these four risks include an outside attacker (Risk 1), denial of service due to malicious code (Risk 2), an inside attacker (Risk 3), and a failure due to an unavailable communication channel (Risk 4). While not exhaustive, the resulting analysis provides a broad range of mitigation requirements that alert originators should consider. The remainder of this section describes each risk and the SEI team's assessment.

5.1.1 Risk 1: Maliciously Sent CAP-Compliant Message

An outside attacker with malicious intent decides to obtain a valid certificate and use it to send an illegitimate CAP-compliant message. The attacker's goal is to send people to a dangerous location, hoping to inflict physical and emotional harm on them. The key to this attack is capturing a valid certificate from an alert originator. Figure 6 illustrates the key elements of this risk.[13]

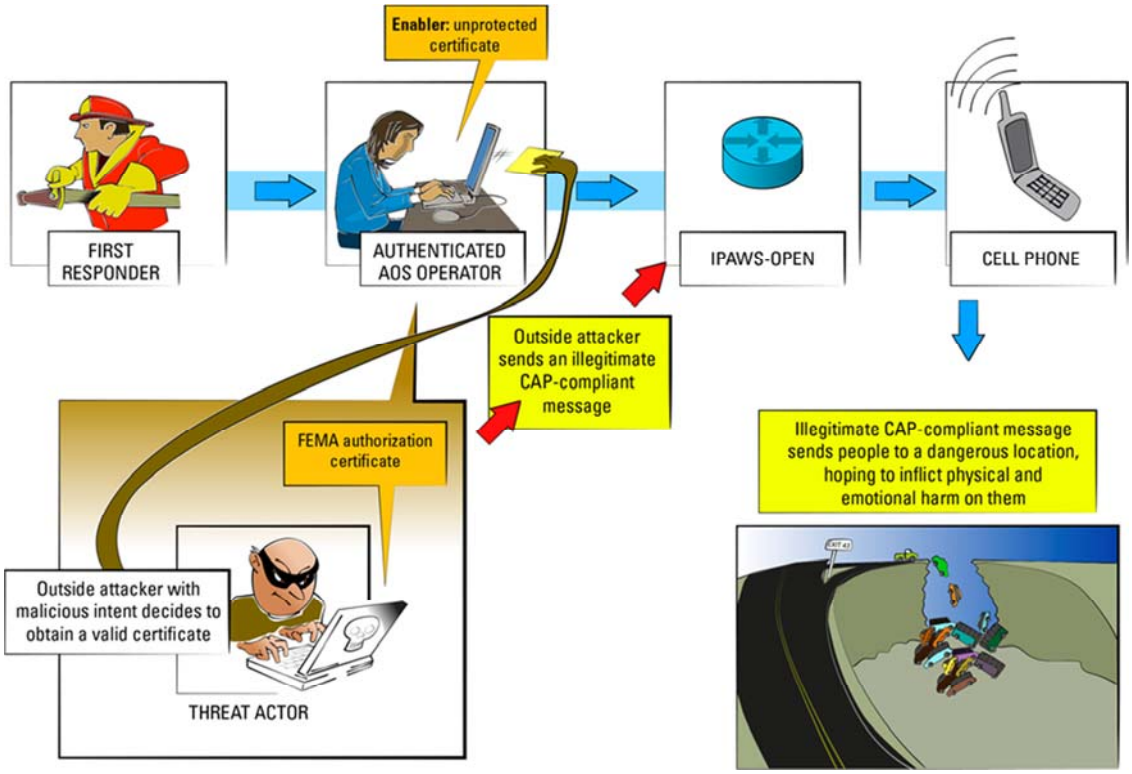


Figure 6: Risk 1: Maliciously Sent CAP-Compliant Message

The attacker develops two strategies for capturing a valid certificate. The first strategy targets an alert originator directly. The second strategy focuses on AOS vendors that provide the WEA capability as a service. When the capability is outsourced in this way, the IPAWS-OPEN MOA provides for security certificates to be given to the vendor. Targeting a vendor could be a particularly fruitful strategy for the attacker. Since only a small number of vendors provide the WEA capability, each vendor may control a large number of certificates. A compromised vendor could provide an attacker with many potential organizations to target.

[13] The pipeline shown at the top of the four figures featured in this section is a simplified view of the WEA pipeline. It emphasizes the elements of the WEA pipeline that are most relevant to alert originators. As a result, the CMSP element of the WEA pipeline is omitted from these figures.

No matter which strategy is pursued, the attacker looks for vulnerabilities (i.e., weaknesses) in technologies or procedures that can be exploited. For example, the attacker will try to find vulnerabilities that expose certificates to exploit, such as

- unmonitored access to certificates
- lack of encryption controls for certificates during transit and storage
- lack of role-based access to certificates

The attacker might also explore social engineering techniques to obtain a certificate. Here, the attacker attempts to manipulate someone from the alert originator or vendor organization into providing access to a legitimate certificate or to get information that will be useful in the attacker's quest to get a certificate.

Obtaining a certificate is not a simple endeavor. The attacker has to be sufficiently motivated and skilled to achieve this interim goal. However, once this part of the scenario is complete, the attacker is well positioned to send an illegitimate CAP-compliant message. The attacker has easy access to publicly documented information defining how to construct CAP-compliant messages.

The attacker's goal in this risk is to send people to a location that will put them in harm's way. To maximize the impact, the attacker takes advantage of an impending event (e.g., weather event, natural disaster). Because people likely will verify WEA messages through other channels, synchronizing the attack with an impending event makes it more likely that people will follow the attacker's instructions.

We expect that a successful attack of this nature will be a rare occurrence because it requires a complex sequence of events to occur. In addition, the attacker has to be highly motivated and skilled to carry out this scenario successfully. Finally, the WEA service needs to have an established track record of success for this scenario to be realized. Otherwise, people might not be inclined to follow the instructions provided in the illegitimate CAP-compliant message.

This scenario could produce catastrophic consequences, depending on the severity of the event with which the attack is linked. Health and safety damages could be significant, leading to potentially large legal liabilities. Such an attack could damage the reputation of the WEA service beyond repair.

5.1.2 Risk 2: Denial of Service from Malicious Code

Figure 7 depicts the second risk scenario. Here, malicious code prevents an operator from entering an alert into the AOS. In this scenario, the AOS is not a specific target of the attack. Malicious code is downloaded to the AOS accidentally. A system can become infected with malicious code in several ways:

- Removable media (e.g., USB drives, CDs) are compromised with malicious code. A staff member from the alert originator who uses the compromised media infects his or her computer. The malicious code eventually propagates to the AOS.
- A staff member at the alert originator accesses a compromised website, which infects his or her computer. The malicious code eventually propagates to the AOS.
- The vendor's computers could be compromised. The malicious code eventually propagates to the AOS.

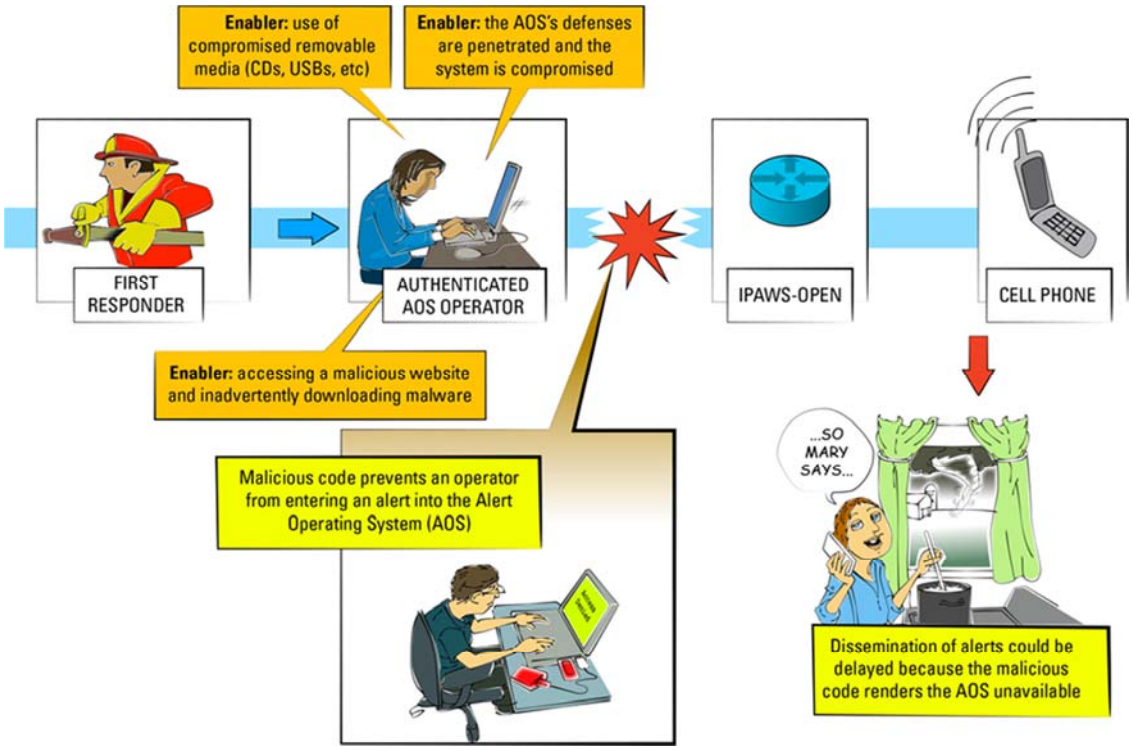


Figure 7: Risk 2: Denial of Service from Malicious Code

This type of attack could delay the dissemination of alerts because the malicious code renders the AOS unavailable to operators or restricts the number of operators who can enter alerts. In addition, the malicious code could be sent to IPAWS, affecting the availability of IPAWS to all alert originators. Ultimately, the attack could adversely affect public health and safety because people would not receive alerts in a timely manner. The alert-originating organization could incur substantial tangible as well as intangible costs as it recovers from this attack. Tangible costs include the cost to respond to and recover from the attack, including labor and materials to remove the malicious code and deal with its effects. Intangible costs include eroded confidence in the WEA service.

We consider this risk scenario to have a remote probability of occurrence, if alert originators take certain precautions. For example, alert-originating organizations may limit the use of equipment to work-related activities; vendors may implement adequate security controls; and the MOA with FEMA may be used to enforce security controls. However, the probability of occurrence could increase over time if organizations are not vigilant about maintaining an acceptable level of security.

The consequences of this risk scenario are low to moderate in severity. The extent of the impact will depend on the effectiveness of an organization's contingency plans. For example, if an alert originator has multiple channels for distributing alerts, then people will be able to receive alerts from sources other than the WEA service, such as through text messages or electronic mail, so the risk seems low. However, individuals generally need to register for these services. If people travel to an area where they are not registered for an alerting service, they would still receive WEA mes-

sages if they have WEA-enabled devices. In this case, if the WEA service is compromised, they will not receive any alerts. This suggests a moderate severity for the risk.

5.1.3 Risk 3: Insider Spoofing Colleague's Identity

In the third risk scenario, an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message under the colleague's name. Here, the insider's goal is to damage a colleague's reputation among his or her peers and managers. This scenario is graphically depicted in Figure 8.

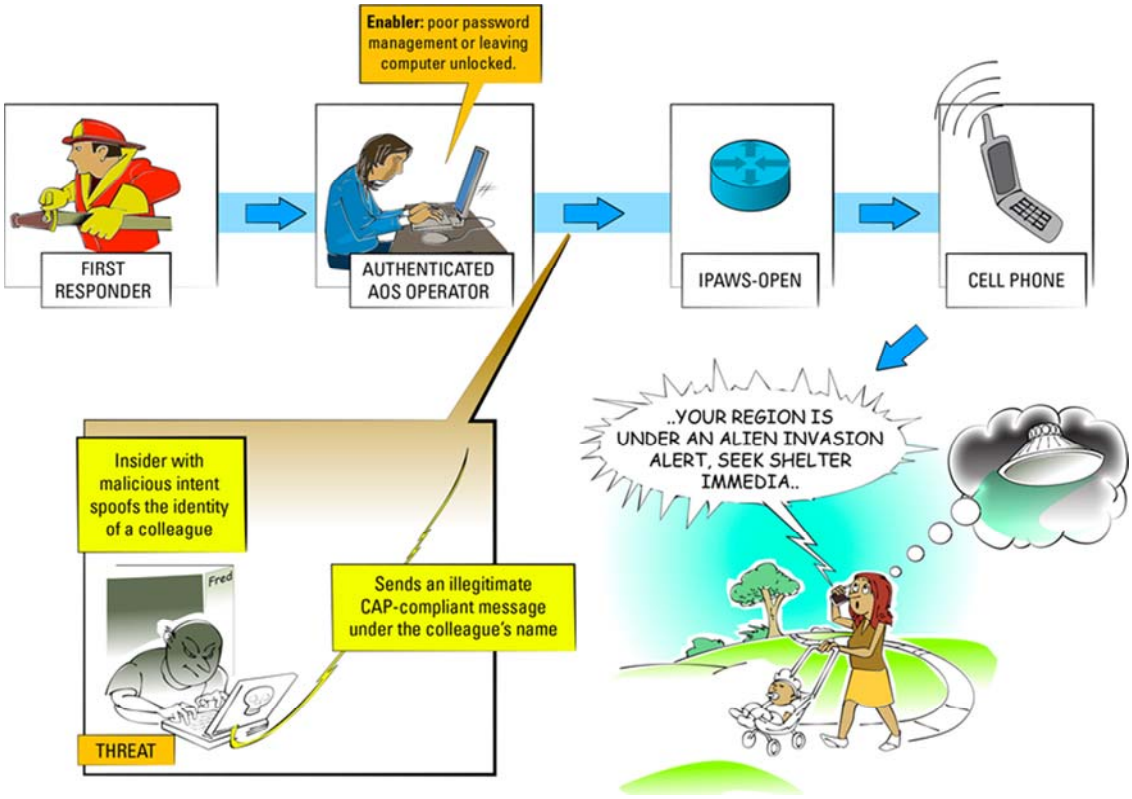


Figure 8: Risk 3: Insider Spoofing Colleague's Identity

Many circumstances can help enable this risk to occur:

- Key loggers or packet sniffers could capture legitimate access information.
- Lack of individualized authentication could enable the insider to spoof a colleague's identity.
- Poor management of passwords (e.g., writing a password on a sticky note and putting it in a visible location) could enable an insider to gain unauthorized access to a colleague's account.
- The insider could have physical access to the colleague's unlocked computer when the colleague is away from his or her desk.
- Unprotected log files could allow the insider to tamper with the files and delete or modify entries.
- The insider could use social engineering techniques to obtain authentication information from the vendor.

- Authentication files could be inadequately protected in the vendor's software.

When realized, this risk has multiple victims: the alert originator whose identity was spoofed and the recipients of the illegitimate WEA message. If this risk were to occur, the alert originator could be perceived as doing a poor job (i.e., sending out illegitimate messages to recipients). Management might require the victim to spend time contacting recipients of the illegitimate message as part of the organization's recovery efforts. The organization could initiate disciplinary actions against the alert originator for sending out illegitimate messages. Ultimately, this type of attack could damage the alert originator's reputation with the public. Also, depending on the content of the illegitimate WEA message, alert recipients could be placed in danger (e.g., if the message sends them to a dangerous location) or incur costs because of the action they take based on the message (e.g., if they do not report to work because of a false alert message that instructs them to shelter in place).

We consider this risk scenario to have a rare to remote likelihood of occurrence. This risk comprises a fairly complex sequence of events and requires a highly motivated insider. In addition, people who are given access to systems at sites normally go through a clearance process, which helps to mitigate this risk. Finally, in some instances dual signatures are required to send an alert, making it extremely difficult for a person to send an alert by himself or herself. If an organization requires dual signatures to send an alert, the insider needs a conspirator to carry out this attack, making it less likely to occur.

The consequences of this scenario are moderate in severity. The alerts that an insider might send out in this type of attack would probably be relatively innocuous; these false alerts likely will not put the health or safety of people in jeopardy. However, people's confidence in the WEA service could be significantly reduced as a result of this scenario.

5.1.4 Risk 4: Unavailable Communication Channel

Figure 9 depicts the final risk scenario, in which the internet communication channel for the AOS is unavailable due to a successful cybersecurity attack on the AOS's internet service provider (ISP).[14] In this scenario, pre-established, secure backup communication channels (e.g., satellite, direct communication) are inadequate or nonexistent.

[14] This risk is an example of an *inherited* cybersecurity risk. Because modern systems are interconnected, an organization can experience a loss resulting from a successful cybersecurity attack on a collaborator, partner, or service provider. An effective risk management strategy requires an organization to implement actions that mitigate the effects of inherited cybersecurity risks.

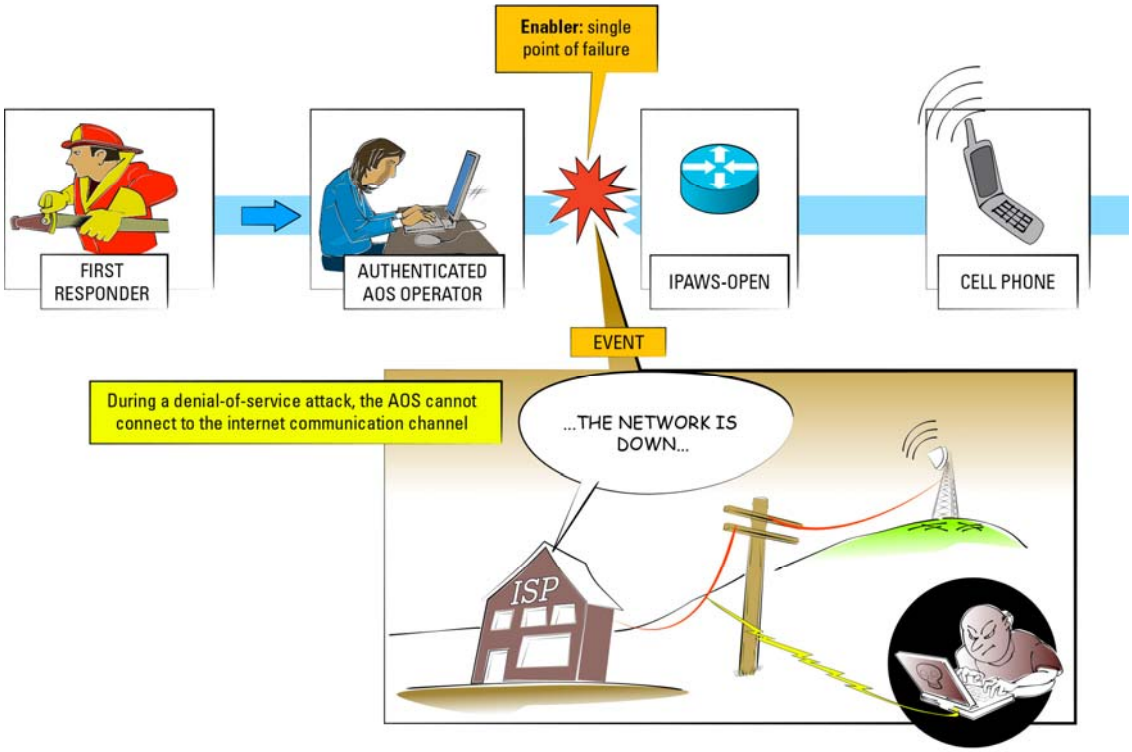


Figure 9: Risk 4: Unavailable Communication Channel

An unavailable communication channel could prevent an organization from sending alert messages to IPAWS. This would delay the dissemination of alerts, or recipients might not receive alert messages at all. Delays in disseminating alerts to the WEA constituency could adversely affect public health and safety.

We consider this risk scenario to have a remote probability of occurrence. Internet unavailability resulting from cybersecurity attacks on ISPs occurs on occasion. However, this risk requires that internet unavailability coincide with an emergency situation for which an organization would issue a WEA message. Emergency situations requiring WEA messages may occur only a handful of times per year.

The consequences of this risk scenario are low to moderate in severity. The analysis is similar to that for Risk 2, Denial of Service from Malicious Code, since both risks affect the outcome in the same way: they prevent timely dissemination of the alert by breaking the link between the AOS and IPAWS-OPEN, disrupting the WEA service.

5.2 Prioritize Risks

Table 8 summarizes the four risks identified for alert originators in priority order. In prioritizing the four risks, we applied the following guidelines (see Appendix D for additional information):

- Impact is the primary factor for prioritizing cybersecurity risks. Risks with the largest impacts have the highest priority.

- Probability is the secondary factor for prioritizing cybersecurity risks. Probability is used to prioritize risks that have equal impacts. Risks of equal impact with the largest probabilities are the highest priority risks.
- Risk exposure is a measure of the magnitude of a risk based on the estimated values for probability and impact (see Section D.2.3.4 in Appendix D for a detailed explanation of how to derive risk exposure).

In addition, we selected one of the following control approaches for each risk:

- *accept* – If a risk occurs, its consequences will be tolerated; the alert originator will take no proactive action to address the risk. When alert originators accept a risk, they document the rationale for doing so.
- *transfer* – A risk is shifted to another party (e.g., through insurance or outsourcing).
- *avoid* – Activities are restructured to eliminate the possibility of a risk occurring.
- *mitigate* – Actions are implemented in an attempt to reduce or contain a risk.

As depicted in Table 8, we selected the control approach "mitigate" for each of the four risks. The far right column in the table documents the rationale for choosing to mitigate each risk.

Table 8: Risk Assessment Summary: Risk, Impact, Probability, Exposure, and Control

ID	Risk Statement	Impact	Probability	Risk Exposure	Control Approach	Control Approach Rationale
1	If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.	High-Max	Rare	Low-Med	Mitigate	This risk could cause severe damage if it occurs, which makes it a good candidate for mitigation. Mitigations for this risk will be relatively cost effective.
3	If an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message, then individual and organizational reputation consequences could result.	Med	Rare-Remote	Min-Low	Mitigate	The impact for this risk is high enough that it warrants mitigation. Organizational and individual liability issues make this risk important to mitigate.
2	If malicious code prevents an operator from entering an alert into the AOS, then health, safety, legal, financial, and productivity consequences could result.	Low-Med	Remote	Min-Low	Mitigate	Alert originators need to show due diligence that they are addressing the basic security challenges inherent in their environment. This risk represents a basic security challenge. This risk has the potential for a higher impact in the future as more people rely on the WEA service to receive alerts.

ID	Risk Statement	Impact	Probability	Risk Exposure	Control Approach	Control Approach Rationale
4	If the internet communication channel for the AOS is unavailable due to a cybersecurity attack on the ISP, then health and safety consequences could result.	Low-Med	Remote	Min-Low	Mitigate	Alert originators need to show due diligence that they are addressing the basic security challenges inherent in their environment. This risk represents a basic security challenge. This risk has the potential for a higher impact in the future as more people rely on the WEA service to receive alerts. Alert originators are in the business of responding to emergencies—they should have contingency plans for their own organizations.

5.3 Select Control Approach and Define Mitigation Requirements

For each risk with a control approach of mitigate, transfer, or avoid, the alert originator develops and documents control plans. In the above analysis, a decision was made to mitigate all four risks identified. As a result, the alert originator will develop a mitigation plan for each risk.

Mitigation plans should be structured around the following three mitigation strategies:

1. Monitor the threat and take action when it is detected (Monitor and Respond).
2. Implement protection measures to reduce vulnerability to the threat and to minimize any consequences that might occur (Protect).
3. Recover from the risk if the consequences or losses are realized (Recover).

Because mitigation plans include actions for preventing, responding to, and recovering from risks, they provide a well-rounded approach for addressing risks to a software-reliant system, like the WEA service. In the remainder of this section, we present a mitigation plan for each of the four risks. Each plan highlights key requirements that alert originators should consider when acquiring or developing an AOS for the WEA service.

5.3.1 Risk 1: Maliciously Sent CAP-Compliant Message

For the first risk, an outside attacker with malicious intent decides to obtain a valid certificate and use it to send an illegitimate CAP-compliant message to WEA constituents, with the goal of inciting physical and emotional harm on people who act on the content of the message. Table 9 presents the mitigation plan for this risk.

Table 9: Mitigation Requirements for Risk 1: Maliciously Sent CAP-Compliant Message

Strategy	Mitigation Requirements
Monitor and Respond	• IPAWS should send an alert receipt acknowledgment to an email address designated in the MOA between the alert originator and the FEMA IPAWS Program Management Office. (This approach uses an alternative communication mechanism from the sending channel.) The alert originator should monitor the IPAWS acknowledgments sent to the designated email address. The alert originator should send a cancellation for any false alerts that are issued. • The alert originator should designate a representative for each distribution region to monitor for false alerts. The representative should have a handset capable of receiving alerts that are issued. If a false alert is issued, the designated representative would receive the alert and should then initiate the process for sending a cancellation of the false alert.
Protect	• The AOS should use strong security controls to protect certificates. – Access to certificates should be monitored. – Encryption controls should be used for certificates during transit and storage. – Access to certificates should be limited based on role. • All alert transactions should have controls (e.g., time stamp) to ensure that they cannot be re-broadcast at a later time. (Note: This requirement requires that the sender time stamps the alert appropriately. The receiver of the alert would need to check the time stamp to determine whether the alert is legitimate or a relay of a previous alert.) • Certificates should expire and be replaced on a periodic basis. • The alert originator should provide user training about security procedures and controls.
Recover	• The alert originator should quickly issue a cancellation before people have a chance to respond to the false alert (i.e., before they have a chance to go to the dangerous location). This might require alert originators to provide additional training and to conduct additional operational exercises. • The alert originator should notify FEMA to determine how to cancel the compromised certificate.

5.3.2 Risk 2: Denial of Service from Malicious Code

Whereas the first risk focuses on an outside attacker with a specific goal to use the WEA service to inflict harm, the second risk is triggered by a more general type of threat. In this case, the actor does not specifically target the WEA service. Here, an operator unintentionally downloads malicious code to the AOS. Table 10 provides the mitigation plan for this risk.

Table 10: Mitigation Requirements for Risk 2: Denial of Service from Malicious Code

Strategy	Mitigation Requirements
Monitor and Respond	• The alert originator should monitor for security patches that can be applied to its AOS. The alert originator should apply security patches to the system as appropriate. • The alert originator should run virus scans on its AOS periodically. The alert originator should respond to viruses found on its systems as appropriate.
Protect	• The alert originator should employ virus protection for its AOS. • The alert originator should control software upgrades to its AOS. • The alert originator should control the use of external devices on its AOS. • The alert originator should employ firewalls to control network traffic to and from the AOS. • The alert originator should isolate alert-originating software from other applications (e.g., web browsers). • The alert originator should use whitelisting practices to ensure that only approved software is installed. • The alert originator should securely configure web browsers. • The alert originator should ensure that warnings and alerts are enabled on web browsers. • Where practical, the alert originator should limit browser usage. • The alert originator should limit users' ability to download software.

Strategy	Mitigation Requirements
	• The alert originator should provide user training about security procedures and controls. • The alert originator should establish a service-level agreement (SLA) with its vendors to ensure appropriate security controls and to establish penalties for noncompliance. (Note: Vendors should employ alternative or backup mechanisms for issuing alerts to ensure that they can meet the terms of their SLAs.) • The alert originator should establish alternative mechanisms for issuing alerts in case its primary communications channels are unavailable.
Recover	• The alert originator should establish procedures for recovering from malicious code attacks. Recovery procedures should address performing analysis activities (e.g., technical analysis, forensic analysis); responding appropriately to the attack (e.g., isolate affected machine, rebuild machine); implementing contingency plans; and notifying appropriate stakeholders. • The alert originator should notify FEMA when a security incident occurs. • The alert originator should update its security policies and procedures based on lessons learned from successful attacks.

5.3.3 Risk 3: Insider Spoofing Colleague's Identity

In Risk 3, an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message under the colleague's name. In this scenario, the insider wants to damage a colleague's reputation among his or her peers and managers. Table 11 outlines mitigation requirements for this risk.

Table 11: Mitigation Requirements for Risk 3: Insider Spoofing Colleague's Identity

Strategy	Mitigation Requirements
Monitor and Respond	• The alert originator should monitor the behavior of its employees for inappropriate actions. • The alert originator should monitor physical and network access to the AOS. • The alert originator should audit remote devices (e.g., laptops) for suspicious activity. • The alert originator should perform periodic inventories of backup devices (e.g., backup computers and other equipment that can be deployed to other sites) to ensure that they are available for use and are not missing (i.e., not taken for inappropriate use).
Protect	• The AOS should use strong authentication and authorization controls (e.g., multifactor authentication). Authentication should be unique to each individual. • The alert originator should promptly address employee behavior problems. • The alert originator should define and enforce an acceptable use policy for its systems and networks. • The alert originator should implement a clearance process that requires periodic renewals. • The alert originator should implement physical security controls that restrict access to devices. – Employ authentication timeouts. – Ensure that alert-originator staff protect their passwords appropriately. – Provide security awareness training to employees. • The AOS should require dual signatures to issue an alert. • The alert originator should provide user training about security procedures and controls. • The alert originator should ensure that the vendor's software adequately protects authentication and authorization information.
Recover	• The alert originator should quickly issue a cancellation before people have a chance to respond to the false alert. This might require alert originators to provide additional training and to conduct additional operational exercises. • The alert originator should notify FEMA when a security incident occurs. • The alert originator should conduct an investigation into the incident and respond appropriately.

5.3.4 Risk 4: Unavailable Communication Channel

In the final risk scenario, the internet communication channel for the AOS is unavailable due to a successful cybersecurity attack on the AOS's ISP, and pre-established, secure backup communication channels (e.g., satellite, direct communication) are inadequate or nonexistent. Table 12 presents the mitigation plan for the fourth risk.

Table 12: Mitigation Requirements for Risk 4: Unavailable Communication Channel

Strategy	Mitigation Requirements
Monitor and Respond	• The alert originator should establish and monitor a "heartbeat" mechanism to ensure that the communication channel is available. (Note: Because the system is not used continuously, alert originators need a mechanism that they can use to check for availability when the system is needed.) • The alert originator should perform periodic dry runs of sending alerts under normal operating conditions. This will help ensure that people know how to send an alert under normal operating conditions. It will also help ensure that people understand what normal operating conditions look like. The alert originator should make sure that it conducts dry runs after the system is updated (e.g., patches applied). • The alert originator should perform periodic dry runs of sending alerts under abnormal conditions, such as power failures. This will help ensure that people know how to send an alert under stress conditions.
Protect	• The alert originator should identify external dependencies (e.g., power sources, communications channels) and establish mitigations for those dependencies. • The alert originator should establish and test off-site capabilities for issuing alerts. • The alert originator should establish and test alternative communications channels for issuing alerts. • The alert originator should establish and test alternative EOCs that could issue alerts, if needed.
Recover	• The alert originator should establish procedures for recovering from an unavailable communication channel. Recovery procedures should address implementing contingency plans and notifying appropriate stakeholders. • The alert originator should notify FEMA when a security incident occurs. • The alert originator should update its security policies and procedures based on lessons learned from problems experienced with communications channels.

5.4 Use the Results of Risk Assessment and Prioritization

The mitigation requirements developed in this section define actions that an alert originator can apply to reduce the risk to the WEA mission. Some of these mitigation requirements can be addressed when the AOS is being acquired and developed, for example, implementing encryption controls for certificates during transit and storage. Here, encryption is a system feature that should be engineered into the AOS as it is being developed or available in an AOS that is being acquired.

However, the majority of the mitigation requirements identified focus on operational issues that should be addressed after an AOS is deployed. Examples include how the AOS configures the system during its operation, the network architecture employed by the AOS, and operational procedures that define how to use the AOS.

Overall, the mitigation requirements documented in Section 5.3 provide guidance that alert originators should consider when they perform the following tasks:

- Define requirements for an AOS that they intend to purchase as a product or service (i.e., from a vendor), acquire (i.e., system development by a third party), or develop (i.e., in-house development).
- Engineer and develop an AOS (if developed in-house).
- Operate and sustain an AOS.

Finally, a key tenet of the CSRM strategy is to ensure that the risk to the WEA mission remains within an acceptable tolerance over time. Implementing the mitigation requirements defined in this section is an important part of making sure that each risk is within an acceptable tolerance. The next section focuses on assigning roles and responsibilities for implementing these requirements.

6 Mitigate Cybersecurity Risks Throughout the Life Cycle

Effective risk-mitigation actions can keep an adversary's initial attack from progressing to disruption of the WEA alerting process. Although IPAWS and CMSPs are responsible for mitigating the risk of attacks on their own systems, they may not be able to detect or mitigate the effects of an attack perpetrated at the start of the alerting pipeline, through the AOS. Therefore, the alert originator is the first line of defense against attacks on the alerting pipeline and has a significant role to play in cybersecurity risk management. While WEA capability product vendors or service providers can assist, alert originators should do their part to ensure that the products and services they acquire are built and operated securely, to secure and monitor their own networks and devices, and to train their staff in effective security practices.

Figure 10 illustrates potential AOS vulnerabilities that can enable successful cyber attacks. In Figure 11, the "X" identifies examples of mitigation actions that the alert originator can take to prevent an attack from successfully disrupting operations.

To plan and implement mitigation actions such as those shown in Figure 11, it is important to understand the following:

- Who in the alert originator's organization is responsible? That is, what are the roles and responsibilities for cybersecurity risk-mitigation actions (Section 6.1)?
- When in the life cycle does the alert originator need to perform risk-mitigation and risk-management tasks (Section 6.2)?
- 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 (Section 6.2.1)?

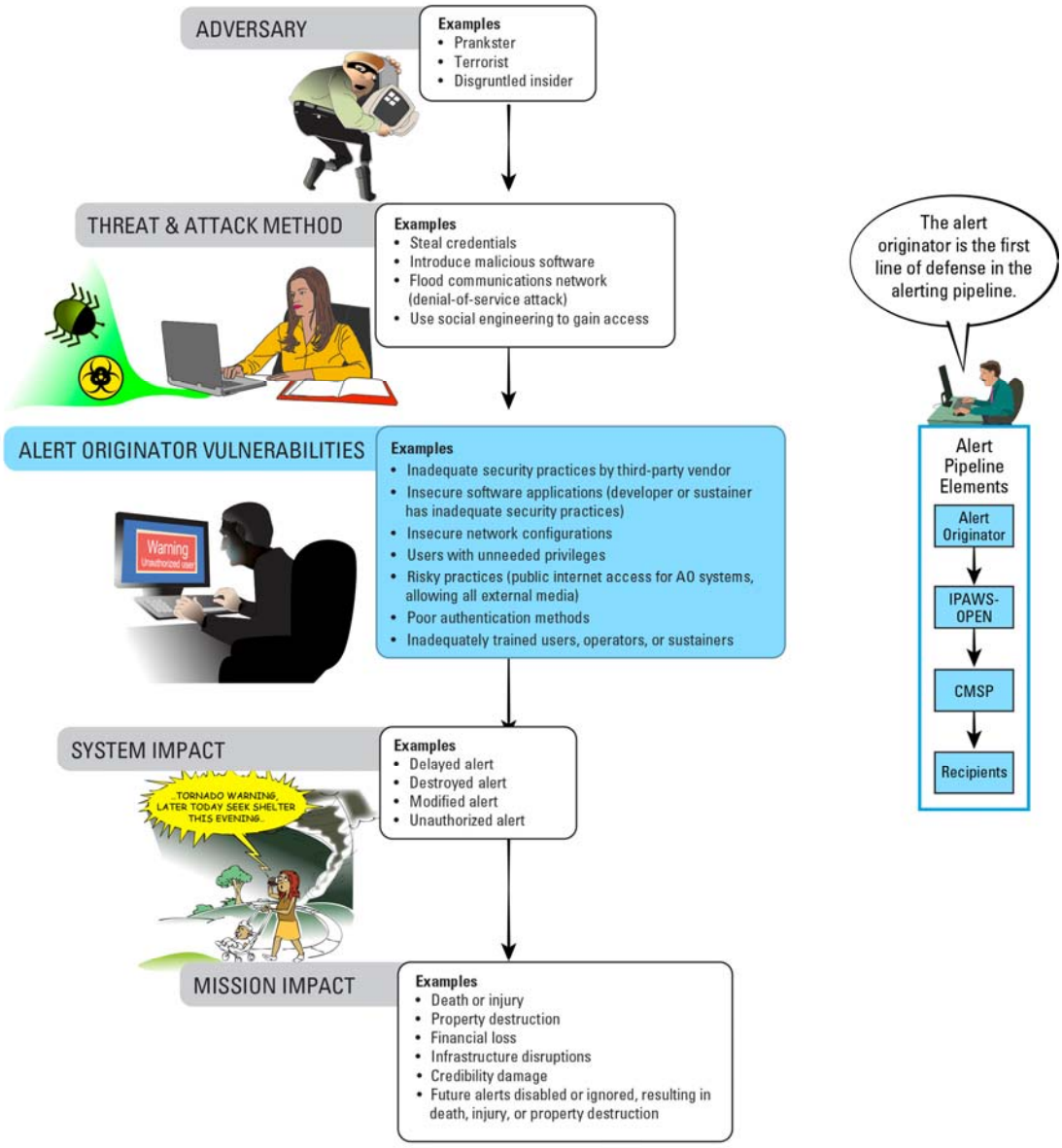


Figure 10: Alert Originator Vulnerabilities

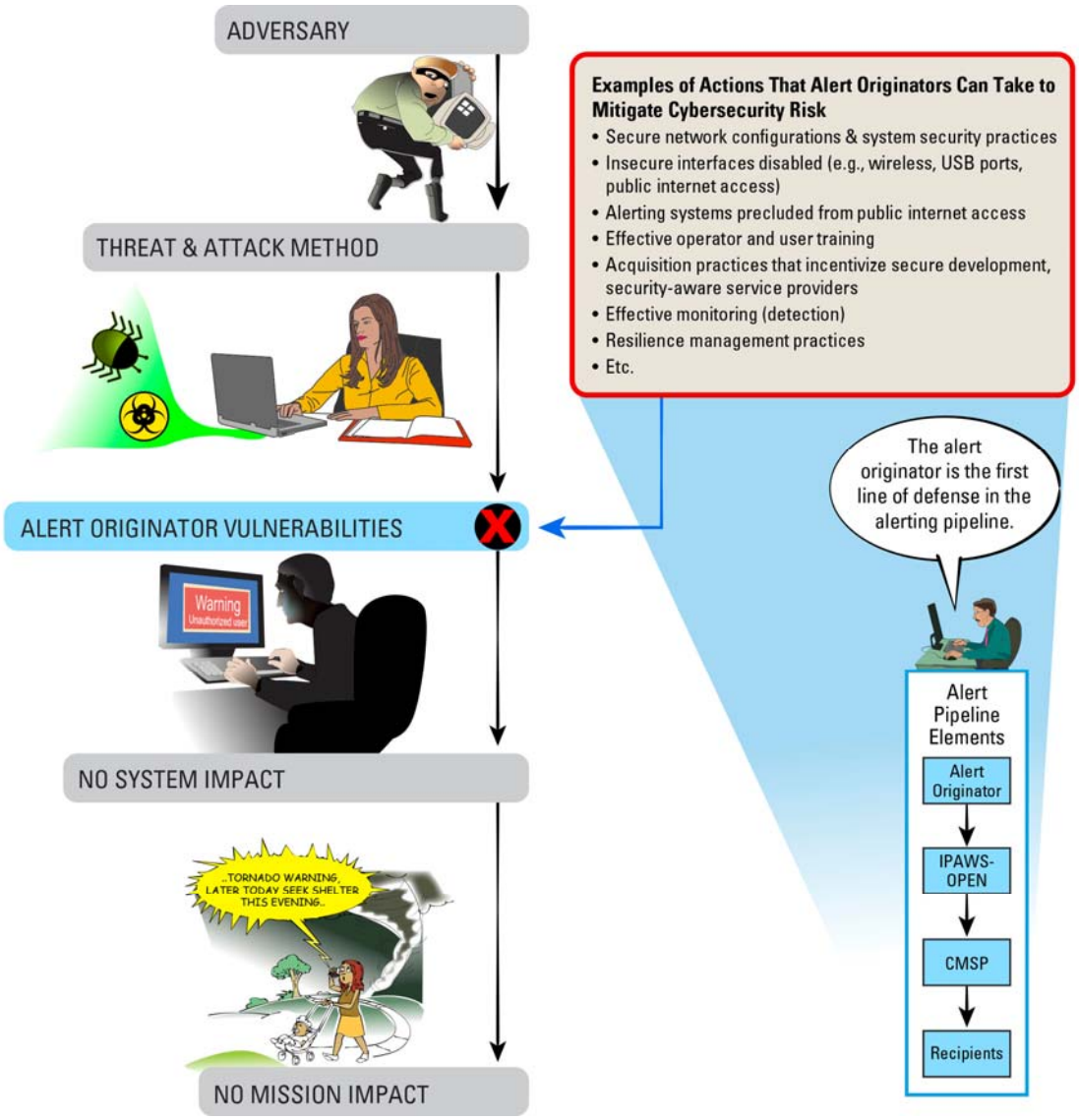


Figure 11: Alert Originator Actions to Reduce Vulnerabilities and Mitigate Cybersecurity Risks

6.1 Define Cybersecurity Risk-Mitigation Roles and Responsibilities for Alert Originators

The alert originator's organization executes a number of roles in carrying out its functions, from executive-level decision making to composing and sending alerts.[15] Different organizations may use different names for these roles, and some roles may be carried out by other parts of the organization, performed by higher level organizations, or delegated to lower level organizations, depending on the organization's size and span of control. For example, some local and county organizations defer to statewide, enterprise-level organizations for such functions as IT product

[15] The organization may have roles in addition to alert origination, but these roles are outside the scope of this report.

selection and service provision. In some organizations, one individual may perform multiple roles or multiple individuals may contribute to a single role.

6.1.1 Identify a Generic Set of Alert Originator Roles and Responsibilities

Table 13 identifies a set of generic alert originator roles that are central to managing cybersecurity risks. The top-level decision maker in the organization (referred to herein as the executive manager) should determine where these roles reside within the organization, or within a larger enterprise, if applicable. Whatever the organizational structure and role assignment, each staff member at each organizational level has some responsibility for cybersecurity risk management. The final allocation of roles and responsibilities should reflect this concept of shared responsibility.

Table 13: Alert Originator Role Names and Descriptions

Alert Originator Role Name	General Responsibilities Relative to IT and Cybersecurity
Executive manager	• Make organizational decisions related to technology adoption, deployment, operations, and sustainment. • Establish cybersecurity policies and direct development of procedures. • Determine where CSRM roles and responsibilities reside for their alert-originating organization and for ensuring that a CSRM plan is developed, trained, implemented, and sustained. • Depending on organization or role in serving a broader enterprise, some alert-originating organizations may include within their executive manager ranks explicit roles for chief information security officer, chief security officer, or chief risk officer. If they exist, these roles would be key participants in cybersecurity risk management.
Personnel manager	• Implement staffing policies and procedures. • Track compliance with training requirements and cybersecurity policies and procedures. • Report and assist in handling deviations.
Technology (product or service) acquisition and contracting staff	• Prepare for product and service acquisitions, articulating operational and technical capability requirements, integration and interoperability requirements, sustainment requirements, and quality attribute requirements (product and service security requirements are important risk mitigators). • Establish performance criteria for vendor or developer, including those for security. • Develop acquisition and contracting documentation. • Support acquisition decision making. • Monitor vendor or developer against established performance criteria. • Verify, to the extent possible, that products and services are developed and supplied in accordance with cybersecurity policies and requirements, whether these are developed, supplied, and sustained in house or by an external party.[16]
Operations manager	• Manage alert origination operations. • Maintain situational awareness of personnel concerns, procedural irregularities, and technology issues; training needs; and risks. • Provide for redundant and resilient operations. • Assume ultimate (management) responsibility for detecting, responding to, and recovering from issues and failures, including those related to cybersecurity incidents. • Ensure that minor and major sustainment actions are planned and executed so as not to interfere with operations.

[16] We say “to the extent possible” because in today’s complex, dynamic environment, the system that complies with requirements and is secure one day may be attacked by new threats or made vulnerable by a configuration change the next. For this reason, we view compliance with static cybersecurity policies and requirements as necessary but not sufficient. Periodic and event-driven application of the CSRM process is one way to address emerging risks.

Alert Originator Role Name	General Responsibilities Relative to IT and Cybersecurity
Operator (AOS user)	• Generate alerts. • Complete required operator training, including cybersecurity training. • Comply with cybersecurity procedures in using AOSs.
Development staff (if in house)	• Translate top-level cybersecurity requirements into technical specifications. • Follow a secure development life-cycle approach. • Complete required development training, including secure development and cybersecurity training. • Comply with cybersecurity procedures in using development, test, and production systems.
IT staff	• Manage in-house IT capabilities and interface with remotely hosted capabilities. • Ensure that users have the IT capabilities needed for operations. This role includes network and system administration functions that provide these capabilities. • Complete required training (e.g., FEMA IPAWS and WEA training, internally required IT training, security training). • Develop cybersecurity procedures. • Comply with cybersecurity procedures in managing and sustaining AOSs. • Assume technical responsibility for procedures and tools used to detect, respond to, and recover from cyber attacks and other IT incidents (define and select these procedures and tools in consultation with information security staff). • Oversee response and recovery procedures. • Perform failure analysis and establish measures to prevent future failures.
Information security staff	• Define proactive security practices, procedures, and training for systems and networks for the alert originator's organization to use. • Recommend information security tools. • Monitor IT systems and practices and employ defined procedures and tools to detect, respond to, and recover from reported issues and cyber attacks. • Perform security audits, vulnerability assessments, and risk assessments. This role includes network and system administration functions focused on proactive security actions (e.g., configuration-related actions such as establishing or modifying user accounts and configuring device and software settings in alignment with security requirements).
Incident response staff	• Continuously monitor IT systems and networks. • Report and respond to cyber events and incidents when they occur. • Implement response and recovery procedures. This role includes network and system administration functions required for incident response and recovery (e.g., revoking account privileges and disconnecting devices from networks).

6.1.2 Assign Mitigation Requirements to Generic Roles: An Example

Section 5 analyzed four plausible WEA cybersecurity risks (maliciously sent CAP-compliant message, denial of service from malicious code, insider spoofing colleague's identity, and unavailable communication channel) and identified risk-mitigation requirements for each one. In this section, we use these risk-mitigation requirements to illustrate the responsibilities of each alert originator role described in Table 13. First, we collect all the mitigation requirements for the four example risks and group them into areas of responsibility that will allow us to better manage implementation. Next, we identify additional mitigation requirements that provide more comprehensive coverage. Finally, we assign the requirements to one or more roles. Table 14 illustrates the results.

Table 14: Mitigation Requirements and Alert Originator Roles Involved: An Example

Alert Originator Areas of Responsibility and Cybersecurity Risk-Mitigation Requirements *Main Source: Table 9–Table 12* *These should NOT be considered exhaustive.*	**Alert Originator Roles Involved**								
	Executive Management	**Personnel Management**	**Technology Acquisition**	**Operations Management**	**Operator**	**Development Staff**	**IT Staff**	**Information Security Staff**	**Incident Response Staff**
Alert Originator Interface with IPAWS-OPEN • Verify that both the alert originator and WEA vendor or service provider comply with the MOA between the alert originator and the FEMA IPAWS Program Management Office, paying close attention to the Rules of Behavior related to cybersecurity [FEMA 2012a].[17] • False alert detection and response: Establish procedures for alert receipt acknowledgment through alternative channel. • Certificate management: Establish and secure initial certificate; request certificate expiration and renewal dates, notification of expiration, and document procedure for canceling compromised certificate.	X			X	X		X	X	
Alert Originator Cybersecurity Policies, Procedures, and Controls • Define acceptable use policy. • Implement employee clearance process with periodic renewals. • Establish equipment and software configuration controls. • Protect system access information.	X	X		X			X	X	
Alert Originator System Development Requirements for Security, Availability, and Resilience • Document operational mission threads (Section 3) to identify cyber threats and vulnerabilities (Section 4), assess and prioritize resultant risks, and identify mitigation requirements (Section 5). • Establish SLAs and contractual requirements for security, availability, and resilience with WEA developers and service providers, and establish penalties for failure to comply (includes secure development practices, secure configuration, personnel security, etc.). • Establish and test against product security requirements (i.e., test against common vulnerabilities [OWASP 2013, SANS 2011]; perform penetration testing and fuzz testing). • Define features to be designed in (e.g., ability to require two signatures before alert is sent, role-based access controls and privileges, multifactor authentication, time stamping of alerts to prevent unauthorized rebroadcast). • Monitor and enforce contracted service agreements.	X		X	X		X	X	X	X

[17] In the cited resource, see Step 2, MOA application. After completing the MOA application, the alert originator will receive a document specifying the Rules of Behavior, a number of which deal with cybersecurity requirements directed to the alert originator and vendor.

Alert Originator Areas of Responsibility and Cybersecurity Risk-Mitigation Requirements *Main Source: Table 9–Table 12* *These should NOT be considered exhaustive.*	Alert Originator Roles Involved								
	Executive Management	Personnel Management	Technology Acquisition	Operations Management	Operator	Development Staff	IT Staff	Information Security Staff	Incident Response Staff
System Configuration • Ensure that designed-in security features are enabled. • Implement strong authentication and authorization controls (e.g., role-based access control and privileges, multifactor authentication, dual signatures for alerts). • Implement security controls to restrict device access and alert issuance (timeouts, password protection, dual signatures for alert issuance). • Isolate alert origination software from other applications. • Employ firewalls to control access to and from AOS. • Control use of external devices. • Securely configure web browsers; enable warnings and alerts; limit browser usage. • Identify external dependencies and develop or recommend resilience mechanisms. • Monitor access to certificates. • Implement encryption controls for certificates (transit and storage). • Limit certificate access based on role. • Implement software protection of authorization and authentication information.			X	X		X	X	X	X
Resilient Alert Originator Operations • Identify and establish redundant alerting channels: – off-site backup capability for issuing alerts – alternative communications channels for issuing alerts – alternative EOCs for issuing alerts • Each time an alert is issued, once the emergency is resolved, incorporate a lessons-learned activity that includes an evaluation of alerting process security and resilience.	X		X	X	X	X	X	X	X
Operator Training and Operational Exercises • Establish and deliver general cybersecurity awareness training and confirm training completion for all alert originator staff. • Instruct alert originator staff on security procedures and controls (e.g., protecting passwords, acceptable use). • Instruct staff on how to detect and quickly respond to and cancel false alerts. • Conduct frequent (per shift) tests of alerting process (reflecting normal and abnormal conditions).		X		X	X		X	X	X

Alert Originator Areas of Responsibility and Cybersecurity Risk-Mitigation Requirements *Main Source: Table 9–Table 12* *These should NOT be considered exhaustive.*	Alert Originator Roles Involved								
	Executive Management	Personnel Management	Technology Acquisition	Operations Management	Operator	Development Staff	IT Staff	Information Security Staff	Incident Response Staff
Software Modifications • Monitor for and apply security patches (using defined procedures). • Control software upgrades (use defined procedures, test before rollout, provide for rollback). • Limit user software downloads, and use whitelisting to ensure that only approved software is installed.			X	X		X	X	X	X
System Monitoring • Establish and monitor a heartbeat mechanism. • Employ virus protection: Execute virus scans and respond accordingly. • Monitor employee behavior and system usage. • Monitor system and network access. • Audit remote devices and backup devices.			X	X		X	X	X	X
Incident Response and Recovery • Establish and apply policies and procedures to respond to and recover from security incidents and communications channel failure. • Identify root causes of problems and mitigation options. • Define instructions to notify FEMA. • Provide updates to security policies and practices based on lessons learned.	X			X			X	X	X
Operations Security • Comply with security policies. • Conduct frequent (per shift) tests of alerting process (reflecting normal and abnormal conditions). • Monitor for false alerts and quickly respond to and cancel them. • Immediately report suspected security incidents. • Promptly address employee behavior and system misuse issues.	X	X	X	X	X	X	X	X	X

Once general responsibilities for cybersecurity risk-mitigation requirements have been assigned to roles, the alert originator should identify and plan the cybersecurity tasks for each life-cycle phase, integrating them with the general tasks of that phase.

6.2 Identify Alert Originator Tasks for Each Life-Cycle Phase

The WEA capability encompasses hardware, software, services, procedures, and personnel that together enable an organization to send timely, accurate WEA messages. Accordingly, WEA life-cycle activities involve much more than selecting a vendor or service provider based on functionality alone. The alert originator is responsible for specifying requirements for behavioral or quali-

ty attributes—such as security, reliability, availability, maintainability, and resilience—that determine selection criteria for products and services. The alert originator should also verify that these requirements are met both on initial delivery of the WEA capability and as patches, updates, and enhancements are applied. Table 15 provides examples of tasks for which the alert originator is responsible in each WEA life-cycle phase (adoption, operations, and sustainment). The first column indicates the life-cycle phase and lists the applicable cybersecurity risk-mitigation action groupings from Table 14. The second column identifies alert originator tasks that should incorporate these cybersecurity risk-mitigation actions.

Table 15: WEA Life-Cycle Phase and Alert Originator Tasks

WEA Life-Cycle Phase and Cybersecurity Risk-Mitigation Action Groupings (see Table 14)	**Alert Originator Tasks**
Adoption • Alert originator interface with IPAWS-OPEN • Alert originator cybersecurity policies and procedures • AOS development requirements for security, availability, and resilience • AOS development and configuration requirements and operational procedures for access control and certificate protection • Resilient AOS operations • Operator training and operational exercises • System configuration	All tasks necessary to acquire or develop the WEA capability and transition it to operations and sustainment, for example, • Eliciting, specifying, and validating requirements • Selecting an approach to obtain the capability (e.g., buying a product, contracting for a service, contracting for custom development, or developing the capability in house) and developing the needed acquisition and SLA documentation (specifying requirements, evaluation criteria, etc.) • Executing the selected approach, including procuring a product or service, managing an internal development, or monitoring a custom development (note that the developer or service provider must have successfully tested its software in the IPAWS-OPEN environment [FEMA 2012a]) • Executing an MOA between the alert originator and the FEMA IPAWS Program Management Office [FEMA 2012a] • Verifying that the capability meets requirements • Preparing for sustainment of the capability (whether performed in-house, externally, or using some combination of internal and external capability) • Preparing the organization for operational use of the capability • Ensuring that equipment is configured securely and is physically protected, per the MOA with FEMA • If mobile devices are used, ensuring that they are approved and configured to lock as required by the MOA with FEMA • If wireless devices are used, ensuring that sensitive information (e.g., passwords and certificates) is encrypted (when processed, stored, or in motion) per the MOA with FEMA • Launching the capability and ensuring it functions as required • Transitioning to normal operations and sustainment
Operations • Alert originator cybersecurity policies and procedures • Resilient AOS operations • Operator training and operational exercises • Operations security	All tasks necessary to generate and transmit alerts to IPAWS and to maintain readiness to generate and transmit alerts, for example, • Using discrete user accounts with passwords as required by the MOA with FEMA • Logging in and accessing alerting functionality • Constructing appropriate WEA message • Signing the WEA message, consistent with security requirements • Transmitting the WEA message • Confirming the intended WEA message was received by IPAWS and by intended recipients • Conducting a lessons-learned activity, at the conclusion of an emergency in which a WEA message was issued, to determine effectiveness and areas for improvement, including an assessment of security practices

WEA Life-Cycle Phase and Cybersecurity Risk-Mitigation Action Groupings (see Table 14)	Alert Originator Tasks
Sustainment • Alert originator cybersecurity policies and procedures • AOS development requirements for security, availability, and resilience • AOS development and configuration requirements and operational procedures for access control and certificate protection • Resilient AOS operations • Operator training and operational exercises • System configuration • Software modifications • System monitoring • Incident response and recovery	All tasks necessary to sustain the operational WEA capability, for example, ensuring that the responsible sustainment group performs the following tasks: • Testing the system periodically • Employing a heartbeat monitor • Performing various system administration functions (adding and deleting users, changing user permissions, configuring operating system parameters, configuring network equipment) • Installing software patches and operating system upgrades • Installing WEA capability upgrades • Modifying equipment configurations • Using required security software as indicated by risk assessments and as required by the MOA with FEMA • Installing new equipment Note: For sustainment, the alert originator should document the organization(s) responsible for different types of sustainment actions and the alert originator roles that either perform the actions or oversee them, if performed by an external party. For example, actions such as adding users may be done on site by system administrators or remotely by a WEA service provider. WEA capability upgrades may be performed in house (if the capability was developed in house), by a vendor, or by a service provider. For major upgrades, the alert originator may need to execute tasks from the adoption activity. In all cases, the alert originator needs to ensure that sustainment actions are performed with security in mind and without disrupting operations.

While performing the tasks in each WEA life-cycle phase, the alert originator makes decisions that can affect operational cybersecurity risk and the degree of control that the alert originator has over risk mitigation. Examples of these decisions include the following:

Adoption

- Choice of source for WEA capability (e.g., vendor or in-house development group)
- WEA capability hosting (e.g., on site, as a delivered application; off site, as a service; or remotely, at a facility operated by another organizational unit)
- Level of integration of WEA capability with other capabilities (e.g., stand-alone; shared user interface or other functionality with other alerting capabilities; or shared interface or other functionality with other emergency management capabilities)

Operations

- Allowable alert origination devices (e.g., desktop systems, laptops, mobile devices)
- User IDs and privileges (limited privileges and access; broad privileges and access)
- Alert message signing (single or dual signature required for alerts)

Sustainment

- Applying software changes, from patches, to system software upgrades, to WEA capability enhancements (e.g., changes applied locally, as a service, or remotely), and robustness of testing before deployment

- Maintaining equipment configuration (policies related to special circumstances for deviating from secure configurations)

Appendix E discusses these decisions and the cybersecurity risks associated with them. The next section provides an example of alert originator tasks that incorporate cybersecurity risk mitigation during the WEA adoption phase of the life cycle.

6.2.1 Example of WEA Adoption Phase Tasks for Cybersecurity Risk Management

The alert originator is responsible for ensuring that the selected WEA capability meets both functionality and quality attribute requirements, including requirements for security. As such, the alert originator has distinct tasks that drive and assess tasks performed by the WEA capability vendor, developer, or service provider. In this section, we refer to all three of these roles (vendor, developer, and service provider) as the supplier. This section uses an abbreviated sequence of adoption activities to show the task interdependencies and to emphasize the role that the alert originator has in ensuring the supplier provides a capability that is resistant to cyber attack. The alert originator cannot assume that the supplier will incorporate secure development practices or product security requirements if the alert originator does not specify, monitor, and verify their implementation.

WEA adoption involves a series of steps that an organization should work through to adjust and change its operational capability. The same format is used for the adoption thread that was used in Section 3 to illustrate an operational mission thread. Table 16 provides the mission thread description and Table 17 the adoption steps of the mission thread.

Table 16: Description for Generic Abbreviated WEA Adoption Mission Thread

Name	Generic Thread for WEA Adoption by an Alert Originator
Vignette (Summary Description)	The alert originator is responsible for 24/7 alerting that encompasses its jurisdiction. One of the alert originator's objectives is to create and disseminate imminent threat alerts to recipients in affected areas. The alerts must be accurate, timely, and usable, informing recipients of recommended actions to take. FEMA has set up IPAWS to support aggregation and dissemination of such alerts. One capability is WEA, which uses IPAWS to disseminate alerts to CMSPs in the affected area. The CMSPs then broadcast the alerts to mobile devices. The alert originator has processes in place for specifying, evaluating, and acquiring technology, which it can use to select a supplier for the WEA capability.
Nodes and Actors	**Directly Engaged in Adoption (decision to implement through launch and transition)** • Alert originator staff (see "Assumptions" under "Organizational" below) • Prospective suppliers • FEMA approval entities **Engaged in Launch of the Capability (possibly in testing, and when it is actually used)** • CMSPs • Mobile device users

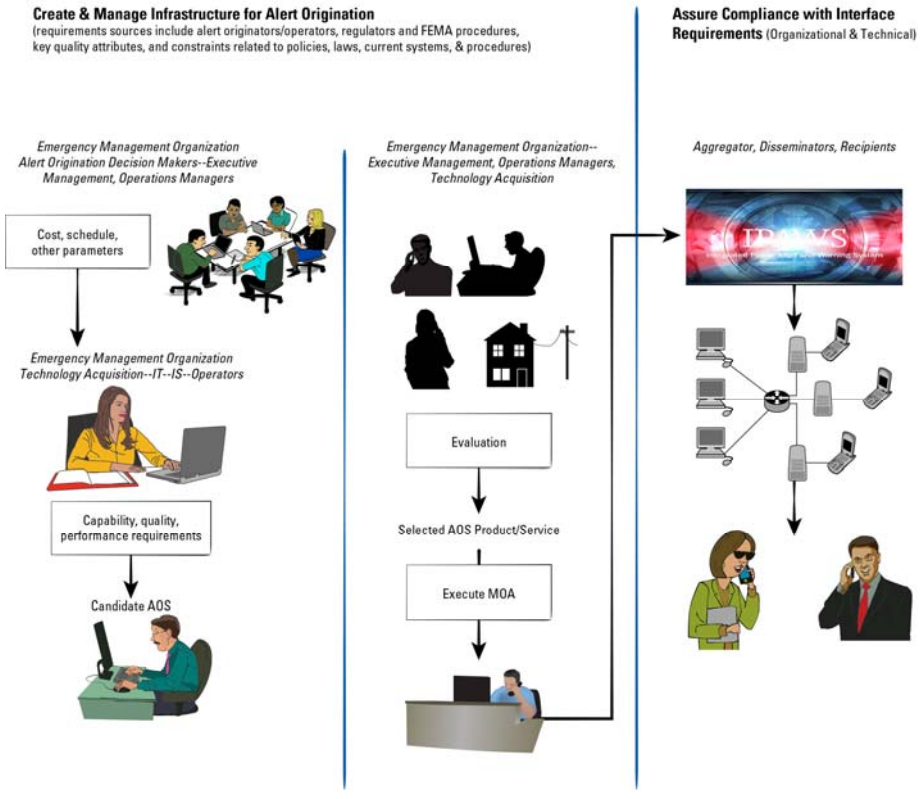
Assumptions	**Situational** • The alert originator has decided to acquire a WEA capability. • The alert originator has justification for using IPAWS and meets alert originator criteria. **Organizational (staffing and procedures)** • The alert originator has acquired products and services for alerting in the past. • Alert originator roles include executive management, personnel management, technology acquisition, operations management, operators, IT staff, information security staff, and incident response staff. • A higher level organization has guidance, constraints, and requirements that this alert originator must follow, but the higher level organization is not acquiring or specifying the supplier for WEA. • The alert originator has cybersecurity policies, procedures, and controls in place. **Technological** • The alert originator has other alerting systems in place. • IPAWS is fully operational and available to accept, process, and transmit alert messages; it consists of the IPAWS-OPEN Gateway, WEA Alert Aggregator, and Federal Alert Gateway. • The CMSP Gateway and Infrastructure are fully operational and available to accept and broadcast WEA messages. • Mobile devices are WEA-capable devices and ready to receive alerts with adequate signal.
Environmental Context Diagram	

Table 17 lists and describes five generic steps for WEA adoption and summarizes the tasks performed in the course of these steps. Each step involves interaction between the alert originator and the supplier to ensure that the capability meets requirements. The table emphasizes cybersecurity-related tasks, so it does not include all adoption tasks. The cybersecurity-related tasks in Table 17 were derived from the following risk-mitigation groupings (see the Adoption row in Table 15):

- AOS interface with IPAWS
- alert originator cybersecurity policies and procedures
- AOS system development requirements for security, availability, and resilience
- AOS system development and configuration requirements and operational procedures for access control and certificate protection
- resilient AOS operations
- operator training and operational exercises
- system configuration

Table 17: Generic WEA Adoption Thread Illustrating Cybersecurity Tasks (Nominal Path)

Adoption Example Step	Generic Adoption Step Description
1	**Identify requirements and prepare for acquisition** • Develop operational mission threads and use them to identify threats and vulnerabilities, assess risks, and document mitigation actions, as input to identifying security requirements. • Identify both capability and quality attribute (including security, resilience, and performance) requirements. Also, develop requirements related to training, support for capability launch, and sustainment. Security requirements include those identified through the four-part CSRM strategy as well as those specified in applicable regulations and standards and the MOA with FEMA. • Prepare applicable acquisition documentation specifying requirements and expectations for supplier, and provide to candidate suppliers. • Accept responses from candidate suppliers.
2	**Select supplier and prepare for risk-based monitoring of development (if applicable) and acceptance review** *Notes: Monitoring is applicable if the supplier is creating a custom capability or modifying an existing product or service to meet specific alert origination requirements, or if the capability is developed by internal alert originator development staff. "Risk-based" means that the monitoring activity focuses on areas identified as risks to successful delivery of the capability.* • Determine whether supplier product or service and practices meet capability and quality attribute requirements. • Select supplier and execute agreement for development monitoring (if applicable) and acceptance review.
3	**Manage risks and prepare for capability launch** • Monitor development (or delivered product or service) against requirements specified in Step 1. • Conduct operator training and operational exercises, to include cybersecurity. • Configure system(s) for new capability. • Prepare for internal sustainment functions. • Develop launch checklist. • Provide feedback to supplier on monitoring activities, and engage with supplier to plan for launch and sustainment.
4	**Conduct acceptance review** • Apply appropriate methods to verify requirements (e.g., inspection, analysis, demonstration, or test) [INCOSE 2010]. • Provide feedback to supplier, and monitor supplier response in resolving issues.
5	**Launch WEA capability and transition to operations and sustainment** • Execute launch checklist. • Operate capability and provide feedback. • Monitor use of capability and provide feedback. • Execute internal sustainment functions and provide feedback. • Monitor supplier-provided operations and sustainment functions and provide feedback.

Figure 12 illustrates the alert originator roles (columns) that might engage in adoption tasks for each step (rows). Again, organizations may differ in how they name and assign these roles. The figure does not show all essential tasks involved in adopting WEA. Its purpose is to emphasize the interaction needed between the alert originator and the supplier to ensure that requirements, including those to mitigate cybersecurity risks, are met. Depending on the size of the alert-originating organization, one individual may function in multiple roles or, conversely, multiple individuals may perform one role.

To assist alert originators in planning for their cybersecurity role in adoption, Appendix F describes in significant detail the tasks in each step of the adoption thread. The descriptions highlight the alert originator's interactions with candidate and chosen suppliers, which can facilitate cybersecurity risk mitigation and result in a more resilient alerting capability.

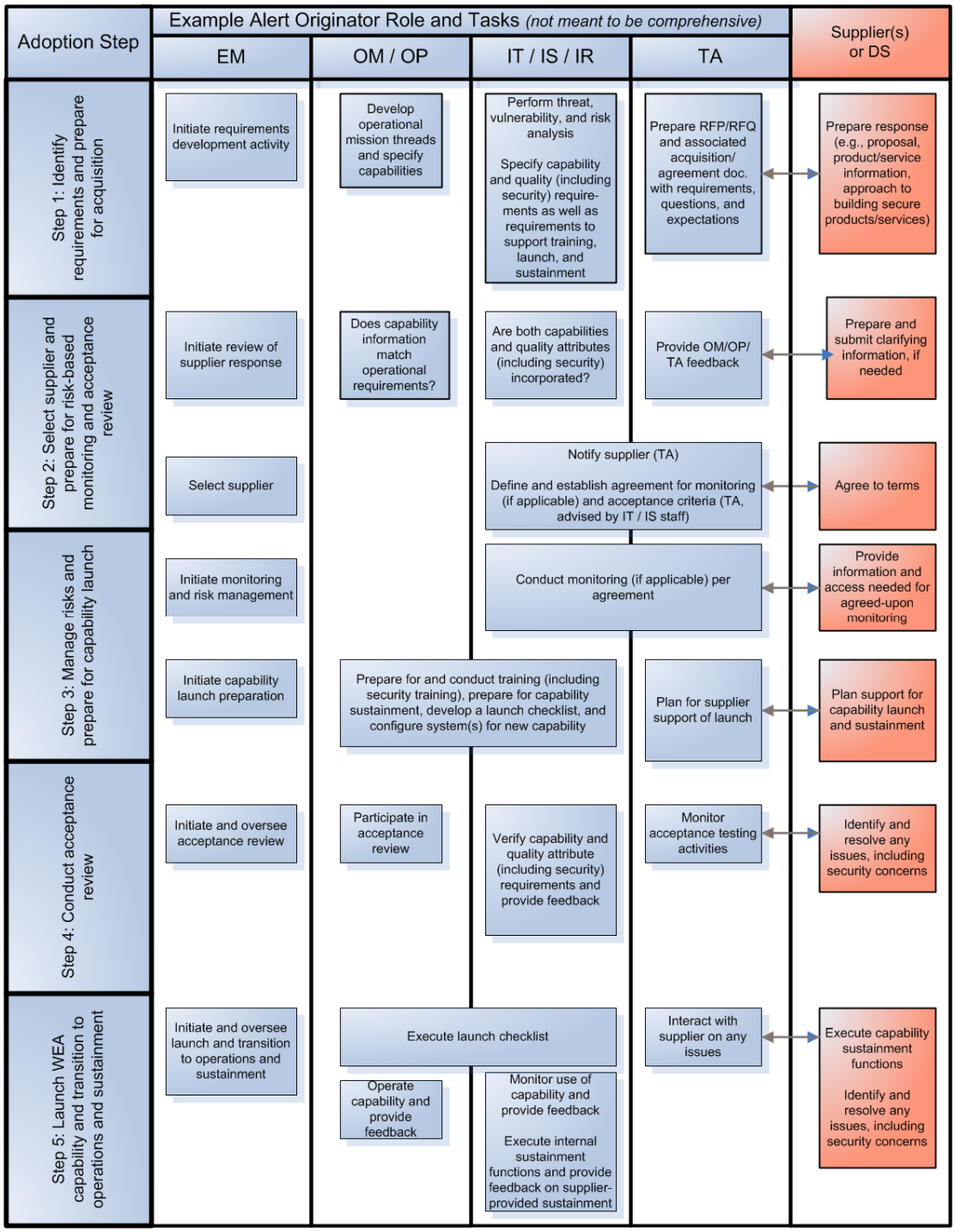


Figure 12: Adoption Steps, Alert Originator Roles, and Alert Originator–Supplier Interaction

DS: development staff; EM: executive management; IR: incident response staff; IS: information security staff; IT: IT Staff; OM: operations management; OP: operator; TA: technology acquisition staff.

7 Plan and Sustain WEA Cybersecurity Risk Management

Sections 3 through 6 described the four stages of the CSRM strategy and provided examples illustrating how alert originators can perform the activities of each stage. This section provides guidance that alert originators can use to plan these activities in an organizational context and establish a governance structure, processes, and operational mechanisms to execute, improve, and sustain the plan.

7.1 An Organizational Framework for Risk Management

Effective risk management for any technology requires planning, training, and sustainment activities. The addition of a wireless emergency alerting capability is no exception. All of these activities are initiated and bounded through organizational governance. Three organizational layers work together to manage risk: governance, processes, and operations. The National Institute of Standards and Technology (NIST) Risk Management Framework, illustrated in Figure 13, depicts this risk management structure. 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. For more general information about applying the NIST Risk Management Framework across the organization, refer to NIST 800-37, Revision 1 [NIST 2010].

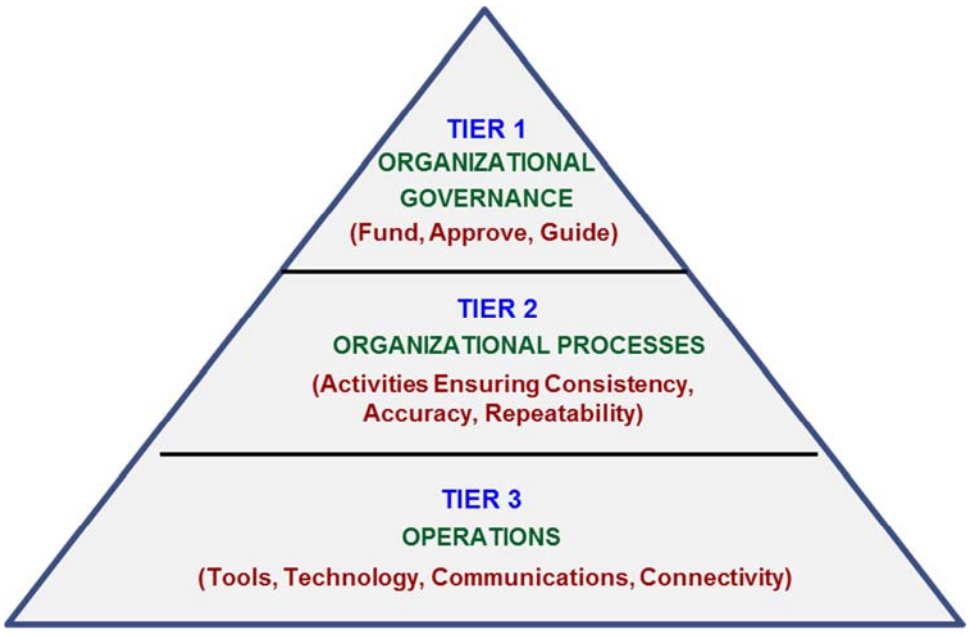


Figure 13: Risk Management Framework [Derived from NIST 2011, p. 9]

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, 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., mission threads, STRIDE analysis, and cybersecurity risk analysis). The remainder of this section provides guidance specific to governance and organizational processes for planning and sustaining a WEA CSRM strategy, which alert originators can tailor to meet their organizations' needs.

7.2 Considerations for WEA CSRM Planning

The decision by an alert-originating organization to add the ability to transmit alerts through the WEA service initiates requirements for resources, training, state and federal approvals, and integration choices for existing capabilities. Decisions in each of these areas can have cybersecurity implications. Once the capability is operational, sustainment activities such as equipment and system upgrades, staff changes, and problem response can also impact cybersecurity.

Effective governance for risk management requires establishing and maintaining a framework and supporting management structure and processes to provide assurance that an organization's security strategy [Bowen 2006]

- is aligned with and supports business objectives
- adheres to policies, standards, and internal controls
- provides assignment of authority and responsibility

An organization may already have risk management processes in place, but these processes may not be sufficient to cover the expansion to the WEA capability. To institute appropriate governance for WEA cybersecurity risk management, the alert originator should develop a plan that enhances the existing organizational processes to address WEA.

Even for small organizations, it helps to assemble a written plan to make sure that critical risks are not missed. For a large organization with many participants, a plan shared by all the participants provides an excellent communication vehicle and makes security needs visible to all. The CSRM planning activity for WEA should consider the following:

- options for implementing the desired WEA capability (if options are still under evaluation)
- relevant policies, standards, and controls for WEA
- cyber threat and vulnerability analysis for each implementation option (if options are still under evaluation) or for the chosen option (once the evaluation and selection process is complete) to identify potential security risks and mitigation needs
- review of current organizational risk management processes to identify new needs and potential limitations of current processes
- steps to take to address critical security gaps and mitigate risks

The formality and specificity of each activity will depend on the needs of each alert-originating organization. It is important for the organization to staff each activity appropriately with assigned responsibilities and target dates to drive toward activity completion. Appendix G provides a general CSRM planning guide.

By following the CSRM strategy presented in this report, management will be prepared to address critical security questions [Allen 2008]:

- What needs to be protected? Why does it need to be protected? What happens if it is not protected?
- What potential adverse consequences need to be prevented? At what cost? How much disruption can we stand before we take action?
- How do we determine and effectively manage the residual risk?

In addition, management should review local, state, and federal compliance standards that the organization should address to ensure that the planned choices for security also meet other mandated standards.

Finally, the organization should incorporate into the plan activities to ensure that it establishes and maintains effective competencies. For WEA, key aspects of assuring competency include

- training on the WEA capability, selected tools and services, and basic information systems security
- acquiring and sustaining expertise in alert origination and emergency management
- identifying security experts who can assist with cybersecurity analysis and provide awareness of the kinds of risks that result from organizational choices

An organization can gain a general understanding of security needs relevant to WEA by reviewing information provided by technology leaders and organizations in other public service industries. The following sources present key cybersecurity issues and ways that other industries have addressed them:

- *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience* [Caralli 2011]
- Guide to developing a cybersecurity and risk-mitigation plan from the power utilities [NRECA 2011]
- *Software Assurance: An Overview of Current Industry Best Practices*, by SAFECode, a consortium of major technology vendors [SAFECode 2008]

Planning should also accommodate the need for ongoing cybersecurity support. Security issues are not static, and the organization's environment will evolve. Periodic reviews are essential to ensure that the organization continues to address cybersecurity risks appropriately.

7.3 Building the CSRM Plan

Cybersecurity planning starts by identifying current alert originator responsibilities and making decisions about the WEA capabilities to be integrated into the operational environment. While many levels of the organization will provide input to the CSRM plan, for effective governance the executive manager should own and monitor the plan (see Table 13 and Table 14 for descriptions of expected organizational roles). Here are some initial questions to assist in assembling information about the current environment and preparing for WEA that are important to cybersecurity risk management:

- What WEA capability do we plan to implement (types of alerts to issue, geographic regions to cover)?
- Can we expand existing capabilities to add WEA, or do we need to obtain new capabilities?

- Do we have good security practices in place for the current operational environment? Is there any history of security problems that can inform our planning?
- Will we use existing resources (technology and people), or do we need to add resources?
- Who will complete the FEMA application for access to IPAWS-OPEN? What internal and external approvals are required? Are new standards and practices needed for approval?
- What training do we need to complete as part of the application process? Will any of this training help identify security issues?

Responses to these questions will begin to frame the target operational context and the critical functionality that organizations should evaluate for operational security. Each organization will have a different mix of acquired technology and services, in-house development components, and existing operational capability into which the WEA capability will be woven. Gathering these details will help organizations adjust and enhance the activities of the CSRM planning guidance (see Appendix G) that they need to consider and the roles that they need to involve in the CSRM plan (see Table 13 and Table 14).

The executive manager should establish the security expectations for the organization as they will relate to the WEA capability. To begin with, to receive approval to use the WEA capability, the alerting organization is required to establish an MOA with FEMA that allows IPAWS-OPEN to accept WEA messages sent from the organization's AOS. This MOA specifies rules of behavior that consist of security guidelines for operating the WEA AOS. The organization is required to agree to comply with these guidelines. The organization may also need approvals at the local, state, and federal levels, and these approvals may require additional security provisions.

The sample activity schedule in Appendix G points to the stages of the CSRM strategy that are relevant to each specific activity. Addressing the four stages of the CSRM strategy will enable an organization to have confidence in the plan to deal with cybersecurity risks:

Prepare for Cybersecurity Analysis

- Review the security requirements to assemble the set appropriate to the organization.
- Tailor the sample operational mission thread in Section 3 to match the planned operational process for providing WEA capability.
- This work is addressed in Activities 1–6 of the sample plan in Appendix G.

Conduct Cybersecurity Analysis

- Build or tailor the STRIDE analysis table to identify threats relevant to the tailored operational mission thread (Steps 4–9 can be tailored from the example in Section 4).
- Review the risks developed in the example analysis and determine similarities and differences.
- For organizations that have vendors, consider inviting them to discuss security requirements, threats, and risks and document how the organization will need to implement their system to appropriately reduce security risk.
- This work is addressed in Activities 7–8 of the sample plan in Appendix G.

Assess and Prioritize Cybersecurity Risks

- Identify which risks to mitigate and which to accept, transfer, or avoid because of resource and technology limitations, and determine mitigation requirements, as shown in Section 5.
- Build a timeline for activities needed to address the organizational cybersecurity requirements and monitor progress.
- This work is addressed in Activity 9 of the sample plan in Appendix G.

Mitigate Cybersecurity Risks Throughout the Life Cycle

- Assign roles and responsibilities for mitigating risks in adoption and operations, and for adapting risk-mitigation actions to address changes in organizational and security needs, as shown in Section 6.
- This work is addressed in Activities 10–11 of the sample plan in Appendix G.

In building the CSRM plan, the alert originator will construct a timeline for performing all the activities and will review and adjust it as needed to accommodate other organizational priorities. This work is addressed in Activities 11–12 of the sample plan in Appendix G.

7.4 Sustaining the CSRM Plan

It is essential to plan for sustainment activities to monitor execution of the CSRM plan, evaluate and improve its effectiveness, and adapt it to changing needs. Planning is not a perfect process, and even if an organization could develop a perfect plan, change is a constant issue. Without a focus on sustainment, the plan will become irrelevant and will not be used, increasing the alert originator's exposure to cybersecurity risks. Accordingly, an organization should build activities into the CSRM plan for review and update of the plan, both periodically and as changes are identified that affect the plan.

Some of the changes that might trigger a review and update include

- staff changes and ongoing training needs
- equipment changes and technology refresh decisions
- vendor technology and service upgrades
- new capabilities from IPAWS that change alert submission rules
- identification of new threats or methods of cyber attack

The example in Appendix G includes activities for sustaining the plan (Activities 13–16).

8 The Big Picture: A Resilient Alert Origination Capability

The WEA capability provides a valuable service, disseminating emergency alerts to users of capable mobile devices if they are located in or travel to an affected geographic area. However, like other cyber-enabled services, WEA is subject to cyber threats that may prevent its use or damage the credibility of the service it provides. Attackers may attempt to delay, destroy, or modify alerts, or even to insert false alerts, actions that may pose a significant risk to the public. Non-adversarial sources of failure also exist, for example, design flaws, user errors, or acts of nature that compromise operations.

This report described a cybersecurity risk management strategy, including a framework and detailed descriptions of activities for WEA alert originators to prepare for and conduct cybersecurity analysis, assess and prioritize risks stemming from all sources of cyber threats and vulnerabilities, and mitigate cybersecurity risks throughout the life cycle. We encourage alert originators to tailor the framework and activities and use them to reduce risk and increase the operational resilience of their alerting capabilities. This report also identified activities to plan, govern execution of, and sustain the CSRM strategy. Again, we suggest that alert originators adapt this information to meet their organizational needs.

Stakeholders operating within each pipeline element have responsibilities for taking action to assure secure, resilient operations. Although this report has focused on a strategy for cybersecurity risk management from the perspective of alert originators, the strategy can be tailored and applied to any element in the pipeline. And while alert originators do not have control over the entire pipeline, they need to be aware of the issues that may unfold throughout the pipeline and respond to them appropriately. We hope this strategy is a useful aid to assuring cyber-resilient operations of the WEA capability and of future alerting and emergency management technologies.

Appendix A General Cybersecurity Observations from Stakeholder and Vendor Interviews

A.1 Introduction

As part of our approach to developing the WEA CSRM strategy, we participated in a number of interviews with WEA stakeholders (alert-originating organizations) and prospective vendors. Our goal in doing so was to gain an understanding of the practices and methods used in their environments to prevent, detect, respond to, and recover from cyber attacks. Generally, we found a lack of focus on cybersecurity, which is not that surprising, given that many organizations across the public and private sectors, even those responsible for our nation's critical infrastructure, have not implemented adequate cybersecurity controls and practices [GAO 2013]. Another reason we were not surprised is that until recently, many of the systems used by emergency managers to generate alerts were not connected to the public internet and so were not exposed to the high degree of risk that they are exposed to today.

In this appendix, we present the responses that we received to security questions posed during interviews as follows:

Alert Originator Cybersecurity Questions

We developed the set of questions identified in Section A.4.1 to determine the level and quality of alert originator focus on security. We soon found that stakeholders were unable to provide satisfactory answers to these questions, which prompted a move to questions tailored to each interviewee's level of expertise and level of concern related to threats and vulnerabilities. Table 18, Stakeholder Responses to Cybersecurity Questions, summarizes responses to these questions.

Vendor Cybersecurity Questions

We developed the set of questions identified in Section A.4.2 to determine the level and quality of vendor focus on cybersecurity. We submitted this list of security questions to selected vendors but did not receive responses to these questions. We also asked general questions during vendor interviews. As Table 20 illustrates, the interviewees provided little information on vendor security practices and methods.

Key Finding and Concern

The key finding from our interviews is that most of the alert-originating organizations we dealt with do not possess a concrete and comprehensive awareness of the cybersecurity risks that they face on a daily basis. Without such awareness, it is difficult to develop a culture of security that clearly articulates each individual's role and responsibilities for mitigating the risk of cybersecurity incidents that could disrupt alerting services, with potentially disastrous results.

Emergency services, including emergency management and alert origination, constitute one of the critical infrastructure sectors identified in *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience* [White House 2013]. PPD-21 highlights the "shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private

owners and operators of critical infrastructure" to "reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts" relative to incidents that include cybersecurity attacks.

We developed our CSRM strategy to (a) raise awareness of the avenues and implications of cyber attacks on the alerting environment (via mission threads and cyber threat and vulnerability analyses), (b) enable alert originators to construct a focused response to the threats and vulnerabilities in their environment (via cybersecurity risk analysis and prioritization), and (c) clearly articulate roles and responsibilities for cybersecurity risk mitigation in WEA adoption, operations, and sustainment.

A.2 Responses to Stakeholder Cybersecurity Questions

Table 18 summarizes responses to questions that we asked stakeholders regarding their cybersecurity practices and methods. The ID column identifies the stakeholder (SH) with a number. The Interviewee Role(s) column identifies their role(s). The Questions Asked and Response columns summarize the questions asked regarding cybersecurity (see Section A.4.1 for more detail) and the responses provided.

Table 18: Stakeholder Responses to Cybersecurity Questions

ID	Interviewee Role(s)	Questions Asked	Response
SH2-3	Emergency management director	• How do you allow people to bring their own device and still maintain security and interoperability? • [Do you have a backup communication channel?]	• [By using an] internet-based, password-protected system. [We] have a satellite failover.
SH3-2	Product manager	• [Describe] fault tolerance capabilities or … concerns that you have in terms of security.	• We have the system in two places and being able to fail over if one of the systems goes out of service for any reason or is under maintenance.
SH4-1	Emergency management director	• Are there any particular security concerns that you have about the implementation of the CMAS system?	• On my side no, on [the vendor's] side yes. I want to use a vendor that we're already comfortable using [to prevent operator error].
SH6-2	Disaster management consultant	• [No specific question]	• The biggest barrier to vendor entry is the certification process that FEMA has set up [rather than lack of technical skills].
SH8-15	Environmental health and safety director	• [What] pathways [are] used to reach constituents? • During your user trial, did you conduct any tests to look for security vulnerabilities and attempts to insert fake alert messages? Do you have concerns about such vulnerabilities or threats to the security of the system in general?	• [Primary is FM-based]; does not use technology-based secondary channels unless a user signs up for voice *and* text. • [The interview didn't discuss this topic in any detail, but the stakeholder said that the system had to pass certain security tests]

ID	Interviewee Role(s)	Questions Asked	Response
SH11-1	RFP	NA[18]	• [The system should] allow for the effective administration of system security … parameters from a centralized location. • The system must prevent inappropriate use and maintain data privacy. This includes login and strong password authentication per user. • Security Sockets Layer [SSL] must be used to transmit data across the Internet. • It is desirable for key data to be encrypted in the database. • Vendor employees with access to any [redacted] County data must have undergone background investigations.
SH11-2	Communications planner and director	• Did you look at the various security implications of the different solutions?	• That wasn't something specifically that we identified in our [RFPs] knowing that the MOA that we have with FEMA defines some of those security requirements.
SH12-1	RFP	NA	• [The system should] provide security by ensuring all documents, contacts, inventory data, and other information is safe and HIPAA [Health Insurance Portability and Accountability Act] compliant. All shared data and information [are] fully encrypted. All users have … unique passwords and logins.
SH13-1	Unknown (no transcript)	Unknown (no transcript)	• Four backup methods for internet connectivity. Two are hard-wired, one satellite through vendor, one is the guy's aircard. • Security is important [from a secure connection standpoint, not so much insider threat, which they downplayed].
SH14-8	Emergency management deputy coordinator	• What are the key kinds of threats that you look at when you're requiring or redeveloping IT? • Where [do] you store the certificate? ... Separate from the terminal? • Are people allowed to put removable media in the system? • [Is there] security training for all the operations?	• Well on the other side of the fence we don't give a rat's butt. We buy what's out there because that's what's being recommended and we go forward with it. • Correct, totally isolated. Now as far as what you have brought up either with cyber secure and all that, that's a point I didn't even think about in regards to somebody coming in and spoofing and doing all that stuff. • Right now in that particular PC, no. There is no access to that thing. There [are] only right now three people who have the password just to even log in to the computer. • Any new IT product ... has to go through [review]. When we first started back in 2003 and we brought all this stuff in, I didn't know what the process was so we [circumvented it].

[18] NA indicates that the source of data in the Response column was a document, such as an RFP, rather than an interviewee.

ID	Interviewee Role(s)	Questions Asked	Response
SH19-1	Grants manager and public information officer	Unknown (no transcript]	• Will have some pretty tight security requirements when they pull the trigger.
SH20-1	Systems engineer	• [Are there] any security issues about making sure that only authorized personnel can get a hold of the equipment or the software?	• I don't believe so. [The servers and clients] that we've deployed are all in, you know, fairly secure areas or places that there's restriction to access. And all the clients make a secure connection through the server and then – and it requires a user name and password to access the system. And then it, you know, it logs – if something is sent out it logs you know the user that sent it so on so forth. So there's, you know, it could be traced if somehow something was done inappropriately.
SH22-3	RFP	NA	• [The system] will be hosted by the vendor "in the cloud" and will be accessible over secure, encrypted internet connection via web browser from any location. • The system will have a mechanism of assignment of Super Administrator, Administrator, and User permissions and passwords such that access to the system of modification of permissions by unauthorized persons is prevented. • When implementing the System in each PSAP, the Vendor will provide the System in accordance with the security requirements of each PSAP [i.e., specific encryption and authentication, authorization, logging requirements]. • Security measures will be provided in accordance with the IT industry's best practices. The bidder shall provide a security plan which addresses the best practices they are using in their proposal. The major components of the security plan will include details concerning the security architecture which includes the Network, Platform, Physical, and Process. • The Vendor's Physical place of business shall provide secure access such as door keys, locks, key cards, security cameras, audible and visual alarms, and system or device labels. • Process security includes Vendor security policy and procedural documentation that governs the creation, use, storage, and disposal of data, as well as the Systems and networks on which the data resides. Process will also include detailed information concerning secure access methods, as well as account and password requirements for obtaining data. • Attention will be given to the privacy of user account information, which will be strictly controlled by the access provider. The successful Vendor will not only provide the listed security best practices, but also provide for data confidentiality, data

ID	Interviewee Role(s)	Questions Asked	Response
			integrity, and data availability. These security items will need to be detailed in the Vendors Proposal. • Precautions will be provided by the Vendor to protect the Confidential Information in [redacted] System. • The Vendor will provide the name and date of any security certification received by Vendor from a third party. • The Vendor shall immediately notify [redacted] of any breach of security where a third party has acquired any of the [redacted] data provided to Vendor.
SH22-7	Communications manager	• Did any of your vendors talk to you about security and how they developed their product?	• [Resilience] was probably higher on our list than maybe security was which is not necessarily a good thing. [The vendor follows] federal guidelines on how they do the passwords to access the system and those kind of things.
SH22-8	County officials, fire chief, and public-safety answering point (PSAP) operators	• [No specific question]	• Confidentiality and personal information is the focus of training. • [The vendor] has encouraged generic login for all dispatchers. • Can log into [the system] from smartphones. • They have separate login for administrators; many operators have administrator privileges. • Don't change generic login when someone leaves. • Dispatchers have thumb drives which they think has some security or protection on them. • Some centers have one network for 911 and CAD that's isolated, but not all of them. The [system] terminal has internet access.
SH23-1	Assistant director	• How important is security and privacy to you relative to ease of use of the system?	• You don't want somebody who can initiate a message who shouldn't. You've got to be able to control that. That would be a really big bad ugly day if somebody got into my system and was able to initiate a message that looked like it was coming from Emergency Management ...; beyond that, I'm not sure that there's much more concern. I would say just access to initiate a message would be the biggest concern.
SH26-1	Emergency management director	• Do you have any security requirements ... ? • How important is the security and privacy of your data?	• [Our system requires] logon credentials to even get into the box to do anything, to even develop a message. • It's pretty important, but you know we also have [systems with databases which are] hosted nationally ...; it kind of depends on the data.

ID	Interviewee Role(s)	Questions Asked	Response
SH27-2	Special projects director	• [Do you have concerns about the] security of your alerting solution?	• Security will be a big piece of it because I can imagine nothing worse than unauthorized entities getting in and monkeying with an alerting system. I mean, there are worse things but as a communicator, that one is pretty scary to me, so security is a big deal.
SH30-45	Physical scientist and warning coordination meteorologist	• How do you authenticate your message(s)? • Does each one of your offices have their own [certificate]? • How do you know that the alerts are going through ...? • Are you keeping all of your software and all your pieces entirely separate? • Do you have requirements for security, reliability, and other things that you're building into this [new package]?	• We just use the standard mechanism ... there's a digital certificate I believe. • No. • [IPAWS] sends us several responses. And one of those is whether or not it qualifies for CMAS ... but that's as far as [it goes]. • We do the post-processing and then we go out over the internet ... to push the message to [IPAWS]. We wanted ... a more dedicated, VPN-like connection to [IPAWS]. And that's something that we're working with them. • Yes, but that's really not my area. I can connect you with the people who can tell you about that stuff.
SH30-46	Physical scientist and software branch chief	• Can you say anything about the certificate management approach you use? • [Do] you have information systems training? ... Do you think it's pretty effective? • Do you do any kind of testing with CMAS specifically? • What did you do to recover from [a removable media violation]? • [Are] insider threats [a] part of your training? • Other than the kinds of risks we discussed, are there any others [that concern you] from a cybersecurity perspective?	• I don't know that we've implemented any specific rules around that certificate. Maybe that's something we should look into. [But it is stored separately.] • We have to take a very basic security training course every year ... it's not perfect by any stretch, but it's pretty effective. • No, we're not doing any sort of a test at this point. [Note: does monitor comm channels for connectivity] • In this particular case the person realized that somebody was missing from the tour ... he turned around and backtracked, saw the person sitting at a workstation, saw the thumb drive and ... walked up immediately behind the PC ... and pulled out the internet cable. • That's part of the IT security [training]. • There's various ones but none ... that jumps out to me.
SH32-1	Executive director, Technology Services Division	• Was [the developer] an experienced web developer familiar with XML, SOAP, security certificates and all that? • [General statement regarding EAS zombie hack]	• Yes. • CMAS has much more stringent [security measures than EAS].
SH33-1	RFP	NA	• The emergency notification system must be delivered via SaaS [software-as-a-service] to ensure that no hardware or software must be purchased or maintained by [redacted] and so that the solution is still secure and easily scalable on-demand.

ID	Interviewee Role(s)	Questions Asked	Response
			• The solution must have the ability to initiate a notification on any PC with a browser through a secure SSL website. • System must adhere to a “defense in-depth” approach to ensure application and infrastructure security. • The system co-location facilities must be housed in a SAS 70 Type II certified facility. Disclose whether or not your facilities have this certification and describe your physical security. • All network and application servers must be “locked down” with no extraneous services running on them. Describe your network security. • The solution must have security to prevent inappropriate use and to maintain data privacy. This includes login and password authentication on the telephone and on the web. • SSL must be used to transmit data across the internet. Describe your transmission security. • Key data must be encrypted in the database. Describe your database security and encryption practices and techniques. • Vendor staff must have undergone personnel security training. Describe the training. • The application must regularly undergo a security audit. Upon request Vendor must be willing to provide the most recent security audit and test report. • Vendor employees with access to any customer data facility must have undergone comprehensive background investigations. Describe the investigation processes your company has completed.
SH39-21	Security officer	• [No specific question]	• There is this balancing act between security and usability ... it better be easy to use and it better be usable because if it's something that you've got to get retinal scans, and 87 imager passwords and all those other [things] that they come up with, it's – you're never going to get – you're going to get one of these too.
SH40-1	Emergency services coordinators and program manager	• What ... are the key ... non-functional quality attribute-type requirements? • Are you doing anything to ensure that your system is secure? Do you have a security strategy of any sort?	• Security is one of our big issues here. ... The thing with [WEA] is that with the guidance that was written up, a lot of people can access it ... by opening it up to all those people makes me very nervous on how we can manage it and share that information between us. ... Who is allowed to use it, how do we manage it, how do we get the training, and how do we get the feedback on when a message has been sent out?

ID	Interviewee Role(s)	Questions Asked	Response
			• We do have a security strategy. As far as the cloud is concerned, we've got basically everything that we can control is passwords. So we make sure we have complex passwords for our mass notification system. But even more than that, we're able to give permission on who is allowed to generate an IPAWS message and we control that through permission. ... We don't have any control over the cloud, over, you know, Chinese hackers, nothing like that. But what we can control, we control through permissions and passwords.
SH40-2	RFP	NA	• The proposed application must be scalable, offering functionality and security for existing and future local and coordinated regional use, and must be made available by the vendor to the Office of Emergency Services and other municipalities and public safety agencies in the region on terms and conditions consistent with the terms and conditions described in this RFP. • The System shall allow for the use of multiple Client Agencies. Each agency will be able to access a secure contact database and map using a unique account. • The System shall be accessible to multiple, up to 5, concurrent users who can provide an authorized login ID and password, Internet access must be provided through secure socket communications. • System shall, using multiple safeguards, allow managers or system administrators to designate authorized users of the system. • The system administrator of an emergency telephone notification system shall have the ability to create, at minimum, three (3) levels of authorized users, and associated user access and privileges. • The System shall support complex passwords; stored password at a minimum with 128 bit encryption and the transmission of user logons must be encrypted over HTTPS port 443. • The system shall have the ability for audit and login tracking.
SH40-3	Senior emergency services coordinator	• [Describe] existing security mechanisms and areas of perceived vulnerabilities. • Did you perform any security evaluation before acquisition? • Do you have a security breach incident response team? • Is hacking a concern? • What about security risks? How are those managed?	• Security is always an issue – with software on cloud, not much control over it. One thing we are maintaining is a system-assigned password, so that is our control. The other piece is a user name, so we can trace back to user. Another security-related concern is on the other side – the timeliness of going through the aggregator. If [we] have all the security credentials ahead of time, hopefully this will be automated and we can send it out quickly, but if there are security issues, certificate is-

ID	Interviewee Role(s)	Questions Asked	Response
		• Are there any risks you've identified in using a cloud-based system?	sues, expired passwords, there may be delays. • Within county, IT reviews were conducted before purchase. We typically use complex passwords, timeouts, etc. for security concerns. Since it's cloud based, we think [security and reliability are] less an issue than if all the hardware and software were in house: not much to do but training. • NO. We can usually stop mistaken alerts. • Mitigations include system-generated password and username traceability. • Within the county system, IT security people do a review as a preliminary of purchasing the software, but from my point of view, our only security protocols [practices] are connecting through a secure website and using complex passwords. We don't have a formal incident response capability for security issues. We have worked with the vendor, and if an alert is generated by mistake, they can sometimes catch it before it goes out. For tracking, we rely on the vendor. • If the internet is down, we can't get the messages out. There is also the potential for saturating the system.
SH46-1	RFP	NA	• System must allow for unique login ID • System must be able to log in to multiple servers for redundancy purposes. System must be able to keep record of anyone that has logged in successfully or unsuccessfully. • System must allow administrator to set specific permissions for specific users. I.e. Some users may not have the ability to make call outs but to view reports. Please define your system user management process.
SH48-2	RFP	NA	• The system must provide security to all personal information for all subscribers. • There must be a SSO [single-signon] capacity for users to enroll and maintain their contact information based on campus security credentials. The user interface must be through an institution branded web-site. • The solution must be able to facilitate unattended, automated and security contact data upload and update from existing database systems.
SH49-1	Interoperability coordinator	• Have you anticipated ... security challenges?	• Yes, and we have security protocols that we put in place for that, that will be also in the RFP to the vendor ... I'm not the cyber guy. I'll have to see where they're at. There's an entire working group dedicated to that. I'll have to see where they're at and maybe get back to you.

ID	Interviewee Role(s)	Questions Asked	Response
SH50-8	Executive director for Converged Technologies for Security, Safety, and Resilience (and others)	• Do you establish approaches for threat identification and vulnerability identification and so forth? • Are you aware of any prior instances where there have been break-ins to your systems? Or attempts to break in? • Is there a community of organizations – IT organizations – that focus on emergency management that you work with or belong to and exchange ideas with?	• I wouldn't personally establish those approaches, but I might work with the IT security office in that capacity. • I think on a university campus there's constant attempts to break in. And in fact, IT security office does have an interesting geographic-based tool to visualize break-ins. • ... from the strictly – just strictly IT, you know, I'm not aware of a whole lot.
SH50-10	Chief technology architect and director of voice and mobile technologies	• Can [you] summarize the cybersecurity risk management approach that they use to guide development or use for procurement? • Are there compliance standards that the chief security officer uses to develop recommendations? • Do they actually specify security requirements along with capability requirements? • What about sustainment with respect to upgrades? Do security practices cover those? • If you suspect an attack, what is the incident response?	• [There is a] set of guidelines that were developed by the chief security officer [that] address most common cybersecurity [threats]. [We] do some penetration testing of applications – test for common vulnerabilities, known sorts of configuration problems with third-party packages, emergency management systems concerning application containers and web services, etc. ... TLS [transport layer security] technology [is] used between components. • [Chief security officer is] very intimately involved with SANS ... find that detail on their website. • Yes – both with respect to end users of applications and intercomponent communications. • [We conduct] periodic reassessment – especially with respect to security requirements imposed by the security office. • A security office should answer. If they suspect a system, it should be removed or cordoned off. [A] small group of folk within the security office do forensics to collect info and track down [the actor].
SH50-18	Chief information security officer	• Were you actually involved in part of the acquisition working with language to make sure that the vendor would be supported of security? • Was there specific acquisition language [relating to security] that that was contracted? • How closely did you actually look at the technology itself? ... You mentioned that you had done a security review. • Was the vendor selected based on their security capabilities? • Are you aware of any current security limitations that that system has?	• Yes. • I don't remember. I know in the time since then we've got sort of a security questionnaire that we hand out to vendors. • It was kind of a high level just to make sure that they weren't, you know, they weren't vulnerable to the sequel injection or cross-site scripting attacks. • Not necessarily. I mean the primary thing was did it actually, you know, do what it was supposed to do. • No, really from a security standpoint right now ... we feel like we've taken ... as many precautions as we can. • No, I would recommend it. In fact I think the one thing I want to emphasize is that the security review process that we did for this particular product was no different

ID	Interviewee Role(s)	Questions Asked	Response
		• Was the strategy that you used with the acquisition review and the security testing something that you would recommend for other organizations? Or ... are there suggestions about how they should do it differently? • Have you experienced any problems with fake messages, spoofing, any [actual] vulnerabilities, attacks or anything like that? • You mentioned the OWASP Top Ten. Are there any other security standards that you enforce that you rely on?	than what we would do for any other product. • No. IP spoofing – while we can't prevent IP spoofing on our network, we ... do know that anybody who manages to do an IP spoof of a machine in our network has to be in the same subnet as the victim machine. • We used to use the SANS Top 20 internet threats. Might be another one that we might use on occasion. But really the reason why we've shifted our focus more to the OWASP one simply because the majority of the applications that we see coming from vendors are web based now.

Analysis of Results Documented in Table 18

As noted previously, the results of our earliest stakeholder interviews illustrated the ineffectiveness of using a standard set of cybersecurity questions. As such, we adopted an interview strategy based on customized lines of questioning. While this method did provide more useful information, it also precluded the ability to make direct comparisons between stakeholder responses. Further, the varying degrees of knowledge and experience among respondents rendered comparison between organizations ineffective at best.

With these limitations in mind, we performed an affinity grouping analysis of stakeholder responses. Table 19 depicts the affinity groups derived from our analysis. Based on these results, we drew the following conclusions:

- Stakeholders most commonly discussed access control, and within access control, their responses typically related to password-based control.
- Though alerting technology is evolving, stakeholders' security knowledge is not keeping pace (evidenced by a lack of discussion regarding topics like cloud-based access or removable media restrictions).
- The breadth of topics (represented by the affinity groupings) and the inconsistency of responses related to each topic indicate that security is a multifaceted area and that the stakeholders we interviewed lack a shared understanding of the issues.

These findings underscore the assertion that many alert-originating organizations lack a concrete and comprehensive awareness of cybersecurity risks. Additionally, individuals often indicated or implied that security is "someone else's problem," be it an associate's, the vendor's, and even FEMA's or DHS's. We believe that this typifies a lack of awareness among many alert originators that security is everyone's job.

Table 19: Affinity Grouping of Stakeholder Responses

ID	Access Control	Availability	Usability	MOA and Certificates	Testing	Encryption	Background Checks	Confidentiality	Threat Modeling	Removable Media	Training	Policy	Logging	Physical Security	Mobile Access	Disruption of Alerting	Scalability	Defense in Depth	Information Sharing	Incident Response	Acquisition
SH2	*	*																			
SH3		*																			
SH4			*																		
SH6				*																	
SH8		*			*																
SH11	*			*		*	*														
SH12	*					*		*													
SH13	*	*																			
SH14	*			*					*	*	*										
SH19												*									
SH20	*												*	*							
SH22	*	*		*		*		*		*		*	*	*	*						
SH23	*		*													*					
SH26	*							*													
SH27	*															*					
SH30	*			*	*				*	*	*	*	*								
SH32				*												*					

ID	Access Control	Availability	Usability	MOA and Certificates	Testing	Encryption	Background Checks	Confidentiality	Threat Modeling	Removable Media	Training	Policy	Logging	Physical Security	Mobile Access	Disruption of Alerting	Scalability	Defense in Depth	Information Sharing	Incident Response	Acquisition
SH33	*				*	*	*	*			*			*			*	*			
SH39			*																		
SH40	*	*		*		*					*		*			*	*				
SH46	*	*																			
SH48	*					*		*													
SH49												*									
SH50					*	*			*			*	*			*			*	*	*
Total	**15**	**7**	**3**	**7**	**4**	**7**	**2**	**5**	**3**	**3**	**4**	**5**	**5**	**3**	**1**	**5**	**2**	**1**	**1**	**1**	**1**

A.3 Responses to Vendor Cybersecurity Questions

Table 20 summarizes responses to questions that we asked vendors regarding their cybersecurity practices and methods. The ID column identifies the vendor (V) with a number. The Questions Asked and Response columns summarize the questions asked regarding cybersecurity and the responses provided.

Table 20: Vendor Responses to Cybersecurity Questions

ID	Question(s) Asked	Response
V1-1	• For your web access does each site have, each county have its own logon or do you have individual people so that you can determine which person actually sent the message? • Can they just log on from any web portal as long as they have their username and password? • Are you using standard web security like SSL for controlling the traffic? • Are you actually getting feedback from IPAWS when you turn the message in?	• Oh yes each county has what we call an account and there's one person there who is the admin that he's the guy that allows his user to use whichever components. • Yes, they need to have username, password, and town. • Definitely, yes. • We do get an acknowledge that IPAWS pretty much delivers the message to the cell carrier. But from that onwards there is no information.
V2-3	• Have you done a formal security evaluation on your technology? • How are you interfacing with the client? • How frequently are you upgrading your software?	• Yes, we do ... code analysis [and] security scans. • It varies from client to client. Most of our systems are typically installed at client site ... We do have a couple sites that are hosted through a cloud provider. • About four upgrades per year. And that's a mixture of feature enhancements and any fixes that might need to happen. Critical vulnerabilities that affect security or just, you know, usability of the system, just making the system unusable will get done outside of that kind of scheduled updates as well.
V3-3	• Can you tell us something about the security aspects of your product?	• Our products are actually certified in accordance with [Federal Information Security Management Act] practices. We also take it a little bit further within the Department of Defense so that everything is certified and accredited under ...DIACAP [Department of Defense Information Assurance Certification and Accreditation Process].
V4-2	• [No specific question]	• [With] our system ... there are no privacy concerns. I mean it's every bit as secure and private as your wireless carrier information is today.
V5-3	• [Does your training include] anything specific to security? • Do you worry about the customers' devices that are connected to your system? • Have you done any kind of defensive programming? • Are you doing any kind of monitoring of that connection for strange behavior? • Are you monitoring in case one of their local devices ends up being compromised? • Does the [alert originator's] certificate when they get their MOA come back to you?	• We don't really offer any of that. • We always worry about that but there is only so much that we can do as a vendor. • Yes ... but it's more on the server side in our infrastructure rather than at the end device. • Yes. • Yes and no. We monitor all of the critical points – so state, federal level, and things like that. Below there, we have station monitoring tools that allow them to monitor who's offline, who's online, what the status of the different endpoints and stuff are. • It goes to the submitter.... And then they pass the certificate to us. So that is encrypted payload that they usually email to us, and then we recommend that they call us and give the passwords so that we can put them into our vault. And then we unlock it and load it on to our IPAWS gateway servers.

ID	Question(s) Asked	Response
	• Have you ever seen [a compromised certificate]? How would you know it's been compromised? • So, you are saying that there really aren't consistent vendor criteria that's being enforced?	• We have certainly not seen that ...; you wouldn't know until it's too late, unless ... it would be reported from the end user. • Not that I have seen ... aside from the MOA.
V6-3	• Could you talk a little bit about the security aspects of the ... product?	• You have to have a password to log in into the system itself ... you have to have a certain level of rights to be able to [generate a message]. [The user takes] some training on IPAWS before the FEMA guys give them that certificate.
V7-1	• [No specific question] • [No specific question] • [No specific question] • Do you have protections on your system for things like the denial-of-service attacks?	• We have our IPAWS system, for security purposes, rather isolated from the rest of [the system]. We actually have the web application software running on computers behind separate firewalls on a separate subnet and have separate login information to protect the private keys of the COGs that we have. • We ask [clients to] send us the private key encrypted by certified mail and then the password to encrypt that separately like by e-mail. And nine out of ten times our clients will e-mail us everything together in one package unsecurely. • If FEMA would work directly with a vendor ... our clients [would] never even see that private key, that's best for everyone involved since they don't need it. We need it because we send the message on their behalf. • We have some dedicated network security appliances in each of our facilities that detect denial-of-service attacks. Some more sophisticated new exploits. I don't know the full details of that, as that's handled primarily by our network administration, whereas I'm really a software developer.
V7-2	• [No specific question] • [No specific question] • [No specific question]	• We are kind of junkies for security anyways. We maintain the keys on separate servers and we co-locate those with our dialing facilities. So we have three separate servers that are maintaining the digital keys for the IPAWS program out there. • We put together this entire process for somebody to send us the key and they would send us that key by set actually. It provides the [inaudible], they send it to us and then they provide the password separately for this one. • We went out there and did some very particular things to protect them. So we don't even keep the digital keys on a server that runs any other component of the [system].
V9-1	• How much visibility do you have of the alerts being successfully sent ... ? • How do you handle the protection of their credentials, because those are actually sent to the originator and then somehow have to get onto this iPad? • Do you actually train your users in security, so they understand the importance of the certificates and protecting their iPad and things like that? • What do you do in terms of the development of your product to address security issues? Have you identified threats and work on vulnerabilities assessments?	• As an originator, we have the ability to post that message to IPAWS and see any returned codes coming back from IPAWS. • Every iPad sends the message through our server, that's how we're allowed to do validation on that message before we post it to IPAWS. So that server is where the digital certificates are stored. They're not stored on iPad individually. • No, I'd have to honestly say, we don't at this point. I think it's an area that we need to do some more with. • You know, it's a little bit outside of my purview in terms of my role with the whole product, so I can't go into too much detail on that.

ID	Question(s) Asked	Response
V10-2	• [No specific question]	• It is a browser-based application. ... We follow the [NIST] security standards. ... You know, we have those levels of security and, you know, we really have – we pass the gold standard with the application. And I can't remember the rest of the nomenclature for doing that. I'm not one of the security guys.
V11-1	Unknown (no transcript)	• Different clients with different level of security

Analysis of Results Documented in Table 20

As was the case with alert originator interviews, we found that we obtained more useful information when we tailored our questions to the interviewee's role. Again, this strategy made direct comparisons between vendors impractical. To analyze our findings, we employed the same affinity grouping analysis framework that we used for stakeholders. The results are depicted in Table 21.

Based on this analysis, we drew the following conclusions about the vendors with whom we spoke:

- The vendors were concerned with a greater variety of security issues than were the alert originators.
- The vendors seemed to be more aware of current security concepts.
- The vendors seemed to be more aware of the security guidelines in the IPAWS-OPEN MOA than their alert originator counterparts.

Unsurprisingly, our findings indicate that vendors were better prepared than alert originators to discuss cybersecurity concerns. However, we cannot conclude that their understanding is complete. Further, we cannot conclude that their products and services reflect their knowledge of cybersecurity risks. This is a concern, as many alert originators rely on their vendors to ensure security. Additionally, some vendors indicated that they do not provide security training to clients, which is a missed opportunity for emphasizing its importance and providing valuable guidance. Finally, the observation that vendors are more aware of security does not apply across the board: One vendor recommended that the alert originator create a single account for all users of the WEA capability.

Table 21: Affinity Grouping of Vendor Responses

ID	Access Control	Availability	Usability	MOA and Certificates	Testing	Encryption	Confidentiality	Threat Modeling	Training	Policy	Logging	Mobile Access	Disruption of Alerting	Scalability	Defense in Depth	System Updates	Secure Coding
V1	*					*					*						
V2	*		*		*											*	
V3				*						*							
V4							*										
V5				*					*		*		*				*
V6	*								*								
V7	*	*		*									*		*		
V9				*				*	*			*	*				
V10					*												
V11														*			
Total	**4**	**1**	**1**	**4**	**2**	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**3**	**1**	**1**	**1**	**1**

A.4 Cybersecurity Question Sets

A.4.1 Stakeholder Cybersecurity Question Sets

We developed two approaches to asking stakeholders cybersecurity questions. The first was to use the set of questions documented in Table 22, designed to be asked along with other questions related to integration strategy during a 60–90 minute interview. The second approach was to ask two more open-ended questions on cybersecurity. We began using the latter approach when the first did not produce results consistent with the level of detail in the questions; that is, responses were along the lines of "I don't know," "That's so-and-so's job," or "Our IT staff handles all that."

Table 22: Stakeholder Cybersecurity Questions

Area of Concern	**Questions** *Begin by ascertaining interviewee roles and modify questions accordingly*
Technology providers–security considerations *[If role includes IT procurement; else ask who has this role]*	In your approach to acquiring IT products and services, • do you use language in your contracts/agreements that specifies requirements for (1) security controls, (2) secure development practices, and (3) product security? • how do you verify compliance with these requirements? How well has your approach worked? Is it effective at • reducing high-impact vulnerabilities before product delivery or deployment? • identifying and mitigating latent security vulnerabilities? What would you do differently? Would you be willing to share any artifacts (acquisition processes, contract and agreement language, product security requirements, required secure development practices) that would help us understand how you address product and development security during acquisition?
Internal development–security considerations *[If role includes development; else ask who has this role]*	For internal development, what security controls and secure development practices do you use? Do you specify security requirements for internally developed systems? How do you verify compliance? How effective are your internal practices at reducing high-impact vulnerabilities? What do you think you need to change?
Security concerns *[If organization participated in user trial]* Additional security questions *[These may be more broadly relevant, but if interviewee cannot answer, ask who has this role]*	During your user trial, did you conduct any test to look for security vulnerabilities or attempts to insert fake messages? Do you have concerns about such vulnerabilities or threats to the security of the system in general?
	What approach(es) do you use to identify threats to your systems? How do you keep your threat assessments current? Do you believe your approach is effective? If not, how would you change it? What do you believe will be the key threats to WEA?
	How do you test new and upgraded products for vulnerabilities? Do you believe your approach is effective? If so, why? If not, how would you change it? What do you believe will be the key product and network vulnerabilities impacting WEA?
	What technical challenges (with respect to security) do you anticipate for WEA over the next 3–5 years? What aids or technologies might help?
Governance–security considerations *[If role includes or is affected by governance]*	What organizational or governance challenges (with respect to security) do you anticipate for WEA? What governance structures might help?

Overarching Stakeholder Cybersecurity Questions

Given the difficulties of gaining access to staff who could respond to the questions in Table 22, we modified our approach to instead ask the following more open-ended questions:

- What are the most significant cybersecurity risks to your alert origination process and technologies (current and planned, including WEA)?
- What are you doing (or planning to do) to manage these risks?

A.4.2 Vendor Cybersecurity Question Set

Based on our discussions with a variety of stakeholders, we developed a question set that may aid alert originators during security-related discussions with prospective vendors:

1. How can you demonstrate that the system complies with the security measures (i.e., the rules of behavior) specified in FEMA's IPAWS Memorandum of Agreement?
2. Do you provide training to system operators? If so, how does training approach the topic of security?
3. How is access to the system controlled?
4. Does the system provide administrative tools to manage user accounts?
5. What protections does the system have to ensure that the alerts I send will successfully reach cell phone recipients?
6. How will you ensure that the system will transmit only authorized alerts?
7. How do you handle system updates?
    a. How often do they occur on average?
    b. How will I ensure that the updates are legitimate?
    c. How will your update process affect my use of the system?
8. Please describe the development practices that you use to ensure security, including
    a. secure development of software that you create
    b. managing risks associated with third-party software that you use to create your products and services (i.e., managing software supply-chain risk)
9. Do you regularly test the system for vulnerabilities? If so, how?
10. If a security incident occurs, what type of support do you offer?

Appendix B WEA Mission Thread Analysis

A mission thread is an end-to-end set of steps taken to respond to an incident or execute a mission. Mission threads are used to describe a process at a level that is meaningful to a system user. Each mission thread begins with an event (e.g., an imminent threat or abduction) that drives the generation of a WEA message.

Alert-originating organizations responsible for acquiring or developing IT products and services to implement a WEA capability often focus more on functional capabilities than on quality attributes such as security, performance, and resilience. Functional capabilities are simpler to envision, specify, and verify than quality attributes. A key benefit of the mission thread approach is that it provides a clear, simple model that organizations can use to identify and address gaps in their current approach to cybersecurity risk management, from early requirements-specification activities through development, delivery, deployment, and sustainment.

For the approach to be effective, validating the mission threads with alert originators is critical: It is imperative that the mission steps capture the key technical, operational, and management process steps subject to cyber threats. Then, alert-originating organizations can analyze these mission steps for vulnerabilities and apply the corresponding mitigations. Validation with alert originators will also elicit information on how the system may not function as intended under all circumstances, and what this means to mission completion. We validated the generic operational mission thread used in Sections 3 and 4 with colleagues in the alert origination community who are also IT and security experts. We encourage readers to review these mission threads and refine them to reflect their own environments, procedures, and scenarios of interest.

B.1 Mission Thread Analysis Approach for Security

Mission thread analysis (MTA) examines in detail each step in the mission thread that is relevant to the quality attribute or system characteristic in question (in this case, security). Each MTA consists of introductory information, a list of relevant steps, and the analysis of each step, which consists of preconditions, actions, postconditions, claims, failure outcomes, potential causes of failure, and issues. In particular, we identify content relevant to the selected analysis focus (security). Claims describing how the actions in the step contribute to success of the selected focus (e.g., security) within the context of the mission thread are assembled along with failure outcomes should each claim fail. Potential causes of failure are the ways in which some element within the step (precondition, action, or postcondition) contributes to a failure outcome.

For the purpose of security analysis, the approach to using mission threads consists of the following five tasks, which are performed iteratively.

Mission Thread Development and Preliminary STRIDE Analysis

Task 1 Analyze scenarios from the *CMAS Concept of Operations* [FEMA 2009] and information from interviews with alert originators. Identify the key components of the WEA pipeline for security analysis. Create preliminary mission threads that represent the nominal behavior of WEA pipeline elements when an alert is generated, processed, and disseminat-

ed. Do this for one imminent threat alert, one AMBER alert, and one presidential alert. This appendix contains a mission thread example for each alert type.

Task 2 Create a generalized mission thread based on the specific mission threads produced in Task 1. Section 3 of this report contains a generic mission thread derived from the three specific mission threads in this appendix.

Task 3 Conduct security analysis using the generalized WEA mission thread produced in Task 2 to identify critical assets, threats to these assets, and common vulnerabilities that might make the assets susceptible to threats. Section 4.1.1 of this report contains a security analysis using the STRIDE approach to identify threats and vulnerabilities to critical WEA assets [Microsoft 2005, Howard 2006].

Mission Thread Validation and Adaptation to Stakeholder Environments

Task 4 Using working sessions or interviews with stakeholders, review the generic and, as applicable, specific mission threads and refine the steps as needed. Review the security (threat and vulnerability) analysis, and ask stakeholders to identify operational variations of interest (see Section 4.2 for examples of operational variations). Tailor the mission thread and security analysis to illustrate the security implications of these variations (see Section 4.2.1 for an example of tailoring and analysis).

Detailed Mission Thread Analysis

Task 5 Following the working sessions or interviews, conduct detailed MTA for each tailored mission thread. MTA examines in detail each mission step that is relevant to security and the causes of failure associated with these mission steps. MTA identifies detailed preconditions, actions, postconditions, claims, failure outcomes, potential causes of failure, and issues. Use the results to identify critical risks and risk-mitigation actions. See the examples that follow.

Tasks 1 and 5 (develop specific mission threads and analyze these threads) are illustrated in this appendix. Tasks 2 and 3 (perform generic mission thread and top-level threat and vulnerability analysis) are shown in Sections 3 and 4 of this report. Task 4, which is not shown in this report, consists of a set of interviews and working sessions that we conducted with stakeholders to validate and supplement the mission threads.

The remainder of this appendix contains three operational mission thread examples, one for an imminent threat alert, one for a presidential alert, and one for an AMBER alert. These examples incorporate Tasks 1 and 5, above. For Task 1, we present the operational mission thread. For Task 5, first, we extract the mission steps relevant to security analysis and decompose them to expose substeps relevant to the analysis. Then, we present the detailed MTA.

B.2 Structure of the Mission Thread Analysis Examples

Each MTA example in this appendix has three sections: the mission thread, mission step decomposition for security, and MTA for security.

Mission Thread Structure

Each mission thread is presented in a table that is structured as follows:

- Mission thread description
  - Name: Name of the mission thread
  - Vignette (summary description): The environment before the event occurs
  - Nodes and actors: People, equipment, and facilities in the environment that may respond to, or be affected by, the event and one another (For the WEA mission threads, nodes and actors represent WEA elements and components.)
  - Assumptions: Conditions related to the environment and characteristics of the nodes and actors that we assume to be true at the start of the mission thread
  - Environmental context diagram: Graphical representation of the environment
- Mission thread steps

Mission Step Decomposition Structure

The mission step decomposition contains

- a header block that includes the following: mission thread name, scope of the analysis, nodes and actors, characteristics analyzed (in our case, security), assumptions, and a systems context diagram
- a table that breaks down steps relevant to security into substeps for detailed analysis

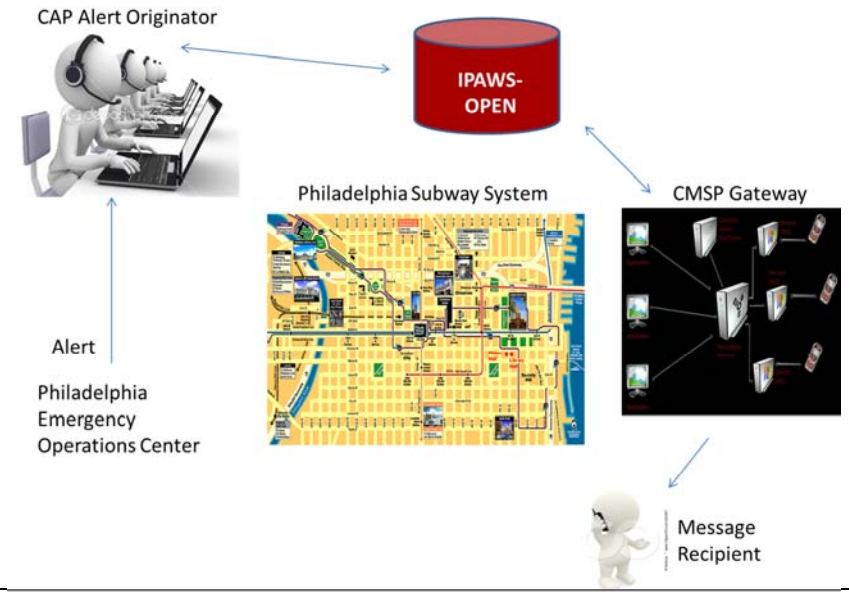
Mission Thread Analysis Structure

The MTA consists of a table for each security-relevant mission thread substep, including

- preconditions, actions, and postconditions relevant to security
- claims describing how the actions in the step contribute to successful implementation of the attribute of interest (e.g., security) within the context of the mission thread
- failure outcomes should each claim fail
- potential causes of failure, that is, the ways in which some element within the step (pre-condition, action, or postcondition) contributes to a failure outcome
- issues that arise during analysis that need further study (Issues may expose additional potential causes of failure or an inability to effectively detect or recover from failure.)

B.3 Mission Thread Analysis: Imminent Threat Alert (Philadelphia Subway Bombing)

B.3.1 Imminent Threat Alert Operational Mission Thread

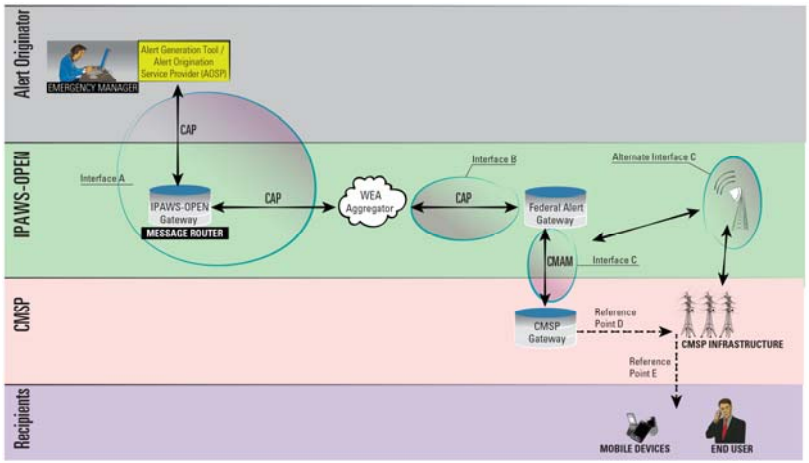
Name	Philadelphia Subway Bombing (Imminent Threat Alert)[19]
Vignette (Summary Description)	The Philadelphia subway system consists of both above- and below-ground stations. Multiple cell phone providers offer coverage for the city of Philadelphia. FEMA has set up IPAWS to support the East Coast of the United States. FEMA has a primary operations center and a regional EOC that covers the East Coast of the United States. For this vignette, a Philadelphia EOC is the CAP alert originator.
Nodes and Actors	Philadelphia Transportation Authority Control Center (alert identifier), Philadelphia EOC (CAP alert originator), IPAWS, cell phone service providers, cell phone subscribers, and FEMA Operations Center (FOC)
Assumptions	• No power disruptions besides where the bomb exploded • Normal weather conditions • Normal civil alert level • Required Monthly Test (RMT) is handled in another mission thread (Note: These messages may take as long as 24 hours to be sent over CMSP Infrastructure.) • All WEA functions are available and operational • IPAWS consists of the IPAWS-OPEN Gateway, WEA Alert Aggregator, and Federal Alert Gateway *Note: These are just example assumptions; there would likely be more.*
Environmental Context Diagram	

[19] The source for this vignette is the CMAS Concept of Operations [FEMA 2009].

Name		Philadelphia Subway Bombing (Imminent Threat Alert)
Mission Steps[20]	**Time**	**Description**
1	6:05 a.m.	The Main Street train has just left the Spring Garden Center Station.
2	6:07	Multiple bombs explode in the Spring Garden Center Station.
3	6:08	The Philadelphia Transportation Authority control center notices loss of video and data communications with the Spring Garden Station.
4	6:10	The Philadelphia Transportation Authority informs the Philadelphia EOC that a problem has occurred and the public should avoid the subway station.
5	6:12	The Philadelphia EOC's CAP console operator sends the message to IPAWS.
6	6:15	IPAWS verifies the message, and the WEA-formatted message is sent to the CMSP Gateway.
7	6:22	The cell phone providers receive the WEA message and then broadcast the message to appropriate territory based on agreed to level of support.
8	6:24	Mobile device subscribers receive the message.
9	6:25	The message displays on mobile devices.
10	7:30	President orders an alert for the entire nation.
11	7:31	The FOC receives the presidential alert.
12	7:33	The FOC's CAP console operator sends the message to IPAWS.
		(Repeat of Steps 6–9)
13	7:36	IPAWS verifies the message, and the CAP message is sent to the WEA Alert Aggregator.
14	7:45	The cell phone providers receive the WEA message and then broadcast the message to appropriate territory based on agreed to level of support.
15	7:47	Mobile device subscribers receive the message.
16	7:48	The message displays on mobile devices.

[20] Mission Steps 10 and 11 initiate a presidential alert sequence. We demonstrate the MTA for the presidential alert in Section B.4.3. These two mission steps are included in the imminent threat mission thread because they are part of the operational sequence even though they do not relate directly to generating the imminent threat alert.

B.3.2 Imminent Threat Alert Mission Step Decomposition – Security

Mission Thread Analysis Name	Philadelphia Subway Bombing (Imminent Threat Alert) – Security
Scope of Analysis	• Message 1 (imminent threat) in the Philadelphia Subway Bombing vignette • The systems and technology interfaces employed during Mission Steps 5–8
Nodes and Actors	Message originator, AOSP, IPAWS-OPEN Gateway, WEA Alert Aggregator, Federal Alert Gateway, CMSP Gateway and Infrastructure, mobile device message recipients
Characteristic Analyzed	System quality attribute: Security
Assumptions	• AOSP is operating normally. • IPAWS is operating normally. • The WEA service will be used as the mobile alert message distribution vehicle. • Message will be sent in text format (current capability). • Disclosure issues will not be provided since this is a publically distributed message.
Systems Context Diagram	

Description and Decomposition of Mission Steps Relevant to Security Philadelphia Subway Bombing (Imminent Threat Alert)				
Mission Step	**Time**	**Mission Step Description**	**Analysis Substep**	**Substep Description**
5	6:12	The Philadelphia EOC's CAP console operator sends the message to IPAWS.	5	Philadelphia regional EOC enters alert into AOSP and sends it to IPAWS-OPEN Gateway.
6	6:15	IPAWS verifies the message, and the WEA-formatted message is sent to the CMSP Gateway.	6.1	IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator.
			6.2	Message is processed by WEA Alert Aggregator.
			6.3	WEA Alert Aggregator sends validated message to Federal Alert Gateway.
			6.4	Federal Alert Gateway receives and validates message.
			6.5	Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways.

Description and Decomposition of Mission Steps Relevant to Security Philadelphia Subway Bombing (Imminent Threat Alert)				
Mission Step	**Time**	**Mission Step Description**	**Analysis Substep**	**Substep Description**
7	6:22	The cell phone providers receive the WEA message and then broadcast the message to appropriate territory based on agreed to level of support.	7.1	CMSP Gateways receive message from Federal Alert Gateway.
			7.2	CMSPs broadcast to customers.
8	6:24	Mobile device subscribers receive the message.	8	Mobile devices receive message.

B.3.3 Imminent Threat Alert Mission Thread Analysis – Security

This section contains example mission thread analyses for Mission Steps 5 and 6, including the substeps for Step 6 (it was not necessary to decompose Step 5). In addition, for Step 7, we begin completing the analysis table with entries in the "issues" row only.

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 5** **Philadelphia regional EOC enters alert into AOSP and sends it to IPAWS-OPEN Gateway**
Preconditions	Policy Governance • Subways for Philadelphia are declared to be unsafe • Approval to send an alert and warning message to mobile devices in the area has been given • Wireless distribution for CMSP is available to subscribers for target area and message type (How determined?) Authorizations • Alert originator has access to a secure, approved submission device • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated on the WEA service; notification is received from IPAWS system operator People skills • Alert originator is trained on AOSP and WEA messages Technology • Submission capability for wireless alert is available – functionality will depend on originator capabilities (Is this the same as for EAS messages?) • IPAWS-OPEN Gateway access is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?) • Alert originator has access to equipment able to generate message
Actions	Message entered in AOSP system Message designated for Philadelphia region appropriate to subway usage CAP format message generated Message format validated locally? Message sent from AOSP to IPAWS-OPEN Gateway
Postconditions	Message in CAP format submitted to IPAWS

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 5** **Philadelphia regional EOC enters alert into AOSP and sends it to IPAWS-OPEN Gateway**
Claims	1. Originator has received appropriate approval to generate message 2. Originator is approved for IPAWS alert generation 3. System used to generate and send alert is available and functions as intended 4. Platform used to generate and send alert is not compromised 5. Connection used to send alert is available and functions as intended
Failure outcomes	Missing or delayed results: • Message submission fails or is delayed (Claim 4 error) Message content error: • Message not in CAP format (Claim 3 error) • Output is not what was approved (Claim 1 error) • Proper credentials not submitted with message (Claim 2 and 3 errors) • Message is corrupted in transmission (Claim 5 error)
Potential causes of failure	Missing or delayed results • Message entry platform is compromised and send instruction is suppressed (integrity) • Authentication actions failed (availability) • WEA Alert Aggregator connection fails (availability) • Message is queued due to line congestion (availability) Message content error • Software supporting alert operator generates invalid format (integrity) • Send action does not complete (availability) • Platform for message sending is compromised and application has been tampered with (integrity) • Connection with IPAWS fails or is corrupted (availability or integrity)
Issues	What are minimum and expected requirements for submission of alerts to WEA Alert Aggregator? Will a user interface be provided for direct submission to IPAWS or application programming interface for automated send from originator system? How will connection be verified as trusted in addition to the actual originating individual? What are options for originator if IPAWS-OPEN Gateway is not available? Will this depend on originator capability? Will there be a “standard” operation with capability for more advanced sites to automate additional capabilities?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.1** **IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator**
Preconditions	Governance • Approval to send to IPAWS-OPEN Gateway has been established (Will this entry point reject senders? Will sender be notified?) Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated for the IPAWS-OPEN Gateway Technology • Wireless message packet arrives for IPAWS (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?)
Actions	Alert is validated and authenticated Error message is returned to originating government entity if needed and mission thread is terminated Converted message is sent to WEA Alert Aggregator
Postconditions	CAP alert message routed to WEA Alert Aggregator
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid 4. Received message is in proper CAP format 5. WEA Alert Aggregator connection is available
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Message cannot be converted (Claim 4 error) Missing or delayed CAP message from originator (Claim 1 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • IPAWS-OPEN Gateway fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to IPAWS does not include an acknowledgment to the originator [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Will there be capability to automatically wait and retry if WEA Alert Aggregator is unavailable?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.2** **Message is processed by WEA Alert Aggregator**
Preconditions	Governance • Approval to send a wireless alert and warning message from IPAWS-OPEN Gateway to the WEA Alert Aggregator has been established (How is trust relationship established?) Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated for the WEA Alert Aggregator system • WEA Alert Aggregator is staffed with appropriately authenticated operators Technology • Wireless message packet arrives for the WEA Alert Aggregator (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?)
Actions	Alert is validated and authenticated Error message is returned to originating government entity if needed and mission thread is terminated
Postconditions	CAP message processed by WEA Alert Aggregator
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Missing or delayed CAP message from originator (Claim 1 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • WEA Alert Aggregator fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to the WEA service does not include an acknowledgment to the originator [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Is there any history of the IPAWS-OPEN Aggregator being spoofed?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.3** **WEA Alert Aggregator sends updated message to Federal Alert Gateway**
Preconditions	Governance Authorizations Technology • Federal Alert Gateway is available (How determined?)
Actions	CAP alert message sent to Federal Alert Gateway
Postconditions	CAP message transferred to Federal Alert Gateway
Claims	1. Received message is from a trusted and properly authorized source
Failure outcomes	Message originator not a trusted source (Claim 1 error) Message fails validation (Claim 1 error)
Potential causes of failure	Authorization errors • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt, message) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • WEA Alert Aggregator connection fails (availability)
Issues	The architecture document does not include specifics about the Federal Alert Gateway, and the concept of operations does not include error message handing [FEMA 2009]. It appears that error messages only return to the prior step, so how will the originator be made aware of errors that occur beyond the IPAWS-OPEN Gateway? Will there be capability to wait and retry if Federal Alert Gateway availability fails?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.4** **Federal Alert Gateway receives and validates message**
Preconditions	Governance • WEA Alert Aggregator has been established as a trusted provider for the Federal Alert Gateway Authorizations Technology
Actions	CAP format verified Alert logged Receipt notification sent to WEA Alert Aggregator
Postconditions	Notification sent to WEA Alert Aggregator Log updated
Claims	1. Received message is from a trusted and properly authorized source 2. Alert is properly logged 3. WEA Alert Aggregator is properly notified of message receipt
Failure outcomes	Message cannot be logged (Claim 2 error) Receipt notification to CMSP Alert Aggregator fails (Claim 3 error)

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.4** **Federal Alert Gateway receives and validates message**
Potential causes of failure	Authorization errors (receipt delivery) • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity)
Issues	What is the value of the log at this point? Why are prior steps not logged? Is there any history of the IPAWS messages sent from unauthorized sources?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 6.5** **Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways**
Preconditions	Governance • CMSP Gateways have been established as trusted recipients for the Federal Alert Gateway Authorizations • Mobile device service providers for the region to be notified have properly established authorization to receive CMSP messages Technology • Wireless distribution for CMSP is available for target area (How determined?) • CMSP Gateway access for the targeted area is available
Actions	CAP message converted to CMAC format Distribution targets identified and selected: match message distribution target to stored CMSP profiles coverage CMAC-formatted alert broadcasted to selected CMSP Gateway destinations
Postconditions	CMAC message broadcasted to selected CMSP Gateways
Claims	1. CAP message is properly converted to CMAC format 2. Targeted CMSP Gateways are appropriately selected 3. Message is broadcasted to selected CMSP Gateways
Failure outcomes	Message cannot be converted to CMAC format (Claim 1 error) Message broadcasted to wrong destination (Claim 2 error) Broadcast fails or is delayed (Claim 3 error)
Potential causes of failure	Authorization errors (broadcast delivery) • CMSP Gateways not established as valid recipients (availability) Missing results • CMSP connection fails (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity) • Error in mapping data to determine appropriate CMSP for target location (integrity)

Issues	Who is notified of a conversion or CMSP message notification failure? How will anyone know if the broadcast succeeded?

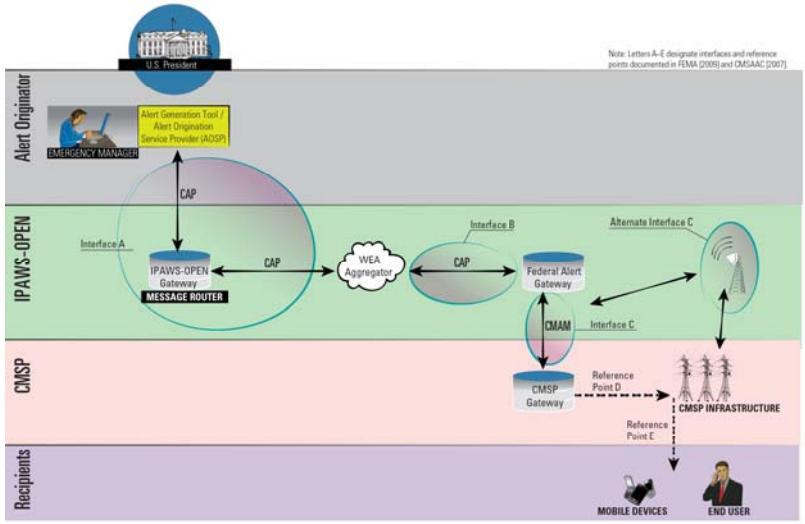
Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 7.1** **Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways**
Preconditions	
Actions	
Postconditions	
Claims	
Failure outcomes	
Potential causes of failure	
Issues	What if the Federal Gateway is spoofed? How do the CMSP recipients know if it is a valid alert?

Philadelphia Subway Bombing (Imminent Threat Alert)	**Mission Step 7.2** **CMSPs broadcast to customers**
Preconditions	
Actions	
Postconditions	
Claims	
Failure outcomes	
Potential causes of failure	
Issues	How does the mobile recipient know if this is a valid alert?

B.4 Mission Thread Analysis: Presidential Alert (Philadelphia Subway Bombing)

B.4.1 Presidential Alert Operational Mission Thread

Mission Thread Analysis Name	Philadelphia Subway Bombing (Presidential Alert) – Security
Scope of Analysis	• Presidential alert message generated in the context of the Philadelphia Subway Bombing vignette • The systems and technology interfaces employed during Mission Steps 12–15
Nodes and Actors	FOC (message originator), IPAWS-OPEN Gateway, WEA Alert Aggregator, Federal Alert Gateway, CMSP Gateway and Infrastructure, mobile device message recipients
Characteristic Analyzed	System quality attribute: Security
Assumptions	• AOS is operating normally. • IPAWS is operating normally. • The WEA service will be used as the mobile alert message distribution vehicle. • Message will be sent in text format (current capability).

	• Disclosure issues will not be provided since this is a publically distributed message.
Systems Context Diagram	

Description and Decomposition of Mission Steps Relevant to Security Philadelphia Subway Bombing (Presidential Alert)				
Mission Step	**Time**	**Mission Step Description**	**Analysis Substep**	**Substep Description**
12	7:33	The FOC's CAP console (AOS) operator sends the message to IPAWS.	12	FOC enters alert into AOS and sends it to IPAWS-OPEN Gateway.
13	7:36	IPAWS verifies the message, and the CAP message is sent to the WEA Alert Aggregator.	13.1	IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator.
			13.2	Message is processed by WEA Alert Aggregator.
			13.3	WEA Alert Aggregator sends validated message to Federal Alert Gateway.
			13.4	Federal Alert Gateway receives and validates message.
			13.5	Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways.
14	7:45	The cell phone providers receive the WEA message and then broadcast the message to appropriate territory based on agreed to level of support.	14	The cell phone providers receive the CMAC message and then broadcast the message to all subscribers.
15	7:47	Mobile device subscribers receive the message.	15	Mobile devices receive the message.

B.4.2 Presidential Alert Mission Thread Analysis – Security

This section contains example mission thread analyses for Mission Steps 12 and 13, including the substeps for Step 13 (it was not necessary to decompose Step 12).

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 12** **FOC enters alert into AOS and sends it to IPAWS-OPEN Gateway**
Preconditions	Policy Governance • National terrorist alert declared by the president • Approval to send an alert and warning message to the nation via mobile devices has been given to FEMA • Wireless distribution for CMSP is available for all subscribers Authorizations • Alert originator has access to a secure, approved submission device • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available (Stored locally or only centrally?) • Approvals for alert originator have been activated on the WEA service; notification is received from IPAWS system operator People skills • Selected FEMA operator is knowledgeable in sending presidential alerts Technology • Submission capability for wireless alert is available; functionality will depend on originator capabilities (Is this the same as for EAS messages?) • WEA Alert Aggregator access is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?) • Alert originator has access to equipment able to generate message
Actions	CAP format message generated Message format validated locally? Message sent to WEA Alert Aggregator
Postconditions	Priority message in CAP format submitted to WEA Alert Aggregator
Claims	1. Originator has received appropriate approval to generate message 2. Originator is approved for alert generation 3. System used to generate and send alert is available and functions as intended 4. Platform used to generate and send alert is not compromised 5. Connection used to send alert is available and functions as intended
Failure outcomes	Missing or delayed results: • Message submission fails or is delayed (Claim 4 error) Message content error: • Message not in CAP format (Claim 3 error) • Output is not what was approved (Claim 1 error) • Proper credentials not submitted with message (Claim 2 and 3 errors) • Message is corrupted in transmission (Claim 5 error)

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 12** **FOC enters alert into AOS and sends it to IPAWS-OPEN Gateway**
Potential causes of failure	Missing or delayed results • Message entry platform is compromised and send instruction is suppressed (integrity) • Authentication actions failed (availability) • WEA Alert Aggregator connection fails (availability) • Message is queued due to line congestion (availability) Message content error • Software supporting alert operator generates invalid format (integrity) • Send action does not complete (availability) • Platform for message sending is compromised and application has been tampered with (integrity) • Connection with IPAWS fails or is corrupted (availability or integrity)
Issues	Will FEMA use originator software or go directly into the WEA aggregator? It will be faster (removes steps) but will require a different set of system capabilities. What are options for originator if WEA aggregator is not available? Will this depend on originator capability? Will there be a "standard" operation with capability for more advanced sites to automate additional capabilities?

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.1** **IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator**
Preconditions	Governance • Approval to send to IPAWS-OPEN Gateway has been established (Will this entry point reject senders? Will sender be notified?) Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available (Stored locally or only centrally?) • Approvals for alert originator have been activated for the IPAWS-OPEN Gateway Technology • Wireless message packet arrives for IPAWS (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?)
Actions	Alert is validated and authenticated Error message returned to originating government entity if needed and mission thread terminates Converted message sent to WEA Alert Aggregator
Postconditions	CAP alert message routed to WEA Alert Aggregator
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid 4. Received message is in proper CAP format 5. WEA Alert Aggregator connection is available

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.1** **IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator**
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Message cannot be converted (Claim 4 error) Missing (or delayed) CAP message from originator (Claim 1 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • IPAWS-OPEN Gateway fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to IPAWS does not include an acknowledgment to the originator [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Will there be capability to automatically wait and retry if WEA Alert Aggregator is unavailable?

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.2** **Message is processed by WEA Alert Aggregator**
Preconditions	Governance • Approval to send a wireless alert and warning message through the WEA Alert Aggregator has been established Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available (Stored locally or only centrally?) • Approvals for alert originator have been activated for the WEA Alert Aggregator system • WEA Alert Aggregator is staffed with appropriately authenticated operators Technology • Wireless message packet arrives for the WEA Alert Aggregator (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?) • Federal Alert Gateway is available
Actions	Alert is validated and authenticated Error message is returned to originating government entity if needed and mission thread terminates Alert is converted to text-based CMAM format Message priority is adjusted (**presidential alert – highest priority**) Converted message is sent to Federal Alert Gateway

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.2** **Message is processed by WEA Alert Aggregator**
Postconditions	CMAM-formatted message sent to Federal Alert Aggregator for distribution
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid 4. Received message can be converted to CMAM format 5. Federal Alert Gateway connection is available 6. Accurate prioritization information is sent to the Federal Alert Gateway 7. CMAM message sent to the Federal Alert Gateway
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Message cannot be converted (Claim 4 error) Missing (or delayed) distribution to Federal Alert Gateway results (Claim 6 error) CMAM message is queued due to line congestion (Claim 5 error) Priority sequence error (Claim 6 error) Missing (or delayed) CAP message from originator (Claim 1 error) Wrong message sent (Claim 7 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • WEA Alert Aggregator fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to the WEA service does not include an acknowledgment to the originator; requirements do not include sending an error message to originator for alerts that fail conversion [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Will there be capability to automatically wait and retry if Federal Alert Gateway is unavailable?

Philadelphia Subway Bombing (Presidential Alert)	Mission Step 13.3 WEA Alert Aggregator sends validated message to Federal Alert Gateway
Preconditions	Governance • WEA Alert Aggregator has been established as a trusted provider for the Federal Alert Gateway • Wireless distribution for CMSP is available to subscribers for target area and message type Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available (Stored locally or only centrally?) • Approvals for alert originator have been activated for the WEA Alert Aggregator system • WEA Alert Aggregator is staffed with appropriately authenticated operators Technology • Wireless message packet arrives from the WEA Alert Aggregator (What is detection mechanism?) • Alert originator is identifiable from message • Wireless distribution for CMSP is available to subscribers for target area (How determined?) • CMSP Gateway access is available
Actions	Alert source and CMAM format verified Failure of verification results in error notice sent to WEA Alert Aggregator Alert logged Receipt notification sent to WEA Alert Aggregator Distribution targets identified and selected: Presidential alert will send to all distribution points CMAM-formatted alert broadcasted to all CMSP Gateway destinations
Postconditions	Notification sent to WEA Alert Aggregator Log updated CMAM message broadcasted to selected CMSP Gateways
Claims	1. Received message is from a trusted and properly authorized source 2. Alert is properly logged 3. WEA Alert Aggregator is properly notified of message receipt 4. Targeted CMSP Gateways are appropriately selected 5. Message is broadcasted
Failure outcomes	Message originator not a trusted source (Claim 1 error) Message fails validation (Claim 1 error) Message cannot be logged (Claim 2 error) Receipt notification to CMSP Alert Aggregator fails (Claim 3 error) Message broadcasted to wrong destination (Claim 4 error) Broadcast fails or is delayed (Claim 5 error)

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.3** **WEA Alert Aggregator sends validated message to Federal Alert Gateway**
Potential causes of failure	Authorization errors • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt, message) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • WEA Alert Aggregator connection fails (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity) • Error in mapping data to determine appropriate CMSP for target location (integrity) Broadcast fails or is delayed • CMSP Gateway is unavailable
Issues	The architecture document does not include specifics about the Federal Alert Gateway, and the concept of operations does not include error message handing [FEMA 2009]. It appears that error messages only return to the prior step. How will the Federal Alert Gateway know that this is a presidential alert and should be sent to all locations? Will there be capability to wait and retry broadcasting if CMSP Gateway availability fails?

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.4** **Federal Alert Gateway receives and validates message**
Preconditions	Governance • WEA Alert Aggregator has been established as a trusted provider for the Federal Alert Gateway Authorizations Technology
Actions	CAP format verified Alert logged Receipt notification sent to WEA Alert Aggregator
Postconditions	Notification sent to WEA Alert Aggregator Log updated
Claims	1. Received message is from a trusted and properly authorized source 2. Alert is properly logged 3. WEA Alert Aggregator is properly notified of message receipt
Failure outcomes	Message cannot be logged (Claim 2 error) Receipt notification to CMSP Alert Aggregator fails (Claim 3 error)

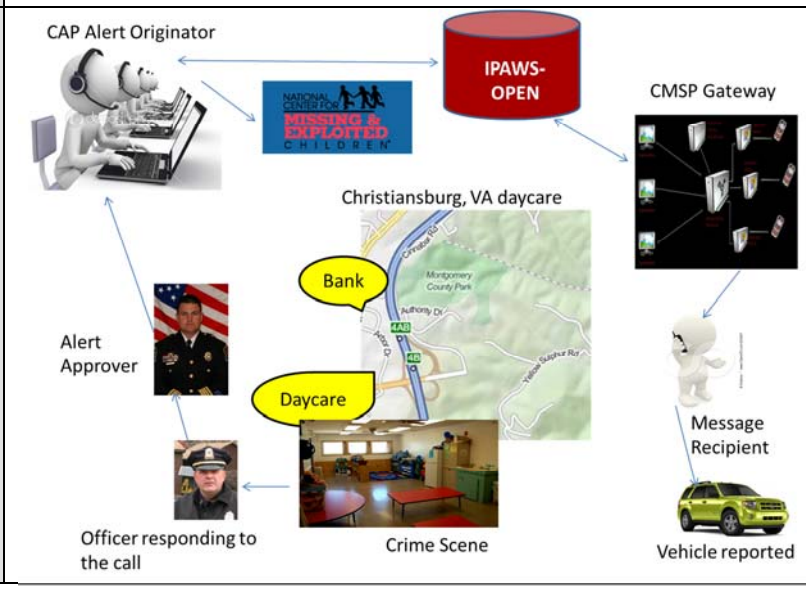
Potential causes of failure	Authorization errors (receipt delivery) • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity)
Issues	What is the value of the log at this point? Why are prior steps not logged? Is there any history of the IPAWS messages sent from unauthorized sources?

Philadelphia Subway Bombing (Presidential Alert)	**Mission Step 13.5** **Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways**
Preconditions	Governance • CMSP Gateways have been established as trusted recipients for the Federal Alert Gateway Authorizations • Mobile device service providers for the region to be notified have properly established authorization to receive CMSP messages Technology • Wireless distribution for CMSP is available for target area (How determined?) • CMSP Gateway access for the targeted area is available
Actions	CAP message converted to CMAC format Distribution targets identified and selected: match message distribution target to stored CMSP profiles coverage CMAC-formatted alert broadcasted to selected CMSP Gateway destinations
Postconditions	CMAC message broadcasted to selected CMSP Gateways
Claims	1. CAP message is properly converted to CMAC format 2. Targeted CMSP Gateways are appropriately selected 3. Message is broadcasted to selected CMSP Gateways
Failure outcomes	Message cannot be converted to CMAC format (Claim 1 error) Message broadcasted to wrong destination (Claim 2 error) Broadcast fails or is delayed (Claim 3 error)
Potential causes of failure	Authorization errors (broadcast delivery) • CMSP Gateways not properly established as valid recipients (availability) Missing results • CMSP connection fails (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity) • Error in mapping data to determine appropriate CMSP for target location (integrity)
Issues	Who is notified of a conversion or CMSP message notification failure? How will anyone know if the broadcast succeeded?

B.5 Mission Thread Analysis: AMBER Alert (Christiansburg Daycare Kidnapping)

B.5.1 AMBER Alert Operational Mission Thread

Name	Christiansburg Daycare Kidnapping (AMBER Alert)
Vignette (Summary Description)	A daycare on Arbor Road in Christiansburg, VA, has opened for child care and received 12 children ages 2–5 for the day. There are four staff members on duty, including the director. The staff and children are gathered in the playroom to start the daily program.
Nodes and Actors	Police deputy (alert identifier), police chief (alert approver), Christiansburg Police Department (CAP alert originator), IPAWS, mobile device service providers, users of WEA-capable mobile devices
Assumptions	• The daycare has the ability to enter missing child information into the National Crime Information Center (NCIC) system. All systems used by the National Center for Missing and Exploited Children (NCMEC) are available and operational. Once law enforcement has determined that the abducted child's case meets their local, regional, and statewide or territorial program's criteria, an AMBER alert is issued via IPAWS to EAS, radio, television, and the WEA service. • There is reasonable belief by law enforcement that an abduction has occurred. • The abduction is of a child age 17 or younger. • The law-enforcement agency believes that the child is in imminent danger of serious bodily injury or death. • There is enough descriptive information about the victim and abduction for law enforcement to issue an AMBER alert to assist in recovering the child. • The child's name and other critical data elements, including the Child Abduction flag, have been entered into the NCIC database available via the internet by NCMEC. • Law enforcement notifies NCMEC when an AMBER alert is released for a specific geographical area. Once NCMEC validates the AMBER alert, it is entered into a secure system and transmitted to authorized secondary distributors for dissemination to customers within the geographic areas specified. All systems used by NCMEC are available and operational. • The Christiansburg police have a central IPAWS entry capability at the police station. • All WEA functions are available and operational. • IPAWS consists of the IPAWS-OPEN Gateway, WEA Alert Aggregator, and Federal Alert Gateway. *Note: These are just example assumptions; there would likely be more.*

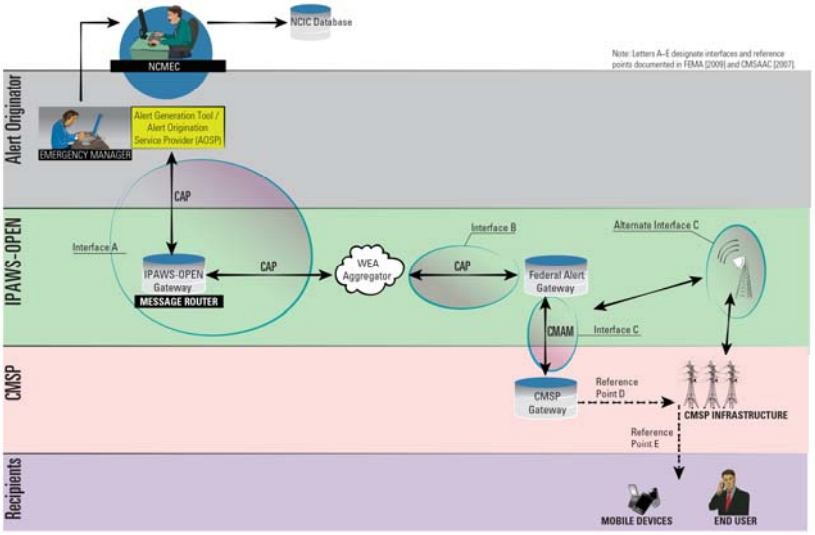
Name	Christiansburg Daycare Kidnapping (AMBER Alert)
Environmental Context Diagram	

Name		Christiansburg Daycare Kidnapping (AMBER Alert)
Mission Steps	**Time**	**Description**
1	7:00 a.m.	Two people wearing black masks force their way into the daycare at gunpoint. One is carrying a photo and matching it to the children as the staff rush to collect and protect them. They push staff and children into the playroom across from the front entrance, which has one door and windows at the back.
2	7:05	The person with the photo grabs four-year-old Nancy and carries her out the door while she kicks and screams. He climbs into the back of a green SUV parked at the front door. Another person is in the driver seat.
3	7:07	At the same time, the second gunman pulls over the toy cabinets and kicks tables to block in the daycare staff and children in the back of the playroom, runs out the door, and jumps onto the passenger side of the SUV as it backs out.
4	7:09	Staff looking out the back window see the SUV turn right out of the parking lot, head down Arbor Road, and turn left in the direction of U.S. 460. They think the SUV turns west on U.S. 460, but trees obscure a clear view.
5	7:09	Director pushes tables out of her way, heads into the office, and calls the police via 911.
6	7:12	Director collects available information for the police (photo, description). Nancy's parents are undergoing a highly contentious divorce. The courts had previously notified the daycare not to release the child to the father because of the risk of abuse.
7	7:18	Christiansburg Police Department deputy officer, who was at a bank just down the road from the daycare, picks up the call and rushes to the daycare.
8	7:22	Deputy officer takes the child's information from the director and calls in the report to the police chief that this case meets the criteria for issuing an AMBER alert.
9	7:27	Police chief agrees and authorizes deputy officer to submit an AMBER alert for Montgomery and Giles counties to cover the towns connected by U.S. 460.
10	7:32	Deputy officer uses his car's workstation to send the data required for the AMBER alert to the command center at the police station.

Name		Christiansburg Daycare Kidnapping (AMBER Alert)
Mission Steps	**Time**	**Description**
11	7:35	The command center officer on duty faxes the information to the NCMEC to have the missing child added to the NCIC database, logs on to the alert aggregator system, and copies the data sent by the deputy officer into the appropriate data fields to submit the CAP message to IPAWS.
12	7:40	IPAWS verifies the message, and the CAP message is sent to the WEA Alert Aggregator, which sends it to the Federal Alert Gateway, which in turn sends the WEA-formatted message to the CMSP Gateway.
13	7:50	The mobile device service providers receive the WEA message and then broadcast the message to mobile devices in the selected counties.
14	8:00	A message recipient seated at a Burger King near U.S. 460 sees a vehicle that fits the description of the van headed west on U.S. 460 and calls the police to report the vehicle location.
15	8:30	Police set up a roadblock at the Montgomery County line. As the van approaches, it does a U-turn and heads in the opposite direction. The police give chase and apprehend the vehicle, arresting the three men (the child's father is driving) and recovering the child, who is scared but uninjured.

B.5.2 AMBER Alert Mission Step Decomposition – Security

Mission Thread Analysis Name	Christiansburg Daycare Kidnapping (AMBER Alert) – Security
Scope of Analysis	A daycare on Arbor Road in Christiansburg, VA, has opened for child care and received 12 children ages 2–5 for the day. There are four staff on duty, including the director. The staff and children are gathered in the playroom to start the daily program. Two gunmen burst into the building, snatch a child, and leave in a green SUV headed toward U.S. 460. Police arrive, collect data about the child, and issue an AMBER alert via the WEA service. Information about the vehicle is reported from a message recipient, the abductors are captured, and the child is recovered unharmed.
Nodes and Actors	Police deputy (alert identifier), police chief (alert approver), Christiansburg Police Department (CAP alert originator), IPAWS, mobile device service providers, users of WEA-capable mobile devices
Characteristic Analyzed	System quality attribute: Security
Assumptions	• Law enforcement notifies the NCMEC when an AMBER alert is released for a specific geographical area. Once NCMEC validates the AMBER alert, it is entered into a secure system and transmitted to authorized secondary distributors for dissemination to customers within the geographic areas specified. • All systems used by NCMEC are available and operational. • The Christiansburg police have a central IPAWS entry capability at the police station. • All WEA functions are available and operational. • IPAWS consists of the IPAWS-OPEN Gateway, WEA Alert Aggregator, and Federal Alert Gateway. *Note: These are example assumptions only; there would likely be more.*

Mission Thread Analysis Name	Christiansburg Daycare Kidnapping (AMBER Alert) – Security
Systems Context Diagram	

Description and Decomposition of Mission Steps Relevant to Security Christiansburg Daycare Kidnapping (AMBER Alert)				
Mission Step	**Time**	**Mission Step Description**	**Analysis Substep**	**Substep Description**
11	7:35	The command center officer on duty faxes the information to the NCMEC to have the missing child added to the NCIC database, logs on to the alert aggregator system, and copies the data sent by the deputy officer into the appropriate data fields to submit the CAP message to IPAWS.	11	
12	7:40	IPAWS verifies the message, and the CAP message is sent to the WEA Alert Aggregator, which sends it to the Federal Alert Gateway, which in turn sends the WEA-formatted message to the CMSP Gateway.	12.1	IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator.
			12.2	Message is processed by WEA Alert Aggregator.
			12.3	WEA Alert Aggregator sends validated message to Federal Alert Gateway.
			12.4	Federal Alert Gateway receives and validates message.
			12.5	Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways.

Description and Decomposition of Mission Steps Relevant to Security Christiansburg Daycare Kidnapping (AMBER Alert)				
13	7:50	The mobile device service providers receive the WEA message and then broadcast the message to mobile devices in the selected counties.	13.1	CMSP Gateways receive message from Federal Alert Gateway.
			13.2	CMSPs broadcast to customers.

B.5.3 AMBER Alert Mission Thread Analysis – Security

This section contains example mission thread analyses for Mission Steps 11 and 12, including the substeps for Step 12 (it was not necessary to decompose Step 11).

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 11** **The command center officer on duty faxes the information to NCMEC to have the missing child added to the NCIC database, logs on to the alert aggregator system, and copies the data sent by the deputy officer into the appropriate data fields to submit the CAP message to IPAWS**
Preconditions	Policy Governance • AMBER alert has been declared for two counties by the Christiansburg, VA, police chief • Approval to send an alert and warning message to mobile devices in the area has been given • Wireless distribution for CMSP is available to subscribers for target area and message type (How determined?) Authorizations • Alert originator has access to a secure, approved submission device • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated on the WEA service; notification is received from IPAWS system operator People skills • Alert originator is trained on AOSP and WEA Technology • Submission capability for wireless alert is available; functionality will depend on originator capabilities (Is this the same as for EAS messages?) • IPAWS-OPEN Gateway access is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?) • Alert originator has access to equipment able to generate message
Actions	Message entered in AOSP system Message designated for Philadelphia region appropriate to subway usage CAP format message generated Message format validated locally? Message sent from AOSP to IPAWS-OPEN Gateway
Postconditions	Message in CAP format submitted to IPAWS

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 11** **The command center officer on duty faxes the information to NCMEC to have the missing child added to the NCIC database, logs on to the alert aggregator system, and copies the data sent by the deputy officer into the appropriate data fields to submit the CAP message to IPAWS**
Claims	1. Originator has received appropriate approval to generate message 2. Originator is approved for IPAWS alert generation 3. System used to generate and send alert is available and functions as intended 4. Platform used to generate and send alert is not compromised 5. Connection used to send alert is available and functions as intended
Failure outcomes	Missing or delayed results: • Message submission fails or is delayed (Claim 4 error) Message content error: • Message not in CAP format (Claim 3 error) • Output is not what was approved (Claim 1 error) • Proper credentials not submitted with message (Claim 2 and 3 errors) • Message is corrupted in transmission (Claim 5 error)
Potential causes of failure	Missing or delayed results • Message entry platform is compromised and send instruction is suppressed (integrity) • Authentication actions failed (availability) • WEA Alert Aggregator connection fails (availability) • Message is queued due to line congestion (availability) Message content error • Software supporting alert operator generates invalid format (integrity) • Send action does not complete (availability) • Platform for message sending is compromised and application has been tampered with (integrity) • Connection with IPAWS fails or is corrupted (availability or integrity)
Issues	What are minimum and expected requirements for submission of alerts to WEA Alert Aggregator? Will a user interface be provided for direct submission to IPAWS or application programming interface for automated send from originator system? How will connection be verified as trusted in addition to the actual originating individual? What are options for originator if IPAWS-OPEN Gateway is not available? Will this depend on originator capability? Will there be a “standard” operation with capability for more advanced sites to automate additional capabilities?

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.1** **IPAWS-OPEN Gateway verifies and routes message to WEA Alert Aggregator**
Preconditions	Governance • Approval to send to IPAWS-OPEN Gateway has been established (Will this entry point reject senders? Will sender be notified?) Authorizations • Alert originator has established appropriate approvals for entry of alerts more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated for the IPAWS-OPEN Gateway Technology • Wireless message packet arrives for IPAWS (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?)
Actions	Alert is validated and authenticated Error message is returned to originating government entity if needed and mission thread is terminated Converted message is sent to WEA Alert Aggregator
Postconditions	CAP alert message routed to WEA Alert Aggregator
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid 4. Received message is in proper CAP format 5. WEA Alert Aggregator connection is available
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Message cannot be converted (Claim 4 error) Missing or delayed CAP message from originator (Claim 1 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • IPAWS-OPEN Gateway fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to IPAWS does not include an acknowledgment to the originator [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Will there be capability to automatically wait and retry if WEA Alert Aggregator is unavailable?

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.2** **Message is processed by WEA Alert Aggregator**
Preconditions	Governance • Approval to send a wireless alert and warning message from IPAWS-OPEN Gateway to the WEA Alert Aggregator has been established (How is trust relationship established?) Authorizations • Alert originator has established appropriate approvals for entry of a WEA message more than 30 days prior; valid certificate is available and stored on selected device • Approvals for alert originator have been activated for the WEA Alert Aggregator system • WEA Alert Aggregator is staffed with appropriately authenticated operators Technology • Wireless message packet arrives for the WEA Alert Aggregator (What is detection mechanism?) • Alert originator is identifiable from message • Alert Distribution Network access to WEA Alert Aggregator is available (How determined?) • Wireless distribution for CMSP is available to subscribers for target area (How determined?)
Actions	Alert is validated and authenticated Error message is returned to originating government entity if needed and mission thread is terminated
Postconditions	CAP message processed by WEA Alert Aggregator
Claims	1. Message is properly received 2. Received message is from an authenticated source 3. Received message structure is valid
Failure outcomes	Message originator not authorized (Claim 2 error) Message fails formatting validation (Claim 3 error) Missing or delayed CAP message from originator (Claim 1 error)
Potential causes of failure	Authorization errors • Alert originator not properly established as valid source (availability) • Alert originator information corrupted in transmission (integrity) Missing results • Connectivity to alert originator fails (availability) • Message from originator is queued due to line congestion (availability) • WEA Alert Aggregator fails due to a software or hardware problem (availability) Wrong message sent • Prioritization error causes wrong message to be sent (integrity) • Other application error triggers wrong message (integrity)
Issues	Text submission to the WEA service does not include an acknowledgment to the originator [CMSAAC 2007, pp. 27–29]. How does originator confirm alert has been properly sent? Is there any history of the IPAWS-OPEN Aggregator being spoofed?

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.3** **WEA Alert Aggregator sends updated message to Federal Alert Gateway**
Preconditions	Governance Authorizations Technology • Federal Alert Gateway is available (How determined?)
Actions	CAP alert message sent to Federal Alert Gateway
Postconditions	CAP message transferred to Federal Alert Gateway
Claims	1. Received message is from a trusted and properly authorized source
Failure outcomes	Message originator not a trusted source (Claim 1 error) Message fails validation (Claim 1 error)
Potential causes of failure	Authorization errors • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt, message) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • WEA Alert Aggregator connection fails (availability)
Issues	The architecture document does not include specifics about the Federal Alert Gateway, and the concept of operations does not include error message handing [FEMA 2009]. It appears that error messages only return to the prior step, so how will the originator be made aware of errors that occur beyond the IPAWS-OPEN Gateway? Will there be capability to wait and retry if Federal Alert Gateway availability fails?

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.4** **Federal Alert Gateway receives and validates message**
Preconditions	Governance • WEA Alert Aggregator has been established as a trusted provider for the Federal Alert Gateway Authorizations Technology
Actions	CAP format verified Alert logged Receipt notification sent to WEA Alert Aggregator
Postconditions	Notification sent to WEA Alert Aggregator Log updated
Claims	1. Received message is from a trusted and properly authorized source 2. Alert is properly logged 3. WEA Alert Aggregator is properly notified of message receipt
Failure outcomes	Message cannot be logged (Claim 2 error) Receipt notification to CMSP Alert Aggregator fails (Claim 3 error)

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.4** **Federal Alert Gateway receives and validates message**
Potential causes of failure	Authorization errors (receipt delivery) • Aggregator not properly established as valid source (availability) • Aggregator information corrupted in transmission (integrity) Missing results (log, receipt) • Connectivity to aggregator fails (availability) • Message from aggregator is queued due to line congestion (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity)
Issues	What is the value of the log at this point? Why are prior steps not logged? Is there any history of the IPAWS messages sent from unauthorized sources?

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.5** **Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways**
Preconditions	Governance • CMSP Gateways have been established as trusted recipients for the Federal Alert Gateway Authorizations • Mobile device service providers for the region to be notified have properly established authorization to receive CMSP messages Technology • Wireless distribution for CMSP is available for target area (How determined?) • CMSP Gateway access for the targeted area is available
Actions	CAP message converted to CMAC format Distribution targets identified and selected: match message distribution target to stored CMSP profiles coverage CMAC-formatted alert broadcasted to selected CMSP Gateway destinations
Postconditions	CMAC message broadcasted to selected CMSP Gateways
Claims	1. CAP message is properly converted to CMAC format 2. Targeted CMSP Gateways are appropriately selected 3. Message is broadcasted to selected CMSP Gateways
Failure outcomes	Message cannot be converted to CMAC format (Claim 1 error) Message broadcasted to wrong destination (Claim 2 error) Broadcast fails or is delayed (Claim 3 error)
Potential causes of failure	Authorization errors (broadcast delivery) • CMSP Gateways not properly established as valid recipients (availability) Missing results • CMSP connection fails (availability) • Log write fails (availability) Message to wrong location • Error in originator message defining target location (integrity) • Error in translation of message corrupting target location (integrity) • Error in mapping data to determine appropriate CMSP for target location (integrity)

Christiansburg Day-care Kidnapping (AMBER Alert)	**Mission Step 12.5** **Federal Alert Gateway converts CAP message to CMAC and sends translated CMAC-formatted message to appropriate CMSP Gateways**
Issues	Who is notified of a conversion or CMSP message notification failure? How will anyone know if the broadcast succeeded?

Appendix C CWE/SANS Software Weakness Examples

This appendix provides definitions of selected examples from the *CWE/SANS Top 25 Most Dangerous Software Errors*, a list of the most common software weaknesses that can lead to exploitable security vulnerabilities [SANS 2011]. CWE stands for "common weakness enumeration." This list is produced through collaboration between the SANS Institute, MITRE, and top software security experts and is regularly updated. Another list, the CVE, identifies vulnerabilities related to weaknesses specific to the operating system in the CWE list. See the SANS Institute website for more information [SANS 2011].

In this appendix, we provide examples of weaknesses from the CWE/SANS list that we used to identify potential vulnerabilities during our STRIDE analysis (summarized in Table 5). The Example Vulnerabilities column in Table 5 provides information that the AOSP should consider during design, development, and operations of systems that the alert originator uses to interface with IPAWS. The three high-level categories within the *CWE/SANS Top 25* are

- Insecure Interaction Between Components: weaknesses related to insecure transmission or receipt of data between separate assets of the system, where assets can be technology items, people, processes, or facilities
- Risky Resource Management: weaknesses related to improper management and use of key system resources, for example, code and data
- Porous Defenses: weaknesses related to improper use of, or failure to use, defensive techniques

Table 23 provides examples of weaknesses in each category along with an explanation of how attackers can exploit each weakness.

Table 23: Examples of Common Software Weaknesses

Category [SANS 2011]	Example	Explanation
Insecure Interaction Between Components		
	Audit files not well protected	Audit files contain information about the state of the system and the user logged on to the system. If these files are not encrypted, then an attacker can potentially perform identity spoofing or gain access to the internals of the software.
	URL redirection to untrusted site	A user clicks a button or link expecting to go to one place, but the user is actually redirected to a malicious site. The malicious site can run malicious scripts, download viruses, or conduct a phishing attack.
	Cross-site request forgery	An attacker tricks a user into sending a request to a site by having him or her click a false button or link (such as in an ad). This request appears to have come from a legitimate user, but the information from the request goes to the attacker.
	Origin validation error	If the software does not properly verify that the source of data is legitimate, then the user could be communicating with an attacker or malicious site instead.

Category [SANS 2011]	Example	Explanation
	Direct requests	If an attacker knows how a site formats its URL strings for any given page, then the attacker can send a direct request to the website. If the website assumes that only people who have logged in can submit that specific URL and thus doesn't check authentication, then the attacker has free run of the site.
Porous Defenses		
	Missing encryption of sensitive data	If sensitive data is not encrypted, then an attacker monitoring traffic on the web can see a user's credentials and steal them. Similarly, if sensitive information is stored locally and not encrypted, then an attacker can take a copy on a flash drive and read it later.
	Reliance on untrusted inputs	A site might require that a digital signature exist to prove the identity of the person trying to connect; however, if the site doesn't check that the digital signature is from a reputable source, then the validity of the digital signature is uncertain.
	Improper restriction of excessive authentication attempts	If there is no lockout after a certain number of failed attempts to log on, then an attacker can use a brute-force method to guess a user's password and gain access.
	Authorization bypass through user-controlled key	In some sites, once a user successfully logs in, he or she is given a key value that then identifies that user for the remainder of that logged-in session. If the user is not careful, then an attacker can take or guess that key and gain access to the user's information.
	Hard-coded credentials	If information about a user's credentials or the password or key used to encrypt files or transmissions is hard coded into the software, then an attacker can easily look at the source code and get the information. The attacker can then decrypt all messages and files, possibly even decrypting a table of usernames and passwords for all users.
	Use of a broken or risky cryptographic algorithm	The strongest cryptographic algorithms are those that are completely known to the public and have stood the test of time. If software is using a nonstandard, known, flawed cryptographic algorithm, then it is very likely that an attacker can break the algorithm and gain access to sensitive information.
Risky Resource Management		
	Inclusion of functionality from untrusted control sphere	Software might provide a function that is implemented by a third party. Even though the software that a user is specifically working with is completely secure, if it is sending sensitive information to the third party for some reason, then there is a possibility that the data could be compromised.
	Uncontrolled format string	It is important that two parts of a system communicate in a very exact and expected way. It is possible for a user to type in a string that is sufficiently long and formatted in a certain way that it will cause the software to perform undefined behavior or even execute malicious code that was included in the string.

Appendix D Cybersecurity Risk Analysis Methodology

During the acquisition and development of software-reliant systems, program personnel normally focus on meeting functional requirements, often deferring security to later life-cycle activities. In fact, security features are usually addressed during system operation and sustainment rather than engineered into a system. As a result, many organizations deploy software-reliant systems with significant residual security risk, putting their associated operational missions in jeopardy.

Operational security vulnerabilities have three main causes: (1) design problems, (2) implementation or coding problems, and (3) system configuration problems. The cybersecurity risk analysis (CSRA) method focuses primarily on analyzing design vulnerabilities that cannot be corrected easily during operations. Early detection and remediation of design vulnerabilities will help reduce residual security risk when a system is deployed.

However, performing a risk analysis early in the life cycle does not guarantee that an organization or a system will handle security risks effectively. Many traditional security risk-analysis methods cannot handle the inherent complexity of modern cybersecurity attacks. These methods are based on a simple, linear view of risk that assumes a single threat actor exploits a single vulnerability in a single system to cause an adverse consequence. In reality, multiple actors exploit multiple vulnerabilities in multiple systems as part of a complex chain of events. Traditional methods are often unable to analyze complex cybersecurity attacks effectively.

The CSRA method is designed for use during early life-cycle activities (e.g., during requirements, architecture, and design). The CSRA method employs scenario-based risk analysis to handle the complex nature of cybersecurity risk. The goal is to identify design vulnerabilities early in the life cycle and enable program personnel to take corrective action. In this way, the organization can mitigate a subset of critical operational security risks long before it deploys a system.

The CSRA method is derived from two risk methods previously developed by the SEI. The first is Continuous Risk Management, which focuses on early life-cycle management of programmatic risks by acquisition and development programs. The second method is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) method, which is designed for the operations and sustainment phases of the software life cycle. OCTAVE enables an organization to assess operational information-security risks to its most critical assets. Both methods have had a considerable impact on risk management practice throughout the software engineering and cybersecurity communities.[21]

In this appendix, we present the CSRA method and show how we used it to analyze cybersecurity risks for the WEA service. We start by defining key risk management terms and concepts in Section D.1. The information presented in Section D.1 provides the conceptual foundation for the CSRA method. Next, in Section D.2, we describe the core tasks to perform when conducting the method. Here, we provide details for each CSRA task, along with selected examples. Finally, in

[21] According to a 2002 survey by the Cutter Consortium, 21% of respondents indicated that they followed SEI's risk methods when managing their programmatic risks. This was second to the ISO risk management standard. An article in the March 2006 edition of *Computerworld* magazine stated that the success of OCTAVE has made the SEI "the closest thing to a leader" in the field of security risk assessment.

Section D.3 we present detailed information for the four risks that we analyzed for the WEA service.

D.1 Risk Management Terms and Concepts

The term *risk* is used universally, but different audiences attach different meanings to it [Kloman 1990]. In fact, the details about risk and how it supports decision making depend on the context in which it is applied [Charette 1990]. For example, safety professionals view risk management in terms of reducing the number of accidents and injuries. A hospital administrator views risk management as part of the organization's quality assurance program, while the insurance industry relies on risk management techniques when setting insurance rates. Each industry thus uses a definition that is tailored to its context. No universally accepted definition of risk exists.

Whereas specific definitions of risk might vary, a few characteristics are common to all definitions. For risk to exist in any circumstance, the following three conditions must be satisfied [Charette 1990]:

1. The potential for loss must exist.
2. Uncertainty with respect to the eventual outcome must be present.[22]
3. Some choice or decision is required to deal with the uncertainty and potential for loss.

The three characteristics can be used to forge a basic definition of risk. Most definitions focus on the first two conditions—loss and uncertainty—because they are the two measurable aspects of risk. Thus, the essence of risk, no matter what the domain, can be succinctly captured by the following definition: *Risk is the probability of suffering harm or loss* [derived from Dorofee 1996].

D.1.1 Cybersecurity Risk

Cybersecurity risk is a measure of the likelihood that a threat will exploit one or more vulnerabilities to produce to an adverse consequence, or loss, coupled with the magnitude of the loss. Figure 14 illustrates the three core components of cybersecurity risk:

- *threat* – a cyber-based act, occurrence, or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss
- *vulnerability* – a weakness in an information system, system security procedures, internal controls, or implementation that a threat could exploit to produce an adverse consequence or loss; a current condition that leads to or enables cybersecurity risk
- *consequence* – the loss that results when a threat exploits one or more vulnerabilities; the loss is measured in relation to the status quo (i.e., current state)

From the cybersecurity perspective, a vulnerability is the passive element of risk. It exposes cyber-technologies (e.g., software application, software-reliant system) to threats and the losses that those threats can produce. However, by itself, a vulnerability will not cause an entity to suffer a loss or experience an adverse consequence; rather, the vulnerability makes the entity susceptible to the effects of a threat [adapted from Alberts 2006].

[22] Some researchers separate the concepts of certainty (the absence of doubt), risk (where the probabilities of alternative outcomes are known), and uncertainty (where the probabilities of possible outcomes are unknown). However, because uncertainty is a fundamental attribute of risk, this report does not differentiate between decision making under risk and decision making under uncertainty.

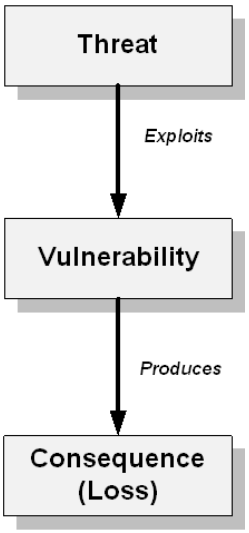


Figure 14: Components of Cybersecurity Risk

Consider the following example of a cybersecurity risk. An organization has acquired and deployed an AOS and has sent several WEA messages to its constituency. However, the system has a significant vulnerability—it has not implemented strong security controls[23] to protect the certificate it uses to send WEA messages. For example,

- access to certificates is not monitored
- encryption controls are not used for certificates during transit and storage
- access to certificates is not limited based on role

If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location (threat), then health, safety, legal, financial, and reputation consequences could result (consequence or loss). In this scenario, the health and safety of people are put in jeopardy due to the malicious action of an individual.

However, if no one attempts to exploit the vulnerabilities and carry out the attack, then no adverse consequences will occur. The vulnerabilities (i.e., poor protection of certificates) lie dormant until a threat actor (i.e., an outside attacker) attempts to exploit them to produce an adverse consequence or loss.

D.1.2 Risk Measures

In general, three measures are associated with any risk: (1) probability, (2) impact, and (3) risk exposure.[24] *Probability* a measure of the likelihood that the risk will occur, and *impact* is a measure of the loss that occurs when a risk is realized. *Risk exposure* provides a measure of the magnitude of a risk based on current values of probability and impact.

---

[23] A *control* is a procedure, policy, or countermeasure that provides a reasonable assurance that technology operates as intended, that data are reliable, and that the organization is in compliance with applicable laws and regulations.

[24] A fourth measure, *time frame*, is sometimes used to measure the length of time before a risk is realized or the length of time in which action can be taken to prevent a risk.

D.1.3 Risk Management

Risk management is a systematic approach for minimizing exposure to potential losses. It provides a disciplined environment for

- continuously assessing what could go wrong (i.e., assessing risks)
- determining which risks to address (i.e., setting mitigation priorities)
- implementing actions to address high-priority risks and bring those risks within tolerance

Figure 15 illustrates the three core risk management activities:

- *assess risk* – Transform the concerns people have into distinct, tangible cybersecurity risks that are explicitly documented and analyzed.
- *plan for controlling risk* – Determine an approach for addressing each cybersecurity risk; produce a plan for implementing the approach.
- *control risk* – Deal with each cybersecurity risk by implementing its defined control plan and tracking the plan to completion.

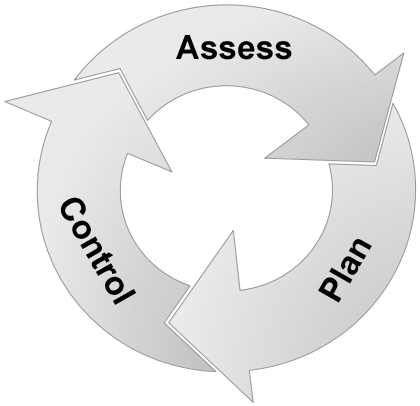


Figure 15: Risk Management Activities

D.1.4 Controlling Cybersecurity Risks

The strategy for controlling a risk is based on the measures for the risk (i.e., probability, impact, and risk exposure), which are established during the risk assessment. Decision-making criteria (e.g., for prioritizing risks or deciding when to escalate risks within an organization) may also be used to help determine the appropriate strategy for controlling a risk. Common control approaches include

- *accept* – If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented.
- *transfer* – A risk is shifted to another party (e.g., through insurance or outsourcing).
- *avoid* – Activities are restructured to eliminate the possibility of a risk occurring.
- *mitigate* – Actions are implemented in an attempt to reduce or contain a risk.

For any cybersecurity risk that is not accepted, the security analyst should develop and document a control plan for that risk. A control plan defines a set of actions for implementing the selected

control approach. For risks that are being mitigated, their plans can include actions from the following categories:

- *monitor and respond* – Monitor the threat and take action when it is detected.
- *protect* – Implement protection measures to reduce vulnerability to the threat and to minimize any consequences that might occur.
- *recover* – Recover from the risk if the consequences or losses are realized.

The risk management concepts presented in this appendix form the basis for the CSRA method that we used to identify and analyze cybersecurity risks to alert originators for the WEA service. The next section provides a detailed description of the CSRA method.

D.2 CSRA Method Description

In this section, we describe the CSRA method by defining the core tasks to perform when conducting the method. The CSRA method is composed of the five tasks described in Table 24.

Table 24: Tasks of the Cybersecurity Risk Analysis

Task	Description
1. Establish operational context.	• Determine the target of the assessment (e.g., the software application or system that is being assessed) first. • Characterize the operational environment for the target of the assessment to establish baseline operational performance. • Analyze cybersecurity risks in relation to this baseline.

2. Identify risk.	• Transform cybersecurity concerns into distinct, tangible risk scenarios that can be described and measured.
	• Document the following elements for each cybersecurity risk:
	  • risk statement
	  • threat
	  • consequence
	  • enablers

3. Analyze risk.	Evaluate each risk in relation to predefined criteria to determine its • probability • impact • risk exposure
4. Determine control approach.	Determine and document a strategy for controlling each risk based on predefined criteria and current constraints (e.g., resources and funding available for control activities). Control approaches for cybersecurity risks include • accept • transfer • avoid • mitigate
5. Develop control plan.	Define and document a control plan for all cybersecurity risks that are not accepted (i.e., risks that will be mitigated or transferred). Risk-mitigation plans typically include actions from the following categories: • monitor and respond • protect • recover

We provide details for each CSRA task, along with selected examples. The examples are not meant to be all-inclusive; rather, we offer them to assist the reader in understanding what a particular task accomplishes.

The CSRA method can be self-applied by the person or group that is responsible for acquiring and developing a software-reliant system or conducted by external parties on behalf of the responsible person or group. We present this section from the perspective of using an external party to conduct the CSRA method. A small team of approximately three to five people, called the *Analysis Team*, is responsible for applying the CSRA method and reporting findings to stakeholders. The Analysis Team typically includes the following people:

- *Analysis Team leader* – one person familiar with the CSRA method who leads the execution of all method tasks
- *Analysis Team members* – two to four people with subject-matter expertise relevant to completing CSRA tasks. Analysis Team members generally include
  - one to two people who are familiar with the target of the analysis and how it functions within its operational environment
  - one to two people who have procedural and technical cybersecurity expertise

Most CSRA tasks are completed in workshop settings, although the Analysis Team leader will complete a few tasks alone, as noted. The Analysis Team leader facilitates each workshop, while Analysis Team members act as participants (i.e., subject-matter experts). Additional people with specific knowledge and expertise relevant to a workshop's activities can be included in the workshop as appropriate. The remainder of this subsection provides the guidelines for conducting the CSRA method, beginning with establishing the operation context for the analysis.

D.2.1 Establish Operational Context (Task 1)

In Task 1, the Analysis Team defines the operational context for the analysis. First, they identify the target of the analysis. The target is typically the software application or system that is the focus of the CSRA. In the next step, they determine how the target supports operations (or is projected to support operations, if the target is not yet deployed).

Each software application or system typically supports multiple operational workflows or mission threads during operations. The goal is to (1) select which operational workflow or mission thread the team will include in the analysis and (2) document how the target of the analysis supports the selected workflow or mission thread. This establishes a baseline of operational performance for the target. The team will then analyze cybersecurity risks in relation to this baseline.

The Analysis Team will complete the following steps during Task 1:

- Establish target of the CSRA (Step 1.1).
- Select workflow and mission thread (Step 1.2).
- Define workflow and mission thread (Step 1.3).
- Document workflow and mission thread (Step 1.4).

Task 1 typically requires two separate sessions, each with a different set of participants. The first session is a meeting with the stakeholders who are sponsoring the CSRA. These stakeholders are usually funding the effort and will define the target of the analysis. The Analysis Team leader

facilitates the meeting with the stakeholders. Analysts Team members generally observe; however, they can participate in the meeting as needed. Step 1.1 is completed during this first meeting with stakeholders.

The second session is a workshop. The Analysis Team leader facilitates the workshop. Analysis Team members act as participants (i.e., subject-matter experts) in the workshop. Additional people who are familiar with the target of the analysis and the workflows or mission threads it supports (i.e., additional subject-matter experts) can be included in the workshop as appropriate. Steps 1.2 and 1.3 are completed during the workshop.

Finally, the Analysis Team leader documents the output in Step 1.4 after the workshop. Guidelines and examples for each step of Task 1 are provided in this subsection.

D.2.1.1 Establish Target of the Cybersecurity Risk Analysis (Step 1.1)

The CSRA method begins by establishing the target of the analysis. Ask participants to focus on the goals of the assessment. Next, ask participants to consider the following question: What technology or system is the focus of the analysis?

Participants might not agree initially on the target of the analysis. Discuss the range of answers provided by the participants. Discuss any discrepancies in their answers. The purpose of the discussion is to help the group reach consensus on the technology (e.g., software application, system) that will be the focus of the analysis. This can take time. Once participants reach consensus, document the target of the analysis on a flip chart for all to see.

Example: The Analysis Team leader facilitates a meeting with the stakeholders who are sponsoring the CSRA. The stakeholders include several senior managers from an alert originator whose organization is acquiring an AOS from a vendor. The group quickly comes to a consensus that the AOS is the target of the analysis.

D.2.1.2 Select Workflow and Mission Thread (Step 1.2)

Ask participants to focus on the target of the analysis and how it supports the operational mission. Next, ask participants to consider the following question: Which workflows or mission threads does the target support?

Document the scenarios on a flip chart for all to see. After the brainstorming of related workflows or mission threads is complete, ask participants to consider the following question: Which workflow or mission thread will be included in the CSRA?

Discuss the range of answers provided by the participants. The purpose of the discussion is to help the group reach consensus on the workflow or mission thread that will provide the operational context for the analysis. This can take time. Once participants reach consensus, document the target of the analysis on a flip chart for all to see.

Example: The Analysis Team leader facilitates a workshop with the Analysis Team and a few additional people from the alert-originating organization who have knowledge of the operational environment in which the AOS will be deployed. The workshop participants quickly come to a consensus that the WEA pipeline used to distribute emergency alerts to wireless devices provides

the overarching context for the CSRA. They also decide that the operational focus for the CSRA will be the alert-originating organization's portion of the WEA pipeline.

D.2.1.3 Define Workflow and Mission Thread (Step 1.3)

The mission and objective(s) of a workflow or mission thread are used to define the operational boundaries of the CSRA. All activities performed in pursuit of the mission and objective(s) are included in the analysis. Here, *mission* is defined as the fundamental purpose of the system that is being examined. An *objective* is defined as a tangible outcome or result that must be achieved when pursuing a mission.

Ask participants to consider the following question: What are the mission and objective(s) of the workflow or mission thread? Discuss the range of answers provided by the participants. The purpose of the discussion is to help the group reach consensus on the mission and objective(s) of the workflow or mission thread. This can take time. Once participants reach consensus, document the mission and objective(s) on a flip chart for all to see.

Once the Analysis Team has identified the mission and objective(s), they will characterize all activities performed in pursuit of the mission and objective(s) to provide a benchmark of operational performance. At a minimum, the team should identify the following performance parameters for the workflow or mission thread being analyzed:

- the sequence and timing of all steps needed to achieve the mission and objective(s), including relevant interrelationships and dependencies among the activities
- roles and responsibilities for completing each step
- technologies (e.g., systems, applications, software, hardware) supporting each step

Ask the participants to consider the following questions:

- What steps are required to complete the workflow or mission thread?
- Who or what (e.g., person, technology) performs each step in the workflow or mission thread?
- What technologies (e.g., systems, applications, software, hardware) support each step in the workflow or mission thread?
- How does the target of the analysis support the workflow or mission thread?
- How does the target of the analysis interface with other technologies?
- What is the flow of data in relation to the target of the analysis?

The Analysis Team can document the workflow or mission thread in several different ways. Two common ways are the diagramming technique (e.g., process flow, swim-lane diagram) and the spreadsheet format. Document the workflow or mission thread using the format (i.e., diagram, spreadsheet, other) preferred by the stakeholders of the analysis.

It is important to note that developing a workflow or mission thread is normally an iterative process. The workshop might require several meetings. After each meeting, the Analysis Team leader can document the results so the team can use them as the basis for beginning the next meeting.

Example: The Analysis Team leader facilitates a workshop with the Analysis Team members and a few additional people from the alert-originating organization who have knowledge of the opera-

tional environment. The participants identify the following mission and objective for the WEA mission thread:

- *Mission* – CMSPs use the WEA pipeline to distribute emergency alerts to mobile phone carriers.
- *Objective* – Alert originators enter a legitimate CAP-compliant alert message into the AOS and transmit it to IPAWS accurately, in a timely manner, and within the constraints of their MOA with FEMA.

Over the course of several sessions, the Analysis Team and the additional operational experts define a mission thread for the mission and objective that they documented. The final mission thread is documented in Table 25.

Table 25: Mission Thread for Alert-Originating Organization

Step	Supporting Technologies
AOS operator attempts to log on to the AOS.	• Server (valid accounts and authentication information) • Logon application • Communications between logon software, server, and AOS
AOS logon activates auditing of the operator's session.	• Auditing application • Communications from accounts to auditing application • Local or remote storage devices
AOS operator enters alert, cancel, or update message with status of "actual."	• Alert scripts • GUI application • Communications between GUI application and alert-generation software (including server and application)
AOS converts message to CAP-compliant format.	• Conversion application
CAP-compliant message is signed by two people.	• Signature entry application • Signature validation application • Public–private key pair for every user
AOS transmits message to the IPAWS-OPEN Gateway.	• Application that securely connects to IPAWS • AOS and IPAWS

D.2.1.4 Document Workflow and Mission Thread (Step 1.4)

Transcribe and document the workflow or mission thread produced during the workshop. The Analysis Team leader (or someone designated by the Analysis Team leader) typically performs the final step of Task 1 alone. However, he or she can consult others when transcribing information to ensure the accuracy of documented data (e.g., clarifying the steps in the mission thread).

D.2.2 Identify Risk (Task 2)

Task 2 focuses on risk identification. Here, the Analysis Team transforms a cybersecurity concern into a distinct, tangible risk scenario that they can describe and measure. The team completes the following steps during Task 2:

- Review operational context (Step 2.1).
- Identify threat (Step 2.2).
- Establish consequence (Step 2.3).

- Identify enablers (Step 2.4).
- Document risk data (Step 2.5).

Task 2 is performed in a workshop setting. Prior to the workshop, Analysis Team members (including the leader) complete Step 2.1 individually as they prepare for the workshop and complete Steps 2.2 through 2.4 during the workshop. The Analysis Team leader facilitates the workshop. Analysis Team members act as participants (i.e., subject-matter experts) in the workshop. Additional people with specific knowledge and expertise relevant to the workshop's activities can be included in the workshop as appropriate. The Analysis Team leader documents the output in Step 2.5 after the workshop.

Guidelines and examples for each step of Task 2 are provided in this subsection.

D.2.2.1 Review Operational Context (Step 2.1)

Ask participants to review the operational context that was generated in Task 1. Make sure that they look at the following items:

- mission and objective(s) of the workflow or mission thread
- steps required to complete the workflow or mission thread
- technologies (e.g., systems, applications, software, hardware) that support the workflow or mission thread
- how the target of the analysis supports the workflow or mission thread
- how the target of the analysis interfaces with other technologies
- the flow of data in relation to the target of the analysis

After participants have reviewed the operational context, move to Step 2.2.

D.2.2.2 Identify Threat (Step 2.2)

Threat identification begins with brainstorming a range of potential threats. Ask participants to focus on the target of the analysis and how it supports the operational mission. Next, ask participants to consider the following question: What scenarios would put the target at risk?

The question is designed to elicit a range of potential threats to the target. To focus the brainstorming activity, have participants consider the following types of scenarios:[25]

- The actor poses as another actor or entity.
- Information or code is modified.
- Sensitive or proprietary information is viewed by the actor or other individuals.
- Access to important information or services is interrupted, temporarily unavailable, or unusable.
- Information is destroyed or lost.
- The actor (human) denies having performed an action that other parties can neither confirm nor contradict.

[25] The actions listed are adapted from the STRIDE method for identifying threats. STRIDE was described in Section 4 of this report.

- The actor gains system access and privileges that he or she is not supposed to have.

Consider using the following questions to refine the participants' scenarios:

- Who or what is the source of the risk?
- How is the target affected?

Document the scenarios on a flip chart for all to see. After the brainstorming is complete, select a scenario for further analysis. Document the selected scenario into a properly worded threat statement, making sure to address the key components of a threat: actor, motive (if applicable), and action. Each threat component is described below, beginning with actor.

The first component of threat, actor, is the source of the threat. It describes who or what causes the threat. Examples of typical actors for cybersecurity threats include

- *outsider* – a person with an outsider's knowledge of the organization
- *insider* – a person with an insider's knowledge of the organization
- *malicious code* – code that is intended to cause undesired effects, security breaches, or damage to a system (e.g., scripts, viruses, worms, Trojan horses, backdoors, and malicious active content)

Motive is the second component of a threat. It defines the reason why the actor attempts to carry out the threat. Examples of motive include

- *intentional or malicious* – a person intentionally tries to cause the action
- *accidental* – a person inadvertently causes the action to occur

In general, motive applies only to human actors. If the Analysis Team selects malicious code (or some other type of non-human actor) as the actor, do not address motive.

The final component of threat, action, describes what the actor does to place the target at risk. The essence of the action should already be documented as part of each scenario that the team identified during the brainstorming activity.

After the three components of a threat are documented, take one of the following actions:

- Select another scenario to develop into a threat statement.
- Conclude Step 2.2 and begin Step 2.3 (establish consequence).

Example: The Analysis Team leader facilitates a brainstorming session with the team members. They identify several threat scenarios during the session. The leader records each scenario on a flip chart for all team members to see. The group then selects one scenario to analyze further and develops the following threat statement: An outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location.

The example threat statement includes the following components of threat:

- *actor* – a person with an outsider's knowledge of the organization
- *motive* – malicious intent
- *action* – the actor obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location

After the Analysis Team documents the threat statements, they need to examine the potential consequences of each threat. This occurs in Step 2.3 of the CSRA method.

D.2.2.3 Establish Consequence (Step 2.3)

Step 2.3 builds on threat identification by examining the potential consequences of each threat. Select a threat on which to focus. Ask participants to consider the following question: If the threat occurs, what impacts might ensue?

The question is designed to elicit a range of potential consequences triggered by the occurrence of the threat. To focus the brainstorming of consequences, have participants consider the following types of potential impacts:

- health and safety issues
- financial losses
- productivity losses
- loss of reputation

Document the consequences on a flip chart for all to see. After the Analysis Team has documented the consequences for the threat, take one of the following actions:

- Select another threat.
- Conclude Step 2.3 and begin Step 2.4 (identify enablers).

Example: The Analysis Team leader selects the following threat for team members to consider: An outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location. The team identifies the following consequences for the threat:

- People could be put in harm's way, resulting in injuries and death.
- Alert originators and state approvers could be held liable for damages.
- The reputation of WEA could be damaged.
- The reputations of alert originators could be damaged.
- Future attacks could become more likely (i.e., copycat attacks).

The leader records the consequences on a flip chart for all team members to see. After consequences are documented for all threats, two of the three components of risk have been established (threat and consequence). In Step 2.4, the Analysis Team identifies and documents the final component of risk—enablers.

D.2.2.4 Identify Enablers (Step 2.4)

Step 2.4 focuses on identifying conditions or circumstances that allow the risk to occur. These conditions or circumstances are referred to collectively as *enablers* and can include vulnerabilities, occurrence of related risks, actions that people might take, and dependencies on related technologies and data.

Select a threat–consequence pair on which to focus. Ask participants to consider the following question: What conditions or circumstances could enable the risk to occur?

To focus the brainstorming activity, have participants consider the following types of enablers:

- organization, policy, or procedure weaknesses
- technical weaknesses or vulnerabilities
- actions of organizations staff (e.g., IT staff, users)
- actions of collaborators or partners
- interfaces of systems
- data flows
- software or system design

Document the enablers on a flip chart for all to see. After the Analysis Team has documented the enablers for the risk, take one of the following actions:

- Select another threat–consequence pair.
- Conclude Step 2.4 and begin Step 2.5 (document risk data).

Example: The Analysis Team leader selects the following threat–consequence pair for the team to consider:

- Threat: An outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location.
- Consequences:
  - People could be put in harm's way, resulting in injuries and death.
  - Alert originators and state approvers could be held liable for damages.
  - The reputation of WEA could be damaged.
  - The reputations of alert originators could be damaged.
  - Future attacks could become more likely (i.e., copycat attacks).

Team members identify the following enablers for the threat:

- An attacker could capture a valid certificate.
  - Certificates are sent to recipients in encrypted email. This email is replicated in many locations, including
    - computers of recipients
    - email servers
    - email server and recipient computer backups
    - off-site storage of backup tapes
  - The attacker could compromise the EOC or vendor to gain access to the certificate (e.g., through social engineering).
  - Limited control over the distribution and use of certificates could enable an attacker to obtain access to a certificate.
- Unencrypted certificates could be stored on recipient's systems.
- Management of certificates is performed manually.
- An EOC's certificate would provide an attacker with access to all IPAWS capabilities.
- The knowledge of what constitutes a CAP-compliant message is publicly documented.

- The number of vendors that provide AOS software is small. Each vendor controls a large number of certificates. A compromised vendor could provide an attacker with many potential targets.

The leader records the enablers on a flip chart for all participants to see. After the Analysis Team has documented enablers for all risks, risk identification is almost complete. The final step is to formally document the risk data.

D.2.2.5 Document Risk Data (Step 2.5)

Transcribe and document the final results of the session (i.e., threats, consequences, and enablers). The Analysis Team leader (or someone designated by the Analysis Team leader) typically performs the final step of Task 2 alone. However, he or she can consult others when transcribing information to ensure the accuracy of documented data.

The Analysis Team leader will document a risk statement for each risk. A risk statement is a succinct and specific description of a risk. Risk statements typically describe (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence). The if-then format is often used to capture a risk. The *if* part of the statement describes the threat, while the *then* part summarizes the consequences.

Example: After the workshop, the Analysis Team leader documents the risk data captured during the facilitated session. For the first risk, the leader records the following risk statement: *If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.*

D.2.3 Analyze Risk (Task 3)

Task 3 focuses on risk analysis. During this task, the Analysis Team evaluates each risk in relation to predefined criteria to determine its probability, impact, and risk exposure. The team completes following steps during Task 3:

- Review data (Step 3.1).
- Establish probability (Step 3.2).
- Establish impact (Step 3.3).
- Determine risk exposure (Step 3.4).
- Document risk data (Step 3.5).

Task 3 is performed in a workshop setting. Prior to the workshop, Analysis Team members (including the leader) complete Step 3.1 individually as they prepare for the workshop and complete Steps 3.2 through 3.4 during the workshop. The Analysis Team leader facilitates the workshop. Analysis Team members act as participants (i.e., subject-matter experts) in the workshop. Additional people with specific knowledge and expertise relevant to the workshop's activities can be included in the workshop as appropriate. The Analysis Team leader documents the output in Step 3.5 after the workshop.

Guidelines and examples for each step of Task 3 are provided in this subsection.

D.2.3.1 Review Data (Step 3.1)

Ask participants to review the operational context that was generated in Task 1. Make sure that they look at the following items:

- mission and objective(s) of the workflow or mission thread
- steps required to complete the workflow or mission thread
- technologies (e.g., systems, applications, software, hardware) that support the workflow or mission thread
- how the target of the analysis supports the workflow or mission thread
- how the target of the analysis interfaces with other technologies
- the flow of data in relation to the target of the analysis

Next, ask participants to review the following risk data that were generated during Task 2:

- threat for each risk
- consequences of each risk
- enablers of each risk

After participants have reviewed the operational context and risk data, move to Step 3.2.

D.2.3.2 Establish Probability (Step 3.2)

Select a risk to analyze. Ask participants to consider the following questions:

- What is the probability that the risk will occur?
- What is the rationale for your estimate of the risk's probability?

Ask participants to consider the following before answering the questions:

- threat, consequence, and enablers for the risk
- probability criteria in Figure 16[26]

Value	Definition	Context/Guidelines/Examples
Frequent (5)	The scenario occurs on numerous occasions or in quick succession. It tends to occur quite often or at close intervals.	≥ one time per month (≥ 12 / year)
Likely (4)	The scenario occurs on multiple occasions. It tends to occur reasonably often, but not in quick succession or at close intervals.	
Occasional (3)	The scenario occurs from time to time. It tends to occur "once in a while."	~ one time per 6 months (~ 2 / year)
Remote (2)	The scenario can occur, but it is not likely to occur. It has "an outside chance" of occurring.	
Rare (1)	The scenario infrequently occurs and is considered to be uncommon or unusual. It is not frequently experienced.	≤ one time every 3 years (≤ .33 / year)

Figure 16: Probability Criteria

[26] Make sure that the probability criteria have been tailored appropriately to the decision-making needs of key stakeholders. Also, the Context/Guidelines/Examples column is based on duration. For some risks, occurrences per use may make more sense than occurrences per month.

Document the probability and rationale on a flip chart for all to see. After the Analysis Team has documented the probability and rationale for the risk, conclude Step 3.2 and begin Step 3.3 (establish impact).

Example: The Analysis Team leader selects the following risk for the team to consider: If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.

Team members then evaluate the risk's probability. The leader documents the probability and rationale on a flip chart for all to see:

Probability: Rare

Rationale:

- This risk requires that a complex sequence of events occurs.
- The attacker has to be highly motivated.
- An event that requires an alert to be issued must already be imminent. People will likely verify WEA messages through other channels. To make maximize the impact, the attacker will likely take advantage of an impending event.
- WEA will need to have an established track record of success for this risk to be realized. Otherwise, people might not be inclined to follow the instructions provided in the illegitimate CAP-compliant message.

D.2.3.3 Establish Impact (Step 3.3)

Ask participants to consider the following questions for the selected risk:

- If the risk were to occur, what would its impact be?
- What is the rationale for your estimate of the risk's impact?

Ask participants to consider the following before answering the questions:

- threat, consequence, and enablers for the risk
- operational context
- impact criteria in Figure 17[27]

[27] Make sure that the impact criteria have been tailored appropriately to the decision-making needs of key stakeholders.

Value	Definition
Maximum (5)	The impact on the organization is severe. Damages are extreme in nature. Mission failure has occurred. Stakeholders will lose confidence in the organization and its leadership. The organization either will not be able to recover from the situation, or recovery will require an extremely large investment of capital and resources. Either way, the future viability of the organization is in doubt.
High (4)	The impact on the organization is large. Significant problems and disruptions are experienced by the organization. As a result, the organization will not be able to achieve its current mission without a major re-planning effort. Stakeholders will lose some degree of confidence in the organization and its leadership. The organization will need to reach out to stakeholders aggressively to rebuild confidence. The organization should be able to recover from the situation in the long run. Recovery will require a significant investment of organizational capital and resources.
Medium (3)	The impact on the organization is moderate. Several problems and disruptions are experienced by the organization. As a result, the organization will not be able to achieve its current mission without some adjustments to its plans. The organization will need to work with stakeholders to ensure their continued support. Over time, the organization will be able to recover from the situation. Recovery will require a moderate investment of organizational capital and resources.
Low (2)	The impact on the organization is relatively small, but noticeable. Minor problems and disruptions are experienced by the organization. The organization will be able to recover from the situation and meet its mission. Recovery will require a small investment of organizational capital and resources.
Minimal (1)	The impact on the organization is negligible. Any damages can be accepted by the organization without affecting operations or the mission being pursued. No stakeholders will be affected. Any costs incurred by the organization will be incidental.

Figure 17: Impact Criteria

Document the impact and rationale on a flip chart for all to see. After the Analysis Team has documented the probability and rationale for the risk, conclude Step 3.3 and begin Step 3.4 (determine risk exposure).

Example: Analysis Team members evaluate impact for the selected risk. The leader documents the impact and rationale on a flip chart for all to see:

Impact: High-Maximum

Rationale:
- The impact will ultimately depend on the severity of the event that is about to occur.
- Health and safety damages could be severe, leading to potentially large legal liabilities.
- The reputation of WEA could be severely damaged beyond repair.

D.2.3.4 Determine Risk Exposure (Step 3.4)

Ask participants to consider the following question for the selected risk: Based on the estimated values of probability and impact, what is the resulting risk exposure?

Use the matrix shown in Figure 18[28] to determine the current value of risk exposure for the selected risk. Risk exposure is the cell at the intersection of the

- column representing the risk's estimated probability
- row representing the risk's estimated impact

[28] Make sure that the risk exposure matrix has been tailored appropriately to the decision-making needs of key stakeholders.

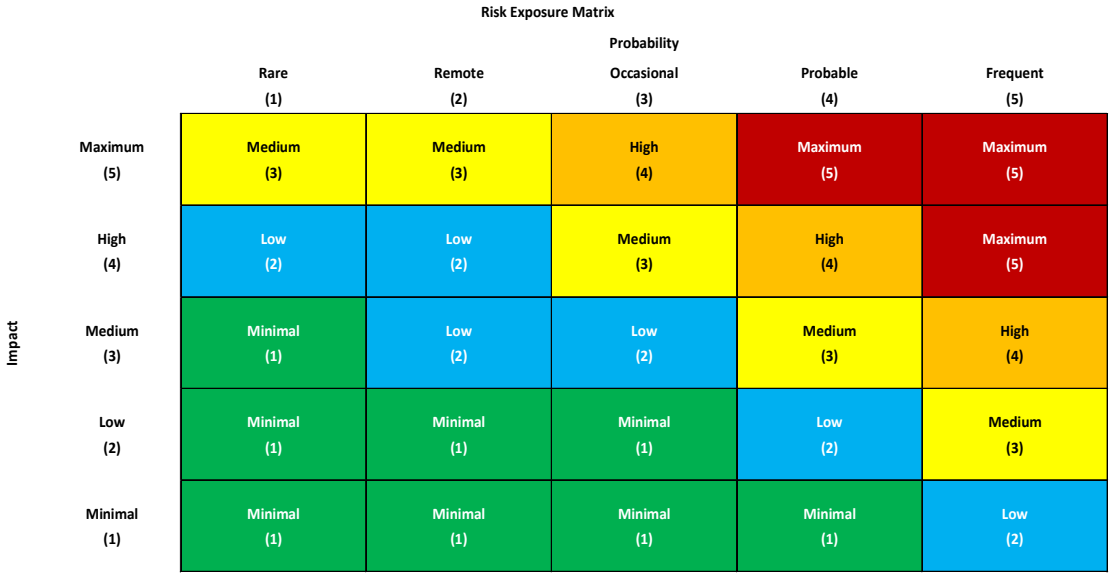


Figure 18: Risk Exposure Matrix

Document the risk exposure on a flip chart for all to see. After the Analysis Team has documented the risk exposure, take one of the following actions:

- Go back to Step 3.2 and analyze another risk.
- Conclude the risk analysis and begin Step 3.5 (document risk data).

Example: The Analysis Team leader determines risk exposure using the current values of probability and impact from the risk matrix. For the selected risk (i.e., the risk selected in Steps 3.1 and 3.2), the leader determined the probability to be rare. As shown in Figure 19, the leader locates the column corresponding to the probability value of *rare* in the matrix.

For the selected risk, the team members determined the impact to be between high and maximum. As shown in Figure 19, the leader locates the rows corresponding to the impact values of *high* and *maximum*. The intersection between the probability and impact values yields a risk exposure of *low-medium*.

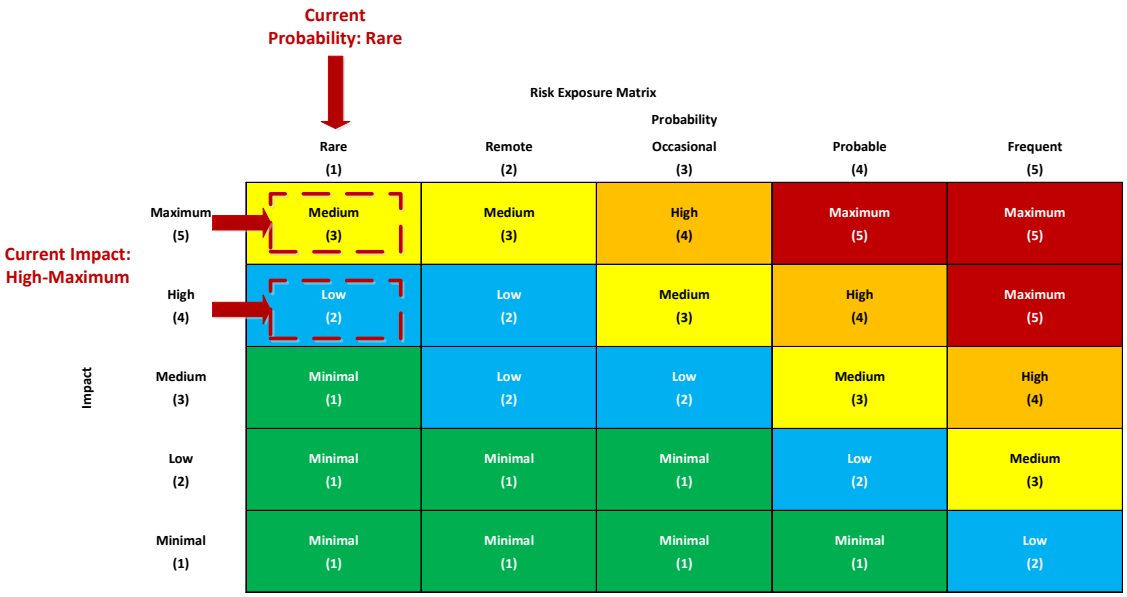


Figure 19: Risk Exposure Example

The leader documents the risk exposure on a flip chart for all to see.

D.2.3.5 Document Risk Data (Step 3.5)

The Analysis Team leader (or someone designated by the Analysis Team leader) typically performs the final step of Task 3 alone. However, he or she can consult others when transcribing information to ensure the accuracy of documented data (e.g., clarifying the rationale for an estimate of an impact value).

Transcribe and document the final results of the session, including the following data for each risk:

- probability and rationale
- impact and rationale
- risk exposure

Finally, consider developing a spreadsheet that provides a succinct summary of all relevant risk information. This type of summary, called a *risk profile*, will be useful in later CSRA tasks.

Example: After the workshop, the Analysis Team leader documents all data from the workshop. In addition, the leader creates a summary of the risk data in a spreadsheet format. The Analysis Team leader's initial risk spreadsheet is shown in Figure 20.

ID	Risk Statement	Impact	Prob	Risk Exp
1	If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.	High-Max	Rare	Low-Med
2	If malicious code prevents an operator from entering an alert into the Alert Originating System (AOS), then health, safety, legal, financial, and productivity consequences could result.	Low-Med	Remote	Min-Low
3	If an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message, then individual and organizational reputation consequences could result.	Med	Rare-Remote	Min-Low
4	If the internet communication channel for the AOS is unavailable due to a cybersecurity attack on the internet service provider, then health and safety consequences could result.	Low-Med	Remote	Min-Low

Figure 20: Example of Initial Risk Spreadsheet

The risk spreadsheet provides only a summary of the data generated for each risk. All of the detailed risk data should be recorded in a risk database or documented in a formal risk report. (The last section of this appendix provides detailed data for all four risks analyzed for the WEA service.)

D.2.4 Determine Control Approach (Task 4)

Task 4 focuses on establishing a control approach for each risk. During this task, the Analysis Team determines a strategy for controlling each risk and documents it as based on predefined criteria and current constraints (e.g., resources and funding available for control activities). The team completes the following steps during Task 4:

- Review data (Step 4.1).
- Prioritize risks (Step 4.2).
- Select control approach (Step 4.3).
- Document risk data (Step 4.4).

Task 4 is performed in a workshop setting. Prior to the workshop, Analysis Team members (including the leader) complete Step 4.1 individually as they prepare for the workshop and complete Steps 4.2 and 4.3 during the workshop. The Analysis Team leader facilitates the workshop. Analysis Team members act as participants (i.e., subject-matter experts) in the workshop. Additional people with specific knowledge and expertise relevant to the workshop's activities can be included in the workshop as appropriate. The Analysis Team leader documents the output in Step 4.4 after the workshop.

Guidelines and examples for each step of Task 4 are provided in this subsection.

D.2.4.1 Review Data (Step 4.1)

Ask participants to review the following data for each risk:

- risk statement
- threat
- consequence
- enablers
- probability and rationale
- impact and rationale
- risk exposure

Participants should also look at the risk spreadsheet that provides a summary, or snapshot, of all risks. After participants have reviewed risk data, move to Step 4.2.

D.2.4.2 Prioritize Risks (Step 4.2)

The Analysis Team leader can perform risk prioritization prior to the session. If risk priorities are established prior to the session, then team members can review the prioritized list of risks and make adjustments as appropriate.

Ask participants to consider the following question: Which risks are of highest priority? Ask participants to consider the following guidelines before prioritizing the list of risks:[29]

- Use impact as the primary factor for prioritizing cybersecurity risks. Risks with the largest impacts are deemed to be of highest priority.
- Use probability as the secondary factor for prioritizing cybersecurity risks. Probability is used to prioritize risks that have equal impacts. Risks of equal impact with the largest probabilities are considered to be the highest priority risks.

Document the prioritized list of risks for all to see. After the Analysis Team has prioritized and documented the risks, conclude Step 4.2 and begin Step 4.3 (select control approach).

Example: Before the session, the Analysis Team leader uses the prioritization guidelines and ranks the risks. The prioritized list of risks (in spreadsheet format) is shown in Figure 21.

[29] Make sure that the prioritization guidelines have been tailored appropriately to the decision-making needs of key stakeholders.

ID	Risk Statement	Impact	Prob	Risk Exp
1	If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.	High-Max	Rare	Low-Med
3	If an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message, then individual and organizational reputation consequences could result.	Med	Rare-Remote	Min-Low
2	If malicious code prevents an operator from entering an alert into the Alert Originating System (AOS), then health, safety, legal, financial, and productivity consequences could result.	Low-Med	Remote	Min-Low
4	If the internet communication channel for the AOS is unavailable due to a cybersecurity attack on the internet service provider, then health and safety consequences could result.	Low-Med	Remote	Min-Low

Figure 21: Prioritized Risk Spreadsheet

The Analysis Team leader shows the prioritized spreadsheet and guidelines to team members. The leader explains the method used to prioritize risks and asks if team members want to make any changes to the guidelines. The team members are satisfied with the list and accept the results.

D.2.4.3 Select Control Approach (Step 4.3)

Select a risk to analyze. Ask participants to consider the following questions:

- What approach will be used to control the risk?
- What is the rationale for choosing that approach?

Ask participants to consider the following options for controlling the risk:

- *accept* – If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented.
- *transfer* – A risk is shifted to another party (e.g., through insurance or outsourcing).
- *avoid* – Activities are restructured to eliminate the possibility of a risk occurring.
- *mitigate* – Actions are implemented in an attempt to reduce or contain a risk.

Document the control approach and rationale on a flip chart for all to see. After the Analysis Team has documented the probability and rationale for the risk, take one of the following actions:

- Select another risk.
- Conclude Step 4.3 and begin Step 4.4 (document risk data).

Example: The Analysis Team leader selects the following risk for team members to consider: If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.

Team members review the data for the selected risk and consider the four control approaches. They then pick a control approach for the risk. The leader documents the control approach and rationale on a flip chart for all to see:

Approach: Mitigate

Rationale:
- This risk could cause severe damages if it occurs, which makes it a good candidate for mitigation.
- Mitigations for this risk will be relatively cost effective.

D.2.4.4 Document Risk Data (Step 4.4)

Transcribe and document the results produced during the session (i.e., control approach and rationale for each risk). The Analysis Team leader (or someone designated by the Analysis Team leader) typically performs the final step of Task 4 alone. However, he or she can consult others when transcribing information to ensure the accuracy of documented data (e.g., clarifying the rationale for a risk's control approach). Finally, consider adding the control approach for each risk to the risk profile.

Example: After the workshop, the Analysis Team leader documents all data from the analysis session. In addition, the leader adds the control approach for each risk to the spreadsheet. The Analysis Team leader's updated risk spreadsheet is shown in Figure 22.

ID	Risk Statement	Impact	Prob	Risk Exp	Control Approach
1	If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.	High-Max	Rare	Low-Med	Mitigate
3	If an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message, then individual and organizational reputation consequences could result.	Med	Rare-Remote	Min-Low	Mitigate
2.	If malicious code prevents an operator from entering an alert into the Alert Originating System (AOS), then health, safety, legal, financial, and productivity consequences could result.	Low-Med	Remote	Min-Low	Mitigate
4	If the internet communication channel for the AOS is unavailable due to a cybersecurity attack on the internet service provider, then health and safety consequences could result.	Low-Med	Remote	Min-Low	Mitigate

Figure 22: Example of Updated Risk Spreadsheet

D.2.5 Determine Control Plan (Task 5)

Task 5 addresses control planning for each risk that has not been accepted (i.e., risks that will be mitigated, transferred, or accepted). The team completes the following steps during Task 5:

- Review data (Step 5.1).
- Establish control requirements (Step 5.2).
- Document risk data (Step 5.3).

Task 5 is performed in a workshop setting. Prior to the workshop, Analysis Team members (including the leader) complete Step 5.1 individually as they prepare for the workshop and complete Step 5.2 during the workshop. The Analysis Team leader facilitates the workshop. Analysis Team

members act as participants (i.e., subject-matter experts) in the workshop. Additional people with specific knowledge and expertise relevant to the workshop's activities can be included in the workshop as appropriate. The Analysis Team leader documents the output in Step 5.3 after the workshop.

Guidelines and examples for each step of Task 5 are provided in this subsection.

D.2.5.1 Review Data (Step 5.1)

Ask participants to review the operational context that was generated in Task 1. Make sure that they look at the following items:

- mission and objective(s) of the workflow or mission thread
- steps required to complete the workflow or mission thread
- technologies (e.g., systems, applications, software, hardware) that support the workflow or mission thread
- how the target of the analysis supports the workflow or mission thread
- how the target of the analysis interfaces with other technologies
- the flow of data in relation to the target of the analysis

Also ask participants to review the following data for each risk:

- threat, enablers, and consequences from Task 2
- impact and rationale, probability and rationale, and risk exposure from Task 3
- control approach and rationale from Task 4

Participants should also look at the risk spreadsheet that provides a summary, or snapshot, of all risks. After participants have reviewed risk data, move to Step 5.2.

D.2.5.2 Establish Control Requirements (Step 5.2)

Select a risk to analyze. Ask participants to consider the following questions based on the designated control approach for the risk:

- *Transfer*: What can be done to transfer the risk? How can the risk be shifted to another party?
- *Avoid*: What can be done to avoid the risk? How can activities be restructured to eliminate the possibility of the risk occurring?
- *Mitigate*: What can be done to mitigate the risk? Which actions can be implemented to reduce or contain the risk?
  - *Monitor and Respond*: What can be done to monitor and respond to the threat?
  - *Protect or Resist*: What can be done to protect against or resist the threat? What can be done to protect against or resist the consequence?
  - *Recover*: What can be done to recover from the risk when it occurs?

Note that *mitigate* has three sub-questions associated with it. Focus on answering the sub-questions when developing control plans for risks that are being mitigated.

Have the participants brainstorm answers to the appropriate questions for the risk being analyzed. Document each control action on a flip chart for all to see. Make sure to phrase each control action as a requirement. For risks that are being mitigated, make sure to note the category (i.e., monitor and respond, protect or resist, recover) for each control requirement that the team documents.

After the Analysis Team has documented control requirements for the risk, take one of the following actions:

- Select another risk.
- Conclude Step 5.2 and begin Step 5.3 (document risk data).

Example: The Analysis Team leader selects the following risk for team members to consider: If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result. The control approach for this risk is *mitigate*.

Team members review the data for the selected risk and consider mitigation actions for the risk. They brainstorm mitigation actions for each of the following categories: monitor and respond, protect or resist, and recover. The leader documents the control plan on a flip chart for all to see:

Monitor and Respond:

- IPAWS should send an alert receipt acknowledgment to an email address designated in the MOA with FEMA. (This approach uses an alternative communication mechanism from the sending channel.) The alert originator should monitor the IPAWS acknowledgments sent to the designated email address. The alert originator should send a cancellation for any false alerts that are issued.
- The alert originator should designate a representative for each distribution region to monitor for false alerts. The representative should have a handset capable of receiving alerts that are issued. If a false alert is issued, the designated representative would receive the alert and should then initiate the process for sending a cancellation for the false alert.

Protect:

- The AOS should use strong security controls to protect certificates.
  - Access to certificates should be monitored.
  - Encryption controls should be used for certificates during transit and storage.
  - Access to certificates should be limited based on role.
- All alert transactions should have controls (e.g., time stamp) to ensure that they cannot be rebroadcast at a later time. (Note: This requirement requires that the sender time stamps the alert appropriately. The receiver of the alert would need to check the time stamp to determine whether the alert is legitimate or a relay of a previous alert.)
- Certificates should expire and be replaced on a periodic basis.
- The alert originator should provide user training about security procedures and controls.

Recover:

- The alert originator should quickly issue a cancellation before people have a chance to respond to the false alert (i.e., before they have a chance to go to the dangerous location). This might require alert originators to provide additional training and to conduct additional operational exercises.
- The alert originator should notify FEMA to determine how to cancel the compromised certificate.

D.2.5.3 Document Risk Data (Step 5.3)

Transcribe and document the control plans produced during the session. The Analysis Team leader (or someone designated by the Analysis Team leader) typically performs the final step of Task 5 alone. However, he or she can consult others when transcribing information to ensure the accuracy of documented data (e.g., clarifying the intent of a control action identified during the session). Make sure that all control requirements are worded in accordance with organizational and industry guidelines for specifying software and system requirements.

D.3 Summary of Risk Information

This subsection documents the detailed information for each risk that was generated using the CERT CSRA method. For each risk, the Analysis Team captured the following data:

- *risk statement* – a succinct and specific description of a risk. A risk statement describes (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence).
- *threat* – a cyber-based act, occurrence, or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss
- *consequence* – the loss that results when a threat exploits one or more vulnerabilities
- *enablers* – current conditions, including vulnerabilities, that lead to or enable a cybersecurity risk
- *probability* – a measure of the likelihood that the risk will occur
- *impact* – a measure of the loss that occurs when a risk is realized
- *risk exposure* – a measure of the magnitude of a risk based on current values of probability and impact
- *control approach* – a strategy for addressing a risk. Examples of common control approaches include accept, transfer, avoid, and mitigate.
- *mitigation requirements* – a set of actions for reducing or containing a risk

The following four risks were analyzed using the CSRA method:

- Risk 1: Maliciously Sent CAP-Compliant Message
- Risk 2: Denial of Service from Malicious Code
- Risk 3: Insider Spoofing Colleague's Identity
- Risk 4: Unavailable Communication Channel

Detailed information for each risk is provided in the remainder of this subsection.

D.3.1 Risk 1: Maliciously Sent CAP-Compliant Message

D.3.1.1 Risk Statement

If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.

D.3.1.2 Threat

An outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that directs people to a dangerous location.

D.3.1.3 Consequence

As a result:

- People could be put in harm's way, resulting in injuries and death.
- Alert originators and state approvers could be held liable for damages.
- The reputation of WEA could be damaged.
- The reputations of alert originators could be damaged.
- Future attacks could become more likely (i.e., copycat attacks).

D.3.1.4 Enablers

A valid certificate could be captured by an attacker.

- Certificates are sent to recipients in encrypted email. This email is replicated in many locations, including
  - computers of recipients
  - email servers
  - email server and recipient computer backups
  - off-site storage of backup tapes
- The attacker could compromise the EOC or vendor to gain access to the certificate (e.g., through social engineering).
- Limited control over the distribution and use of certificates could enable an attacker to obtain access to a certificate.

Unencrypted certificates could be stored on recipient's systems.

Management of certificates is performed manually.

An EOC's certificate would provide an attacker with access to all IPAWS capabilities.

The knowledge of what constitutes a CAP-compliant message is publicly documented.

The number of vendors that provide AOS software is small. Each vendor controls a large number of certificates. A compromised vendor could provide an attacker with many potential targets.

D.3.1.5 Probability

Probability: Rare

Rationale:

- This risk requires that a complex sequence of events occurs.
- The attacker has to be highly motivated.
- An event that requires an alert to be issued must already be imminent. People will likely verify WEA messages through other channels. To make maximize the impact, the attacker will likely take advantage of an impending event.
- WEA will need to have an established track record of success for this risk to be realized. Otherwise, people might not be inclined to follow the instructions provided in the illegitimate CAP-compliant message.

D.3.1.6 Impact

Impact: High-Maximum

Rationale:

- The impact will ultimately depend on the severity of the event that is about to occur.
- Health and safety damages could be severe, leading to potentially large legal liabilities.
- The reputation of WEA could be severely damaged beyond repair.

D.3.1.7 Risk Exposure

Low-Medium

D.3.1.8 Control Approach

Approach: Mitigate

Rationale:

- This risk could cause severe damages if it occurs, which makes it a good candidate for mitigation.
- Mitigations for this risk will be relatively cost effective.

D.3.1.9 Mitigation Requirements

Monitor and Respond:

- IPAWS should send an alert receipt acknowledgment to an email address designated in the MOA with FEMA. (This approach uses an alternative communication mechanism from the sending channel.) The alert originator should monitor the IPAWS acknowledgments sent to the designated email address. The alert originator should send a cancellation for any false alerts that are issued.
- The alert originator should designate a representative for each distribution region to monitor for false alerts. The representative should have a handset capable of receiving alerts that are issued. If a false alert is issued, the designated representative would receive the alert and should then initiate the process for sending a cancellation for the false alert.

Protect:

- The AOS should use strong security controls to protect certificates.
  - Access to certificates should be monitored.
  - Encryption controls should be used for certificates during transit and storage.
  - Access to certificates should be limited based on role.
- All alert transactions should have controls (e.g., time stamp) to ensure that they cannot be rebroadcast at a later time. (Note: This requirement requires that the sender time stamps the alert appropriately. The receiver of the alert would need to check the time stamp to determine whether the alert is legitimate or a relay of a previous alert.)
- Certificates should expire and be replaced on a periodic basis.
- The alert originator should provide user training about security procedures and controls.

Recover:

- The alert originator should quickly issue a cancellation before people have a chance to respond to the false alert (i.e., before they have a chance to go to the dangerous location). This might require alert originators to provide additional training and to conduct additional operational exercises.
- The alert originator should notify FEMA to determine how to cancel the compromised certificate.

D.3.2 Risk 2: Denial of Service from Malicious Code

D.3.2.1 Risk Statement

If malicious code prevents an operator from entering an alert into the AOS, then health, safety, legal, financial, and productivity consequences could result.

D.3.2.2 Threat

Malicious code prevents an operator from entering an alert into the AOS.

D.3.2.3 Consequence

As a result:

- Dissemination of the alert could be delayed.
- The number of operators that can enter alerts could be restricted because the AOS is unavailable.
- The malicious code could be sent to IPAWS, affecting the availability of IPAWS.
- Public health and safety could be adversely affected because people do not receive alerts in a timely manner.
- Productivity at the alert-originating organization could be reduced during the attack.
- The alert-originating organization could incur substantial recovery costs.

D.3.2.4 Enablers

Removable media (e.g., USB drives, CDs) are compromised with malicious code. Staff members who use the compromised media infect systems in the alert-originating organization.

Physical security practices related to removable media are inadequate.

Staff members at the alert-originating organization access a compromised website.

Critical system resources are not properly managed ("risky resource management"), allowing malicious code to be downloaded.

The vendor's service could be compromised.

D.3.2.5 Probability

Probability: Remote, if certain precautions are taken

Rationale:

- The system is used actively only during an emergency, which is not a frequent occurrence.
- Malicious code attacks occur relatively often throughout the community. However, for the purpose of this analysis, we will assume that
  - vendors generally implement reasonable security precautions
  - use of an alert originator's equipment is limited to work-related activities
  - adequate security controls are generally implemented
  - security controls are enforced by the MOA with FEMA
- The probability could increase over time if organizations are not vigilant about maintaining an acceptable level of security.
  - Interviews with vendors have shown some evidence of the existence of security vulnerabilities.
  - Alert originators could be vulnerable to targeted attacks (e.g., spear phishing).

D.3.2.6 Impact

Impact: Low-Medium

Rationale:

- The extent of the impact will depend on the effectiveness of organization's contingency plans.
- Multiple channels exist for sending alerts. If the WEA service is unable to distribute alerts, many people will be able to receive them from other sources.
- Some number of people will not receive the alert if the WEA service is unable to distribute alerts

D.3.2.7 Risk Exposure

Minimal-Low

D.3.2.8 Control Approach

Approach: Mitigate

Rationale:

- Alert originators need to show due diligence that they are addressing the basic security challenges inherent in their environment. This risk represents a basic security challenge.
- This risk has the potential for a higher impact in the future as more people rely on the WEA service to receive alerts.

D.3.2.9 Mitigation Requirements

Monitor and Respond:

- The alert originator should monitor for security patches that can be applied to its AOS. The alert originator should apply security patches to the system as appropriate.
- The alert originator should run virus scans on its AOS periodically. The alert originator should respond to viruses found on its systems as appropriate.

Protect:

- The alert originator should employ virus protection for its AOS.
- The alert originator should control software upgrades to its AOS.
- The alert originator should control the use of external devices on its AOS.
- The alert originator should employ firewalls to control network traffic to and from the AOS.
- The alert originator should isolate alert-originating software from other applications (e.g., web browsers).
- The alert originator should use whitelisting practices to ensure that only approved software is installed.
- The alert originator should securely configure web browsers.
- The alert originator should ensure that warnings and alerts are enabled on web browsers.
- Where practical, the alert originator should limit browser usage.
- The alert originator should limit users' ability to download software.
- The alert originator should provide user training about security procedures and controls.
- The alert originator should establish an SLA with its vendors to ensure appropriate security controls and to establish penalties for noncompliance. (Note: Vendors should employ alternative or backup mechanisms for issuing alerts to ensure that they can meet the terms of their SLAs.)
- The alert originator should establish alternative mechanisms for issuing alerts in case its primary communications channels are unavailable.

Recover:

- The alert originator should establish procedures for recovering from malicious code attacks. Recovery procedures should address performing analysis activities (e.g., technical analysis, forensic analysis); responding appropriately to the attack (e.g., isolate affected machine, rebuild machine); implementing contingency plans; and notifying appropriate stakeholders.
- The alert originator should notify FEMA when a security incident occurs.
- The alert originator should update its security policies and procedures based on lessons learned from successful attacks.

D.3.3 Risk 3: Insider Spoofing Colleague's Identity

D.3.3.1 Risk Statement

If an insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message, then individual and organizational reputation consequences could result.

D.3.3.2 Threat

An insider with malicious intent spoofs the identity of a colleague and sends an illegitimate CAP-compliant message.

D.3.3.3 Consequence

As a result:

- The victim of the attack (i.e., the colleague) could be perceived as doing a poor job (i.e., sending out illegitimate messages to recipients).
- The victim of the attack could be required to spend time contacting recipients of the illegitimate message.
- The organization could initiate disciplinary actions against the victim of the attack for sending out illegitimate messages.
- Public perception of the alert originator could be damaged.

D.3.3.4 Enablers

Key loggers or packet sniffers are used to capture legitimate access information.

Lack of individualized authentication could enable the insider to spoof a colleague's identity.

Poor management of passwords (e.g., writing a password on a sticky note and putting it in a visible location) could enable an insider to gain unauthorized access to a colleague's account.

The insider could have physical access to the colleague's unlocked computer when the colleague is away from his or her desk.

Unprotected log files could allow the insider to tamper with the files and delete or modify entries.

The insider could use social engineering techniques to obtain authentication information from the vendor.

Authentication files could be inadequately protected in the vendor's software.

Limited control over the distribution and use of certificates could enable the insider to obtain access to a certificate.

An EOC's certificate would provide an attacker with access to all IPAWS capabilities.

D.3.3.5 Probability

Probability: Rare-Remote

Rationale:

- People who are given access to systems at sites normally go through a clearance process.
- This risk requires that a fairly complex sequence of events occurs.
- The insider has to be highly motivated to conduct this attack.
- Dual signatures are often required to send an alert. One person cannot send an alert by himself or herself. (This is a best practice.)

D.3.3.6 Impact

Impact: Medium

Rationale:

- The alerts being sent out in this attack are assumed to be relatively innocuous. These false alerts likely will not put the health or safety of people in jeopardy.
- Stakeholders' confidence in WEA could be significantly reduced.
- A moderate investment may be required to restore the reputation of WEA, including oversight and regular audits of the alert originator.

D.3.3.7 Risk Exposure

Minimal-Low

D.3.3.8 Control Approach

Approach: Mitigate

Rationale:

- The impact for this risk is high enough that it warrants mitigation.
- Organizational and individual liability issues make this risk important to mitigate.

D.3.3.9 Mitigation Requirements

Monitor and Respond:

- The alert originator should monitor the behavior of its employees for inappropriate actions.
- The alert originator should monitor physical and network access to the AOS.
- The alert originator should audit remote devices (e.g., laptops) for suspicious activity.
- The alert originator should perform periodic inventories of backup devices (e.g., backup computers and other equipment that can be deployed to other sites) to ensure that they are available for use and are not missing (i.e., not taken for inappropriate use).

Protect:

- The AOS should use strong authentication and authorization controls (e.g., multifactor authentication). Authentication should be unique to each individual.
- The alert originator should promptly address employee behavior problems.
- The alert originator should define and enforce an acceptable use policy for its systems and networks.
- The alert originator should implement a clearance process that requires periodic renewals.
- The alert originator should implement physical security controls that restrict access to devices.
- Authentication timeouts should be employed.
- Alert-originator staff should protect their passwords appropriately.
- Security awareness training should be provided to employees.
- The AOS should require dual signatures to issue an alert.
- The alert originator should provide user training about security procedures and controls.
- The alert originator should ensure that the vendor's software adequately protects authentication and authorization information.

Recover:

- The alert originator should quickly issue a cancellation before people have a chance to respond to the false alert. This might require alert originators to provide additional training and to conduct additional operational exercises.
- The alert originator should notify FEMA when a security incident occurs.
- The alert originator should conduct an investigation into the incident and respond appropriately.

D.3.4 Risk 4: Unavailable Communication Channel

D.3.4.1 Risk Statement

If the internet communication channel for the AOS is unavailable due to a cybersecurity attack on the ISP, then health and safety consequences could result.

D.3.4.2 Threat

The internet communication channel for the AOS is unavailable due to a cybersecurity attack on the ISP.

D.3.4.3 Consequence

As a result:

- Alert messages cannot be sent to IPAWS.
- Dissemination of the alert could be delayed.
- Recipients do not receive alert messages.

- Public health and safety could be adversely affected because people do not receive alerts in a timely manner.

D.3.4.4 Enablers

Pre-established, secure backup communication channels (e.g., satellite, direct communication) are inadequate or nonexistent.

D.3.4.5 Probability

Probability: Remote

Rationale:
- Internet unavailability due to cybersecurity attacks occur on occasion.
- Internet unavailability would have to coincide with an emergency situation that requires a WEA message to be issued. Emergency situations requiring alerts might occur only a handful of times per year.

D.3.4.6 Impact

Impact: Low-Medium

Rationale:
- The extent of the impact will depend on the effectiveness of organization's contingency plans.
- Multiple channels exist for sending alerts. If the WEA service is unable to distribute alerts, many people will be able to receive them from other sources.
- Some number of people will not receive the alert if the WEA service is unable to distribute alerts

D.3.4.7 Risk Exposure

Minimal-Low

D.3.4.8 Control Approach

Approach: Mitigate

Rationale:
- Alert originators need to show due diligence that they are addressing the basic security challenges inherent in their environment. This risk represents a basic security challenge.
- This risk has the potential for a higher impact in the future as more people rely on the WEA service to receive alerts.
- Alert originators are in the business of responding to emergencies—they should have contingency plans for their own organizations.

D.3.4.9 Mitigation Requirements

Monitor and Respond:

- The alert originator should establish and monitor a "heartbeat" mechanism to ensure that the communication channel is available. (Note: Because the system is not used continuously, alert originators need a mechanism that they can use to check for availability when the system is needed.)
- The alert originator should perform periodic dry runs of sending alerts under normal operating conditions. This will help ensure that people know how to send an alert under normal operating conditions. It will also help ensure that people understand what normal operating conditions look like. The alert originator should make sure that it conducts dry runs after the system is updated (e.g., patches applied).
- The alert originator should perform periodic dry runs of sending alerts under abnormal conditions, such as power failures. This will help ensure that people know how to send an alert under stress conditions.

Protect:

- The alert originator should identify external dependencies (e.g., power sources, communications channels) and establish mitigations for those dependencies.
- The alert originator should establish and test off-site capabilities for issuing alerts.
- The alert originator should establish and test alternative communications channels for issuing alerts.
- The alert originator should establish and test alternative EOCs that could be used to issue alerts, if needed.

Recover:

- The alert originator should establish procedures for recovering from an unavailable communication channel. Recovery procedures should address implementing contingency plans and notifying appropriate stakeholders.
- The alert originator should notify FEMA when a security incident occurs.
- The alert originator should update its security policies and procedures based on lessons learned from problems experienced with communications channels.

Appendix E Alert Originator Adoption, Operations, and Sustainment Decisions and Cybersecurity Risk

Throughout the WEA life cycle—in adoption, operations, and sustainment—the alert originator makes decisions that can affect both the level of operational cybersecurity risk and the degree of control that the alert originator has over risk mitigation. Examples of these decisions include the following:

Adoption

- Source of WEA capability (e.g., vendor or in-house development group)
- WEA capability hosting (e.g., on site, as a delivered application; off site, as a service; or remotely, at a facility operated by another organizational unit)
- Level of integration of WEA capability with other alert originator capabilities (e.g., standalone, shared user interface or other functionality with other alerting capabilities, or shared interface or other functionality with other emergency management capabilities)

Operations

- Allowable alert origination devices (e.g., desktop systems, laptops, or mobile devices)
- User IDs and privileges (limited privileges and access; broad privileges and access)
- Alert message signing (single or dual signature required for alerts)

Sustainment

- Applying software changes: from patches, to system software upgrades, to WEA capability enhancements (e.g., changes applied locally, as a service, or remotely; and robustness of testing before deployment)
- Maintaining equipment configuration (policies related to special circumstances for deviating from secure configurations)

This appendix describes these decisions, their impacts on cybersecurity risk, and approaches to risk mitigation.

E.1 Adoption Decisions and Cybersecurity Risk

Among the many decisions made during adoption, the alert originator chooses a source (supplier) for the WEA capability, determines where the capability will be hosted, and decides whether and how to integrate the WEA capability with other alerting and emergency management technologies. Each decision will affect the level of cybersecurity risk as described in this section.

Source of WEA Capability (Supplier). The alert originator's options in choosing a source, or supplier, for the WEA capability depend on many factors, for example, the alert originator's internal resources and its position within an enterprise that may control the selection of IT products and services. In general, adoption paths include

- in-house (alert-originating organization) development

- acquisition of custom application
- off-the-shelf purchase of application from a vendor
- contracting for a service from a vendor

The WEA capability development, acquisition, purchasing, or contracting activity may be directed by the alert originator end-user organization or by a higher level entity to which the alert originator belongs. For example, a state authority may select the WEA supplier for counties within its jurisdiction. Based on the information gathered through interviews with prospective alert originators, we expect most AOs to either purchase an application, contract for a service from a vendor, or use a capability selected by a higher level entity, although a few AOs will acquire a custom-built capability or develop one on their own [SEI 2013].

Regardless of the chosen path, the alert originator should choose a software developer that has executed an MOA with FEMA for system testing [FEMA 2012a]. This MOA includes a set of security requirements and rules of behavior for the developer. The alert originator should verify to the extent possible that the developer's solution meets these requirements. Also, for each path, the alert originator is responsible for developing and monitoring agreements regarding product and service security requirements and secure development practices. However, the level of insight and control over these items will vary depending on the chosen path.

In-house development generally offers more direct control over and insight into risk-mitigation actions. The alert originator should document and apply secure development practices. Experts within or hired by the alert originator should specify product security requirements. Resources for secure development include Allen, DHS, Howard, McGraw, OWASP, SAFECode, SANS, and Seacord [Allen 2008, DHS 2013, Howard 2006, McGraw 2012, OWASP 2013, SAFECode 2013, SANS 2011, Seacord 2013]. These requirements may specify the use of secure coding standards [Seacord 2013] and testing for, and removal of, certain common vulnerabilities [OWASP 2013, SANS 2011]. They may also specify the use of testing methods such as fuzz testing, penetration testing, or other techniques. Finally, they may include requirements for security features, such as requirements for strong passwords, encryption, dual signatures for alerting, role-based access controls and privileges, and multifactor authentication.

When acquiring a custom-built application, the alert originator can use contractual mechanisms to influence the security of the product. As with the in-house development path, the alert originator is responsible for specifying requirements for secure development practices (design, coding, and testing), as well as product security requirements, and for verifying that the developer meets these requirements. If the alert originator does not have the visibility or technical expertise to verify requirements, this represents an increased risk.

For off-the-shelf product purchases, the alert originator should inquire about the supplier's cybersecurity practices and how the supplier establishes and verifies product security requirements. Since the alert originator is not likely to have visibility or input into the product as it is developed, the alert originator should frame agreements so that the vendor is motivated to take cybersecurity risk seriously and is required to fully address any security issues discovered after delivery. While AOs may not be able to specify requirements up front, they can use a list of product security requirements and accepted secure development practices to evaluate and compare various off-the-

shelf products and suppliers. Appendix A, Section A.4.2, provides a starter set of questions for the alert originator to ask vendors.

Finally, for contracted services, in addition to the actions for off-the-shelf purchases, the alert originator should define the security requirements and practices for interfacing with the service provider's WEA capability. Once again, AOs can use a list of product security requirements and development practices to evaluate and compare WEA service providers.

For all four adoption paths, the developer or supplier will have some reliance on externally developed products, such as operating system software, device firmware, software library functions, and software development environments. These products are all part of the supply chain used to construct the WEA capability. It is not possible for the alert originator or the supplier to guarantee that all products in the supply chain will be free from defects and vulnerabilities, due to product complexity, interactions between products, lack of detailed insight into individual products, and the need to stay current with product updates. The objective is to ensure that the supplier is aware of the risks, uses reasonable practices to avoid products that carry greater risk, and works to mitigate the risk that supply-chain vulnerabilities will impact the WEA capability.

Finally, in all cases, tradeoffs exist between quality requirements. One frequently discussed tradeoff is that between security and usability requirements. AOs must be able to send an alert in an emergency without hindrance. Security is often perceived as interference. Yet it is critical to effective operations. Operational procedures and frequent training exercises can help ensure that the alert originator can quickly send alerts while adhering to good security practices.

WEA Capability Hosting. Another decision that affects cybersecurity involves where to host the WEA capability. This choice can affect the alert originator's control and influence over sustainment actions and possibly availability. The basic options include

- on-site hosting of the WEA capability
- enterprise-level hosting of the WEA capability (e.g., a county EOC uses a state-hosted application)
- third-party service-provider hosting of the WEA capability

There are some advantages to off-site hosting. If the alert originator facility itself is affected by an incident and the WEA capability is hosted on site, the alert originator would need to activate a backup mechanism to generate alerts. Off-site hosting, appropriately implemented, would facilitate transmission of alerts in such situations, provided the incident does not also affect the off-site location.

Wherever the capability is hosted, the alert originator should take measures to ensure that the AOS and its interface with IPAWS are protected from cyber threats. For on-site hosting, such measures might include blocking general public internet access and prohibiting the use of removable media on equipment that hosts the WEA capability. For both on-site and off-site hosting, the alert originator and service provider must implement access controls per the MOA with FEMA, including using discrete login accounts for all operators, complying with requirements for strong passwords, and ensuring that digital certificates are securely managed.

Level of Integration of WEA Capability with Other Capabilities. The decision to integrate WEA capabilities with other capabilities, often made to enhance usability, can affect cybersecurity. Choices range from no integration to a very high level of integration, as follows:

- stand-alone WEA capability with its own user interface
- separate WEA capability that is accessed via a user interface shared with other capabilities
- WEA capability that is integrated with other alerting capabilities such that one-time entry of alert information may generate both WEA messages and other types of alerts
- WEA capability that is integrated with other emergency management functions

With a stand-alone capability, risks generally relate to the WEA capability and its interfaces with system and networking software. Changes to the WEA capability or any of the components it interfaces with can change the level of risk. For a separate WEA capability accessed via a common user interface, the interface with the common user interface introduces another area of risk. The interface should be designed such that data is not shared with other applications and such that other applications cannot interfere with the WEA capability. Validation of information passed to and from the WEA capability is an essential risk mitigator. These cautions and recommendations extend to the final two cases, in which the WEA capability is integrated with other alerting or emergency management functions. Additionally, maintenance and upgrade actions for these other functions can affect the security of the WEA capability.

E.2 Operations Decisions and Cybersecurity Risks

Decisions related to operations may also affect cybersecurity risk. While AOs will make some of these decisions during the adoption phase, they implement those decisions during operations, and operations may require changes. Such decisions include

- allowable alert origination devices
- operational system user IDs and access privileges
- alert message signing

Allowable Alert Origination Devices. Given today's available and emerging communications technologies, WEA alert originators seek flexible options for generating alert messages, which may include

- fixed workstations located in EOCs
- hardened, portable devices stored in a kit and taken from the EOC in the event of an evacuation
- mobile devices such as smartphones and tablets

If the alert originator will use mobile devices, the MOA with FEMA states that they must be officially issued through or approved by DHS, FEMA, or approved emergency management organizations [FEMA 2012a]. These devices must be configured to lock after a specified period of inactivity. Finally, sensitive information stored, processed, or transmitted to and from wireless devices must be encrypted.

With the increase in bring-your-own-device (BYOD) policies, AOs may begin to inquire about whether they can configure their own devices to generate alerts. At this time, the MOA with FEMA does not permit the use of personal devices. BYOD policies best serve noncritical func-

tions. The ease of breaking into and gathering information from personally owned and maintained mobile devices makes their use for critical functions highly risky.

Operational System User IDs and Privileges. Some of the individuals we interviewed explained that their policy is to have one logon ID per shift, shared by all individuals on that shift. This violates the security quality of nonrepudiation (this means a user cannot claim that he or she did not send a message that he or she did in fact send). The MOA with FEMA includes rules of behavior stating that all users must have discrete user accounts that cannot be shared [FEMA 2012a]. It is also important to enable only the privileges needed by each user. In our interviews, at least one organization grants all user accounts full administrative privileges. This is a high-risk practice. Even if a single individual is responsible for both operator and system administrator roles, the individual should use separate accounts for the separate roles, one with operator privileges and the other with system administrator privileges.

Alert Message Signing. WEA allows alert messages to be sent with only one operator signing the message. However, as mentioned in Section 4.2.1, it is a best practice to have WEA messages signed by two operators with distinct user IDs, which reduces the risk of insider threat as well as the risk of sending an erroneous message.

E.3 Sustainment Decisions and Cybersecurity Risks

AOs make many decisions in the sustainment phase, and these decisions can have a major impact on operations in general as well as on cybersecurity risk specifically. Two of these decisions include the following:

- when and how to apply software changes (patches, upgrades, and enhancements)
- how to maintain equipment configuration

Applying Software Changes. From patches, to system software upgrades, to WEA capability enhancements, software changes are necessary for a variety of reasons. For example, AOs may need to apply security patches and fix defects to ensure correct and secure operations. They may need to upgrade system software (e.g., operating system software), either to correct a problem or to provide new features and compatibility with new technologies. Finally, the alert originator may wish to install enhanced WEA capability software.

In each of these cases, the choice of when and how to apply a change is critical. First, the sustainment staff evaluate the likely impacts of the change, an activity that can be quite complex. The staff should have some degree of assurance that security requirements will be upheld and that the changes will not insert vulnerabilities. If changes do insert vulnerabilities, the staff should be prepared to monitor and respond to them. If possible, the sustainment organization should have a test environment that enables them to execute and evaluate the new software in an environment nearly identical to but isolated from the operational environment. Unless the software change is critical, the alert originator should defer installation if a known pending or current event, such as a storm watch or warning, may require an alert.

Maintaining Equipment Configuration. AOs make many configuration choices during sustainment activities. Even if policies specify certain configurations, in times of stress or equipment failure, these policies may be violated. Some simple equipment configuration policies that protect against cybersecurity threats include not connecting alerting workstations to the public internet,

prohibiting removable media (e.g., USB drives), and ensuring that users change networking device passwords from manufacturer settings to complex passwords. If AOs make exceptions to these policies, they should document a written justification along with a process and timeline for reverting to the secure configuration.

Appendix F Cybersecurity Tasks for WEA Adoption

Section 6.2, Table 1Table 17, presented an overview of the five steps in the generic adoption thread. This appendix describes the cybersecurity tasks for alert originators, for each of the five steps, in detail:

1. Identify requirements and prepare for acquisition.
2. Select supplier and prepare for risk-based monitoring of development (if applicable) and acceptance review.
3. Manage risks and prepare for capability launch.
4. Conduct acceptance review.
5. Launch WEA capability and transition to operations and sustainment.

For each step, the following descriptions highlight the alert originator's interactions with candidate and chosen suppliers, which can facilitate cybersecurity risk mitigation and result in a more resilient alerting capability.

F.1 Adoption Example Step 1: Identify Requirements and Prepare for Acquisition

In this step, the alert originator identifies requirements and prepares for acquisition of the WEA capability. In many cases, the acquisition activity will focus on comparing vendor products or services that exist or are in development. In others, the activity will involve specifying requirements for a custom-built capability (or for modifications to an existing capability). Whatever the approach, the alert originator will need to identify and communicate key requirements, including those for security, and to evaluate candidate suppliers' responses. Appendix A.4.2 suggests questions that the alert originator can ask candidate suppliers regarding their security practices.

The executive manager for the alert originator initiates Adoption Step 1, ensuring that roles and responsibilities are assigned and resources are allocated. The operations manager and operations staff develop one or more operational mission threads that describe the steps they execute in generating alert messages (see Section 3, Prepare for Cybersecurity Analysis, for a description of this activity). In addition, they document requirements for the alerting capability from an operational perspective.

IT, information security, and incident response staff analyze the operational mission threads developed by the operations manager and staff, identifying potential issues related to cybersecurity, performance, resilience, and other quality attributes that they deem essential. For cybersecurity, this includes identifying cyber threats and vulnerabilities (see Section 4). Next, they analyze these threats and vulnerabilities, assess and prioritize resultant risks, and identify cybersecurity risk-mitigation actions (see Section 5).

The cybersecurity risk-mitigation actions may be documented in some or all of the following:

- alert originator operational procedures
- alert originator training modules
- alert originator equipment configuration requirements

- supplier product security requirements
- supplier development practice requirements

The alert originator's technical acquisition staff gathers these requirements and documents and disseminates them to candidate suppliers. The form this documentation takes will depend on the type of acquisition and the alert originator's practices for acquiring products and services. Table 26 describes the CSRM tasks for Adoption Step 1.

Table 26: Alert Originator CSRM Tasks for Adoption Step 1: Identify Requirements and Prepare for Acquisition

Alert Originator CSRM Tasks		Supplier Tasks in Response to Alert Originator CSRM Tasks
• Execute the CSRM strategy: (1) Develop operational mission threads depicting the steps in their expected WEA alerting scenarios, (2) identify cyber threats and vulnerabilities in these steps, (3) assess risk and identify mitigation actions, and (4) mitigate risks. • Prepare for acquisition (i.e., prepare a request for proposal (RFP) or a request for quote specifying requirements and selection criteria; identify risk factors under consideration). – Document and provide to candidate suppliers security (and other quality attribute) and capability requirements as well as supplier selection criteria. Capability requirements define functions; quality requirements include, e.g., reliability, security, and usability. Security requirements should draw on results from executing Stages 1–4 of the CSRM strategy, any mandated compliance standards for the alert originator's organization, and the rules of behavior specified in the MOA with FEMA for access to IPAWS-OPEN. In addition to standard alert-generation capability requirements, include requirements for level of integration with existing systems, hosting, training, sustainment, supply-chain risk management, and cost and schedule parameters. Include the expected supplier support for acceptance review, capability launch, and operations and sustainment in the requirements and request for information.	→	Respond to alert originator requirements, including those for security. This may be accomplished through formal proposals, capability demonstrations with question and answer sessions, or other means. Describe approach to identifying threats and vulnerabilities in development activities and to assessing risks and developing cybersecurity risk-mitigation and management plans. Include with proposals identification of risks and plans for risk-based monitoring of development activities and service provision (to include the supplier's own acquisition and supply-chain monitoring).
– Request that candidate suppliers describe the security practices and controls used in operations, development, and sustainment, and the security features of their products and services. Request identification of any coding or development standards the supplier uses that enhance cybersecurity [for examples, see Allen 2008, DHS 2013, Howard 2006, McGraw 2012, OWASP 2013, SAFECode 2013, SANS 2011, Seacord 2013]. – Ask potential suppliers (development, service provision, and sustainment) to perform a threat and vulnerability analysis and risk assessment of ▪ their development environment and processes, including how they manage supply-chain risks (i.e., risks introduced by the use of third-party products) ▪ the WEA product or service they are offering – Ask potential suppliers to develop and execute risk-mitigation and management plans based on the results.	←	

F.2 Adoption Example Step 2: Select Supplier and Prepare for Risk-Based Monitoring of Development (if applicable) and Acceptance Review

In this step, the alert originator reviews proposals from, and information about, candidate suppliers and their products and services, and selects a supplier. The alert originator and supplier finalize an agreement (this may be a contract, an SLA, or some other vehicle). The alert originator then begins preparing for acceptance review of the product or service, based on the terms of the agreement. If the supplier will develop a custom product or service or substantively modify an existing product or service, the alert originator should also prepare for risk-based monitoring of development. This monitoring may include review of progress reports provided by the supplier, interim demonstrations, inspection of technical artifacts, or other activities driven by identified risks. Table 27 describes the CSRM tasks involved in Adoption Step 2.

Table 27: Alert Originator CSRM Tasks for Adoption Step 2: Select Supplier and Prepare for Risk-Based Monitoring of Development (if Applicable) and Acceptance Review

Alert Originator CSRM Tasks		Supplier Tasks in Response to Alert Originator CSRM Tasks
Alert originator reviews proposal and technical information and selects solution provider, ensuring that • capability information provided matches operational requirements • both capabilities and quality attributes (including security) are incorporated • any other required aspects of the capability (e.g., integration with existing alerting or emergency management capabilities) are sufficiently described	←	Candidate solution providers prepare and submit proposals, offer demos, etc. Candidate solution providers include with their proposals identification of cybersecurity risks and plans for risk-based monitoring of development activities and service provision (to include their own acquisition and supply-chain monitoring).
Alert originator prepares for risk-based monitoring of development (if applicable) and acceptance testing: • Identify risks associated with the supplier's development approach and products • Develop strategy for monitoring these risks (e.g., regular discussions, progress reports, demonstrations, inspections) Alert originator and supplier agree to terms. Alert originator has now selected an approved IPAWS developer and can complete the MOA with FEMA [FEMA 2012a].	→	Supplier agrees to terms, including requirements, cost, schedule, monitoring, and interaction during development, if applicable. Supplier refines risk management plan for capability development and service provision, if needed, to meet terms of agreement.

F.3 Adoption Example Step 3: Manage Risks and Prepare for Launch

In this step, the alert originator performs risk-based monitoring of the supplier's development activities (if applicable) and works with the supplier to plan launch of the capability. The alert originator will also prepare internally for capability adoption, identifying and managing risks, preparing for operations and sustainment, developing and conducting training, configuring equipment, and working with external organizations to raise awareness of the new capability.

From a cybersecurity perspective, the new capability may introduce risks that the alert originator did not encounter previously. For example, the alert originator may need to limit user privileges

on accounts used to transmit WEA messages to reduce the risk of compromises that could impact alerting. It may also be necessary to prohibit the use of removable media on devices used to send alerts. Careful attention to system and network configuration, along with appropriate training, will mitigate a number of security-related adoption risks. Table 28 lists CSRM tasks for Adoption Step 3.

Table 28: Alert Originator CSRM Tasks for Adoption Step 3: Manage Risks and Prepare for Launch

Alert Originator CSRM Tasks		Supplier Tasks in Response to Alert Originator CSRM Tasks
Execute risk management activities. • Observe or participate in verification activities, per the terms of the alert originator–supplier agreement, and provide feedback. • Monitor implementation and verification of security-related requirements.	→	Supplier executes risk management plan. Supplier develops, acquires, and installs hardware or software capability (hosted per contractual agreement) and verifies and validates requirements, to include both operational and post-launch sustainment requirements.
Plan and prepare for launch. • Coordinate activities with supplier, including planning and preparation for acceptance review and launch. – Acceptance review should address the alert originator's concerns and requirements about the capability, quality attributes, support for launch, and sustainment. – Cybersecurity requirements and procedures should be part of the acceptance review. Include participants from operations, IT, information security, and incident response roles in the review. – Acceptance review should include a mission thread or scenario that demonstrates simple sustainment actions, such as adding and removing a user and applying a minor patch.	←	Supplier works with alert originator to plan and prepare procedures for acceptance review and launch activities. Supplier works with alert originator to complete sustainment plans, addressing concerns regarding how security will be maintained as patches, upgrades, and enhancements are supplied.
• Plan for and execute internal activities: – operations and sustainment plans and procedures – training – external interface activities (local first responders, public awareness) – schedule for launch		

F.4 Adoption Example Step 4: Conduct Acceptance Review

In this step, the alert originator and supplier conduct a joint acceptance review. The WEA capability must pass this review before it can be launched. Prior to this review, the supplier should have conducted development and integration testing to verify requirements implementation and the alert originator should have received satisfactory evidence that this testing was done. The acceptance review is a less rigorous but nonetheless important demonstration of readiness for launch. Table 29 lists CSRM tasks for the acceptance review.

Table 29: Alert Originator CSRM Tasks for Adoption Step 4: Conduct Acceptance Review

Alert Originator CSRM Tasks		Supplier Tasks in Response to Alert Originator CSRM Tasks
With supplier, finalize procedures for acceptance review.		With alert originator, finalize procedures for acceptance review.
Engage operations management, operations, IT, and information security staff roles in review, which will include cybersecurity requirements and procedures.	←	
Conduct review and evaluate results. • If satisfactory with no issues, this step is complete. • If satisfactory with issues that do not preclude launch, document the issues and coordinate with supplier on resolution. • If unsatisfactory, document issues and coordinate with supplier to resolve them before launch.	→	Participate in review, document any issues identified, and coordinate with alert originator on resolution and next steps.
Update capability launch plan, as needed.		

F.5 Adoption Example Step 5: Launch WEA Capability and Transition to Operations and Sustainment

In this step, the alert originator executes the capability launch plan and transitions the capability to operations and sustainment. As the capability is operated and sustained, the alert originator conducts lessons-learned sessions designed to improve performance and resilience of the alerting capability. The supplier will support launch of the capability. If the supplier is responsible for operations or sustainment (e.g., if the WEA capability is provided as a service), they will also be engaged in lessons-learned sessions. Table 30 lists CSRM tasks for launching the WEA capability and transitioning it to sustainment.

Table 30: Alert Originator CSRM Tasks for Adoption Step 5: Launch WEA Capability and Transition to Operations and Sustainment

Alert Originator CSRM Tasks		Supplier Tasks in Response to Alert Originator CSRM Tasks
Execute capability launch plan. • Ensure that security controls have been implemented.		Support alert originator in capability launch.
• Conduct internal tests.	←	Support alert originator in lessons-learned sessions, as applicable.
Declare capability operational.		
Initiate operational use, conducting a lessons-learned session each time an alert is issued (include cybersecurity lessons).		Support alert originator in monitoring (and minimizing) impacts of sustainment actions on operations.
Initiate sustainment activities, monitoring impacts on operations for • internal sustainment actions that affect the WEA capability (e.g., adding users or modifying user privileges, and applying internal patches and system software upgrades)		
• external sustainment actions (e.g., application of a WEA capability upgrade)	→	
• cybersecurity impacts of sustainment actions (e.g., need to elevate privileges, accidental insertion of malware) • incident response impacts (e.g., responding to a cyber attack)		

Appendix G Sample CSRM Planning Guide

We offer the following sample CSRM plan activities for alert-originating organizations to tailor to their WEA security risk management needs. The sequence and nature of some activities may vary depending on the implementation choices that an organization makes, and parts of some activities may be handled by resources outside of the organization, such as a vendor (e.g., Activity 3 has several options).

Activity Number	Activity Goal	Assigned to	Target completion date	Planning activities
1	Define organizational security requirements	Executive manager with assistance from others as needed	Immediately	Review the set of IPAWS alert originator security requirements and your IPAWS application; tailor the security requirements to fit your organizational needs
2	Complete mandated IPAWS training and any additional competency training needed for WEA preparation	Operations manager and others as appropriate	Immediately	In preparation for WEA planning, at least one member of the management team must complete the IPAWS training to be familiar with the steps needed to implement WEA capability
3a	Select the organizational security requirements to assign to acquired technology and services	Technology acquisition and contracting staff	Immediately	Review the organizational security requirements from Activity 1, and select the security requirements that acquired technology and services must address
3b	Select the organizational security requirements to assign to operational staff	Operations manager	Immediately	Review the organizational security requirements from Activity 1, and select the security requirements that acquired technology and services must address
3c	Select the organizational security requirements to assign to development staff	Development staff		Review the organizational security requirements from Activity 1, and select the security requirements that acquired technology and services must address
4	Identify remaining unaddressed security requirements, and define how to address them	Executive manager with assistance from others as needed	Immediately	Review security requirements not allocated in Activities 3a, 3b, and 3c to determine if they will be met, and identify who will be responsible
5	Prepare for cybersecurity analysis – build an operational mission thread (Note: Additional activities such as training for selected vendor tools may be necessary before performing Activity 5)	Technology acquisition and contracting staff, operations manager, and development staff representative		Review the sample operational mission thread in Section 3 of the CSRM strategy report, and tailor it to match the planned WEA alerting environment; tailor the sample mission thread assets to match the planned organizational components of the target operational environment

Activity Number	Activity Goal	Assigned to	Target completion date	Planning activities
6a	Validate the operational mission thread developed in Activity 5 with planned acquisition technology and service providers	Technology acquisition and contracting staff		Confirm that the operational plan is feasible based on input from the planned organizational suppliers
6b	Validate the operational mission thread developed in Activity 5 with current operational users to ensure completeness	Operations manager		Confirm that the operational plan is feasible based on input from the current operational staff
6c	Validate the operational mission thread developed in Activity 5 with current development staff	Development staff		Confirm that the operational plan is feasible based on input from the development staff
7	Conduct a cybersecurity analysis	Technology acquisition and contracting staff, operations manager, development staff, and security expertise (if available)		At a minimum, review the STRIDE analysis example (provided in Section 4 of the CSRM strategy report) that was developed for the sample mission thread, and tailor it to match the threats and vulnerabilities in the organization's target operational environment; or apply another analysis technique to identify threats and vulnerabilities
8	Review the decisions of threats and vulnerabilities with the vendor (if appropriate) and the executive manager	Technology acquisition and contracting staff, operations manager, and development staff		Confirm that the threats and vulnerabilities selected by the organization are reasonable; define how risks that are not prevented or mitigated will be monitored to recognize, resist, and recover as needed
9	Assess and prioritize cybersecurity risks	Technology acquisition and contracting staff, operations manager, and development staff representative		Review the sample risk information provided in Section 5 of the CSRM strategy report. If your operational environment is similar to the example mission thread, these will be a useful starting set. Otherwise, follow the guidance provided in Appendix D to build and prioritize your organizational risks
10	Review and augment the organizational security requirements developed in Activity 1 to ensure that they are sufficient to address the cybersecurity risks that must be mitigated (determined in Activity 9)	Technology acquisition and contracting staff, operations manager, and development staff		Assign new requirements to an organizational owner (review and adjust the assignments from Activities 3a, 3b, 3c, and 4)

Activity Number	Activity Goal	Assigned to	Target completion date	Planning activities
11	Construct a timeline of activities that must be completed to address all of the assigned cybersecurity requirements, and assign roles and responsibilities for each activity	Technology acquisition and contracting staff, operations manager, and development staff representative		Build a simple GANTT chart (using Microsoft Project or similar tool) that lists the activities and expected completion dates. See Section 6 of the CSRM strategy report for example role-responsibility assignments.
12	Review the timeline and adjust as needed to consider other organizational priorities	Executive manager with assistance from others as needed		
13	Schedule periodic meetings to review the timeline, confirm completeness of requirements, and respond to new information and changes (repeat prior activities as needed to ensure completeness of the timeline)	Executive manager with assistance from others as needed	Throughout the implementation cycle	
14	Construct an operational security risk management plan to ensure that cybersecurity risks continue to be addressed once the WEA capability is fielded	Operations manager		Ensure that risks not prevented or mitigated can be recognized, resisted, and recovered from (based on information assembled in Activity 8)
15	Review the operational security plan for completeness, and assign monitoring responsibility for activities as needed across the organizational WEA capability participants	Executive manager with assistance from others as needed	Prior to “Go Live”	
16	Periodically review the operational security plan to ensure that cybersecurity issues are being addressed	Executive manager, operations manager, and other participants as needed		Review at least annually, and assemble lessons learned from each WEA use

Acronym List

Acronym	Definition
AMBER	America's Missing: Broadcasting Emergency Response
AOS	alert origination system
AOSP	alert origination service provider
CAP	Common Alerting Protocol
CMAC	Commercial Mobile Alert for C Interface
CMAS	Commercial Mobile Alert System; also, Commercial Mobile Alert Service, the former name of the Wireless Emergency Alerts (see also PLAN and WEA)
CMSP	commercial mobile service provider
CSRA	cybersecurity risk analysis
CSRM	cybersecurity risk management
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security Science and Technology Directorate
DS	development staff
EAS	Emergency Alert System
EM	executive management
EOC	emergency operations center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FOC	FEMA operations center
GUI	graphical user interface
IPAWS	Integrated Public Alert and Warning System
IPAWS-OPEN	Integrated Public Alert and Warning System Open Platform for Emergency Networks
IR	incident response
IS	information security
ISP	internet service provider
IT	information technology
MOA	memorandum of agreement
MTA	mission thread analysis
NCIC	National Crime Information Center
NCMEC	National Center for Missing and Exploited Children
OM	operations management
OP	operator
OPEN	See IPAWS-OPEN
OWASP	Open Web Application Security Project
PLAN	Personal Localized Alerting Network (former FCC term for CMAS; see also WEA)
PM	personnel management
PSAP	public-safety answering point
RDT&E	Research, Development, Testing, and Evaluation
RFP	request for proposal

Acronym	Definition
SLA	service-level agreement
SSL	Security Sockets Layer
STRIDE	spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege
TA	technology acquisition
URL	Uniform Resource Locator
USB	Universal Serial Bus
WEA	Wireless Emergency Alerts (see also CMAS and PLAN)

Glossary of Key Terms and Concepts

alerting authority	Public official granted the authority to alert the public of emergency situations through federal, state, and local laws. [FEMA 2012b]
alert origination service provider (AOSP)	An entity internal or external to an emergency manager's organization that provides an interface between emergency managers and IPAWS. An AOSP may be a vendor providing the IPAWS interface as a service or supplying software or hardware that the emergency manager can use on site to access IPAWS. An AOSP may also be a qualified internal unit within the emergency manager's organization (e.g., an information technology development unit).
alert originator	"[Entity r]esponsible for creating [WEA] alert messages and monitoring the message feedback that results from those messages. Possibly responsible for countersigning/verifying other [WEA] alert messages. Must be verified by system maintainer and federal identity management as an eligible originator." [FEMA 2009, p. 13]
AMBER alert	One of the three categories of alerts sent by WEA. The other categories are imminent threat and presidential. The AMBER Alert Program is a voluntary partnership between law enforcement agencies, broadcasters, transportation agencies, and the wireless industry. [FEMA 2012b]
attack, cyber	"An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." [CNSSI 2010, p. 22]
attacker	See *threat actor*.
cyber environment	"Users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks." "The software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices." [ITU 2008, p. 2, 6]
cybersecurity	"Ability to protect or defend the use of cyberspace from cyber attacks." [CNSSI 2010, p. 22] "Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training,

	best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." [ITU 2008, p. 2]
cybersecurity risk management	Application of risk management practices to cybersecurity.
imminent threat alert	One of the three categories of alerts sent via WEA. The other threats are AMBER and presidential. Imminent threat alerts must meet specific criteria for urgency, severity, and certainty. Examples include tornado, flash flood, or hurricane warnings; hazardous material incident warnings; or terrorist threat warnings. [FEMA 2012b]
mission thread	Set of steps taken to respond to an incident or execute a mission. [Gagliardi 2013]
mission thread description	Includes the environment in which the mission thread takes place, a diagram illustrating the environment, and the organizational assets and actors involved in the steps of the mission thread.
operational resilience	"The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk." [Caralli 2011, p. 976–977]
presidential alert	One of the three categories of alert messages used by WEA. The other categories are AMBER alert and imminent threat alert. Presidential alerts are reserved for use by the president of the United States in the event of a national emergency. [FEMA 2012b]
risk	"The possibility of suffering harm or loss. From a resilience perspective, risk is the combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited," and the presence of uncertainty. "In the CERT-RMM [Resilience Management Model], this definition is typically applied to the asset or service level such that the risk is the possibility of suffering harm or loss due to disruption of high-value assets and services." [Caralli 2011, p. 983]
risk management	"Process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk-mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the infor-

	mation system; and 4) documenting the overall risk management program." [CNSSI 2010, p. 62]
risk management strategy	"Course of action or actions to be taken in order to manage risks." [DHS 2010, p. 31]
risk mitigation	"Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process." [CNSSI 2010, p. 62]
STRIDE	Method for categorizing cyber threats. The name STRIDE is derived from the first letter in each threat category: spoofing, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege. [Microsoft 2005, Howard 2006]
threat actor (also attacker)	"A situation, entity, individual, group, or action that has the potential to exploit a threat." [Caralli 2011, p. 987]
threat, cyber	"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." [CNSSI 2010, p. 75]
threat environment	"The set of all types of threats that could affect the current operations of the organization." [Caralli 2011, p. 987]
threat source	"The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability." [CNSSI 2010, p. 75]
vulnerability	"Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." [CNSSI 2010, p. 81]
WEA alerting pipeline	End-to-end set of elements and interfaces that implement the WEA capability from alert origination, through IPAWS and the CMSP, to dissemination of alerts to intended recipients.

References

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

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

[Alberts 2006]
Alberts, Christopher. *Common Elements of Risk* (CMU/SEI-2006-TN-014). Software Engineering Institute, Carnegie Mellon University, 2006. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7899

[Allen 2008]
Allen, Julia H.; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; & Mead, Nancy R. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008.

[Bowen 2006]
Bowen, Pauline; Hash, Joan; & Wilson, Mark. *Information Security Handbook: A Guide for Managers, NIST Special Publication (SP) 800-100.* NIST, U.S. Department of Commerce, 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[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.

[Charette 1990]
Charette, Robert N. *Application Strategies for Risk Analysis*. McGraw-Hill Book Company, 1990.

[CMSAAC 2007]
Commercial Mobile Service Alert Advisory Committee. *Commercial Mobile Alert Service Architecture and Requirements* (Version 1.0). FCC, 2007.

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

[DHS 2010]
Department of Homeland Security. *DHS Risk Lexicon*. http://www.dhs.gov/files/publications/gc_1232717001850.shtm (2010).

[DHS 2013]
Department of Homeland Security. *Build Security In.* https://buildsecurityin.us-cert.gov/bsi/home.html (2013).

[Dorofee 1996]
Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Software Engineering Institute, Carnegie Mellon University, 1996. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30856

[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 2010]
Federal Emergency Management Agency. *CMAS Alert Origination System to Alert Aggregator Interface Requirements Document (IRD)* (Version 1.0). FEMA, March 2010.

[FEMA 2012a]
Federal Emergency Management Agency. *IPAWS Alerting Authorities*. http://www.fema.gov/alerting-authorities (2012).

[FEMA 2012b]
Federal Emergency Management Agency. *IPAWS Glossary.* http://www.fema.gov/library/viewRecord.do?id=5578 (2012).

[Gagliardi 2013]
Gagliardi, Mike; Wood, Bill; & Morrow, Tim. *Introduction to the Mission Thread Workshop* (CMU/SEI-2013-TR-003). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=63148

[GAO 2013]
Government Accountability Office. *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges.* http://www.gao.gov/assets/660/652817.pdf (2013).

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

[INCOSE 2010]
International Council on Systems Engineering. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities* (INCOSE-TP-2003-002-03.2). INCOSE, 2010.

[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.

[Kloman 1990]
Kloman, H. F. “Risk Management Agonists.” *Risk Analysis 10*, 2 (June 1990): 201–205.

[McGraw 2006]
McGraw, Gary. *Software Security: Building Security In.* Addison-Wesley, 2006.

[McGraw 2012]
McGraw, Gary; Migues, Sammy; & West, Jacob. *Building Security In Maturity Model 4.* Creative Commons, 2012.
http://www.bsimm.com

[McGregor 2013]
McGregor, John D.; Elm, Joseph P.; Trocki Stark, Elizabeth; Lavan, Jennifer; Creel, Rita; et al. *Best Practices in Wireless Emergency Alerts* (CMU/SEI-2013-SR-015). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=70001

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

[NIST 2010]
National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems* (NIST Special Publication 800-37, Revision 1). NIST, U.S. Department of Commerce, 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[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

[NRECA 2011]
National Rural Electric Cooperative Association Cooperative Research Network. *Guide to Developing a Cyber Security and Risk Mitigation Plan* (DOE Award No: DE-OE0000222). NRECA, 2011.

[OWASP 2013]
Open Web Application Security Project. *The OWASP Top Ten – Ten Most Critical Web Application Security Risks.* https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (2013).

[SAFECode 2008]
SAFECode. *Software Assurance: An Overview of Current Industry Best Practices*.
http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf (2008).

[SAFECode 2013]
SAFECode. *SAFECode Publications.* http://www.safecode.org/publications.php (2013).

[SANS 2011]
SANS Institute. *CWE/SANS Top 25 Most Dangerous Software Errors.* http://www.sans.org/top25-software-errors (2011).

[Seacord 2013]
Seacord, Robert C. *Secure Coding in C and C++*. Addison-Wesley, 2013.

[SEI 2012a]
Software Engineering Institute. *Commercial Mobile Alert System (CMAS) Alerting Pipeline Taxonomy* (CMU/SEI-2012-SR-019). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=70067

[SEI 2012b]
Software Engineering Institute. *Commercial Mobile Alert System (CMAS) Scenarios* (CMU/SEI-2012-SR-020). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=70075

[SEI 2013]
Software Engineering Institute. *Study of Integration Strategy 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

[White House 2013]
White House. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2013).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators	FA8721-05-C-0003

6. AUTHOR(S)

The WEA Project Team

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-018

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)

The Wireless Emergency Alerts (WEA) service depends on computer systems and networks to convey potentially life-saving information to the public in a timely manner. However, like other cyber-enabled services, it is susceptible to risks that may enable attackers to disseminate unauthorized alerts or to delay, modify, or destroy valid alerts. Successful attacks may result in property destruction, financial loss, injury, or death and may damage WEA credibility to the extent that users ignore future alerts or disable alerting. This report describes a four-stage cybersecurity risk management (CSRM) 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. In Stage 1, alert originators document mission threads, describing the process for generating WEA messages. In Stage 2, they examine the mission threads to identify threats and vulnerabilities. In Stage 3, they use the identified threats and vulnerabilities to assess and prioritize risks according to their likely impact on WEA operations. Finally, in Stage 4, they use the results of risk assessment to define cybersecurity roles and assign risk-mitigation actions. The four stages are repeated periodically and as procedures, threats, technology, and staff assignments change.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cybersecurity, cyber threats, emergency alerting, risk management, Wireless Emergency Alerts, WEA	183

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102