Software Engineering Institute
Carnegie Mellon University

Wireless Emergency Alerts Commercial Mobile Service Provider (CMSP) Cybersecurity Guidelines

Christopher Alberts
Audrey Dorofee
Carol Woody, PhD

June 2016

SPECIAL REPORT
CMU/SEI-2016-SR-009

CERT Division, Software Solutions Division

http://www.sei.cmu.edu

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.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

Operationally Critical Threat, Asset, and Vulnerability Evaluation℠

DM-0003539

Table of Contents

List of Figures

List of Tables

Executive Summary

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that includes the cellular industry, Federal Communications Commission, Federal Emergency Management Agency (FEMA), and U.S. Department of Homeland Security Science and Technology Directorate. 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. Like other cyber-enabled services, however, 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 (e.g., design flaws, user errors or acts of nature that compromise operations).

The end-to-end WEA alerting pipeline consists of the following four major elements that implement the alerting process:

1. *Alert originators*—the people, information, technology and facilities that initiate and create an alert, define a target distribution area (i.e., targeted geographic area) and convert the alert information into the appropriate format for dissemination
2. *Integrated Public Alert and Warning System Open Platform for Emergency Networks*—a collection of FEMA systems that receives, validates, authenticates and routes various types of alerts to the appropriate disseminator, such as WEA, the Emergency Alert System or the National Oceanic and Atmospheric Administration
3. *Commercial mobile service providers (CMSPs)*—commercial wireless carriers that broadcast WEA messages to a designated geographic area
4. *Alert recipients*—the WEA-capable mobile devices located in the targeted alert area

This report presents the results of a study of the CMSP element of the WEA pipeline conducted by the CERT® Division at Carnegie Mellon® University's Software Engineering Institute (SEI). The goal of this study is to provide members of the CMSP community with practical guidance that they can use to better manage cybersecurity risk exposure. For the study, the research team performed a security risk analysis of the CMSP WEA infrastructure to identify and analyze security risks. We then used the results of the security risk analysis to develop cybersecurity guidelines tailored to the needs of CMSPs.

We used the Security Engineering Risk Analysis (SERA) Method to develop cybersecurity guidelines tailored to the needs of CMSPs. The SERA Method was developed at the SEI CERT Division. We selected this method because it is designed to analyze security risks in highly complex, multisystem operational environments such as the WEA alerting pipeline. The SERA Method incorporates a variety of models that can be analyzed at any point in the lifecycle to (1) identify security threats and vulnerabilities and (2) construct security risk scenarios. An organization can

® CERT and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

then use those scenarios to focus its limited resources on controlling the most significant security risks.

To conduct the study, several documents that described CMSP WEA processes and technologies prior to performing the security risk analysis were collected and reviewed. After applying the SERA Method, the results were used to develop a draft version of the CMSP Security Guidelines. In the draft version of the guidelines, the raw risk data that was generated by applying the SERA Method to the four security risk scenarios was reviewed, with a variety of subject-matter experts (SMEs) who were familiar with the CMSP WEA alerting infrastructure and process. Based on the feedback provided by the SMEs, the guidelines were updated and refined, producing a baseline version of the CMSP Security Guidelines.

The following four security risk scenarios were identified and analyzed using the SERA Method:

1. *Risk 1: Insider Sends False Alerts:* An insider inserts malicious code designed to replay a nonsense or inflammatory alert message repeatedly in the CMSP Gateway. As a result, customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.
2. *Risk 2: Inherited Replay Attack:* The carrier receives emergency alerts from an upstream replay attack on an alert originator and sends these messages repeatedly to customers in the designated geographic area. As a result, customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.
3. *Risk 3: Malicious Code in the Supply Chain*: Malicious code designed to disseminate alerts as broadly as possible and change the priority of all alerts into presidential alerts is inserted into a carrier's WEA alerting system by a supply-chain subcontractor. As a result, customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.
4. *Risk 4: Denial of Service*: An outside actor with malicious intent uses a denial-of-service attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack. As a result, people could be unaware of the attack and be put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

These scenarios provide a broad cross section of the types of issues likely to affect the CMSP WEA alerting system. Although not exhaustive, the resulting analysis provides a broad range of mitigation requirements that CMSPs should consider.

CMSP Security Guidelines are a set of high-priority security controls that a CMSP should consider implementing to protect its WEA alerting system. These guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study. We identified security controls in the following areas:

- *Human Resources*—the part of an organization that is responsible for finding, screening, recruiting and training job applicants; administering employee-benefit programs; conducting performance appraisals; and administering performance-based rewards

- *Training*—the process by which an individual is taught the skills needed to perform designated job duties
- *Contracting*—the process of developing a formal agreement with a third party to provide a product or service
- *Physical Security*—the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to an organization and its mission
- *Change Management*—the process of requesting, analyzing, planning, implementing and evaluating changes to a system
- *Access Control*—the process of limiting access to system and network resources
- *Information Management*—an approach for (1) collecting and managing information from one or more sources and (2) distributing that information to one or more audiences
- *Vulnerability Management*—the practice of identifying, classifying, remediating and mitigating cybersecurity vulnerabilities
- *System Architecture*—a conceptual model that defines the structure and behavior of a system
- *System Configuration*—the software and system configuration settings that (1) address known security risks and (2) comply with an organization's security policies
- *Code Analysis*—methods, tools and techniques for analyzing code for the presence of security vulnerabilities and malicious code
- *Technical Monitoring*—the collection and analysis of system and network data to identify suspicious or unusual behavior
- *Independent Reviews*—an activity performed by an objective third party to *provide insight into an activity's progress, current performance and risks*
- *Incident Response*—an organizational practice for detecting, analyzing and responding to cybersecurity events and incidents
- *Disaster Recovery*—an activity that enables the recovery or continuation of critical technology infrastructures and systems following a natural or human-induced disaster

A CMSP can use the Security Guidelines to assess its current security controls and chart a course for improvement. To do so, the CMSP begins by assessing the extent to which it implements the CMSP Security Guidelines. It then selects which gaps to address (based on resources available and current risk exposure) and develops an improvement plan for the selected controls. Finally, the CMSP implements its improvement plan, with the goal of reducing its exposure to the four risk scenarios featured in this study.

Abstract

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that enables local, tribal, state, territorial, and federal public safety officials to disseminate geographically targeted emergency alerts to users of capable mobile devices in an affected geographic area. The end-to-end WEA alerting pipeline comprises the following four major elements: (1) alert originators, (2) Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN), (3) commercial mobile service providers (CMSPs), and (4) alert recipients. This report presents the results of a study of the CMSP element of the WEA pipeline conducted by researchers at the Software Engineering Institute (SEI). The goal of the study is to provide members of the CMSP community with practical guidance that they can use to better manage their cybersecurity risk exposure. To conduct the study, the SEI research team used the Security Engineering Risk Analysis (SERA) Method to assess high-priority cybersecurity risks in the CMSP WEA infrastructure. The research team used the results of the risk analysis to develop a set of cybersecurity guidelines tailored to the needs of CMSPs.

1 Background

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that includes the cellular industry, Federal Communications Commission (FCC), Federal Emergency Management Agency (FEMA), and U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T). The WEA capability provides a valuable service, enabling local, tribal, state, territorial and federal public safety officials to disseminate geographically targeted emergency alerts to users of capable mobile devices if they are located in, or travel to, an affected geographic area. Like other cyber-enabled services, however, 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, including design flaws, user errors and acts of nature that compromise operations.

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

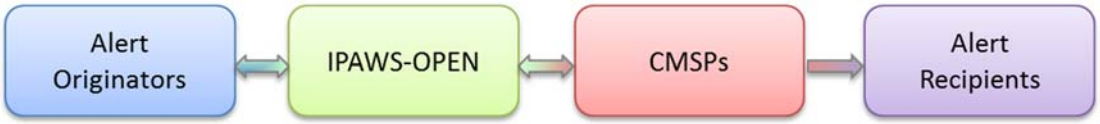

Figure 1: The Four Elements of the WEA Alerting Pipeline

The *alert originators* (AOs) 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 AOs 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.

This report presents the results of a study of the CMSP element of the WEA pipeline conducted by the CERT® Division at Carnegie Mellon® University's Software Engineering Institute (SEI). The goal of this study is to provide members of the CMSP community with practical guidance that they can use to better manage their cybersecurity risk exposure. This study builds on work that was completed by CERT Division technical staff in 2013, which focused on AOs [SEI 2014]. The 2013 study examined the AO WEA infrastructure and produced a cybersecurity risk management strategy for AOs.

For the current study, a security risk analysis of the CMSP WEA infrastructure was performed, to identify and analyze security risks in detail. The research team then used the results of the security risk analysis to develop cybersecurity guidelines tailored to the needs of CMSPs.

1.1 Risk-Based Analysis

A risk-based analysis is a useful approach for prioritizing which controls to address first. For example, the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, titled *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, defines more than 200 controls across 18 categories [NIST 2013]. An organization with limited resources cannot implement all controls specified in the NIST document. Organizational decision makers need a way to set priorities about which controls are most important to the organization's mission. NIST recommends a risk-based approach for identifying high-priority controls. Decision makers can initially focus on the subset of controls that mitigate their highest priority cybersecurity risks. We employed this perspective in our study.

We used the Security Engineering Risk Analysis (SERA) Method to develop cybersecurity guidelines tailored to the needs of CMSPs. The SERA Method was developed at the SEI CERT Division. We selected this method because it is designed to analyze security risks in highly complex, multisystem operational environments such as the WEA alerting pipeline. The SERA Method incorporates a variety of models that can be analyzed at any point in the lifecycle to (1) identify security threats and vulnerabilities and (2) construct security risk scenarios. An organization can then use those scenarios to focus its limited resources on controlling the most significant security risks.

1.2 Developing and Applying CMSP Cybersecurity Guidelines

Figure 2 illustrates two distinct types of activities: (1) the approach used by the research team to conduct this study and (2) how the results of the study can be applied and updated. Both types are discussed in this section, beginning with how we conducted the study.

For the current study, we performed a security risk analysis of the CMSP WEA infrastructure using the SERA Method. This analysis is represented in Figure 2 by the four tasks of the SERA Method:

1. Establish operational context.
2. Identify risk.
3. Analyze risk.
4. Develop control plan.

We collected and reviewed several documents that described WEA processes and technologies for CMSPs prior to performing the security risk analysis. After applying the SERA Method, we used the results to develop a draft version of the CMSP Security Guidelines. We then reviewed the draft version of the guidelines—including the raw risk data that we generated by applying the SERA Method to the four security risk scenarios—with a variety of subject-matter experts (SMEs) who were familiar with the CMSP WEA alerting infrastructure and process. (The top feedback loop in Figure 2 represents the SME reviews of the draft guidelines.) Based on the feedback provided by the SMEs, we updated and refined the guidelines, producing a baseline (or final) version of the CMSP Security Guidelines. The

completion and delivery of this report marks the end of our study into developing security guidelines for CMSPs.

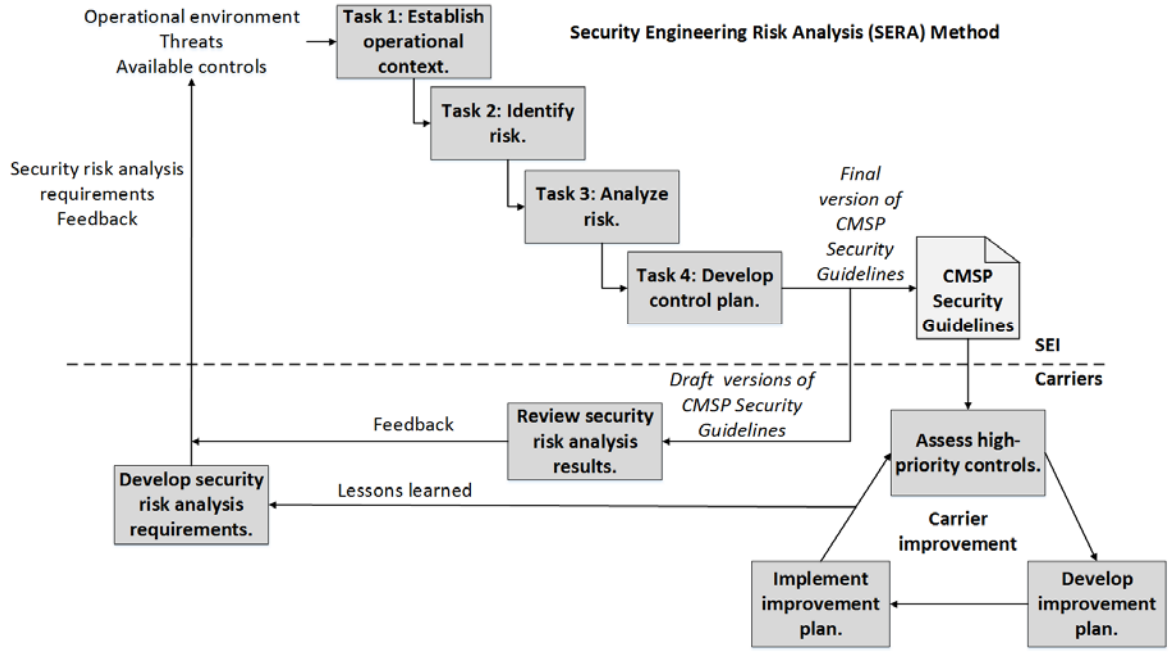

Figure 2: Approach for Improving CMSP Security

CMSPs are the primary audience for the results of the study. CMSP personnel will be responsible for applying the guidelines. Figure 2 presents three activities that a CMSP can perform to improve the security posture of its WEA alerting infrastructure. The CMSP begins by assessing the extent to which it implements the CMSP Security Guidelines. It then selects which controls to address, based on available resources and current risk exposure, and develops an improvement plan for the selected controls. Finally, the CMSP implements its improvement plan, with the goal of reducing its exposure to the four risk scenarios featured in this study.

Computing technology is constantly changing. As a result, new types of cyber threats continually emerge. In addition, cyber attackers continually look for new ways to attack existing technologies, leading to the discovery and exploitation of new types of vulnerabilities. Over time, these changes will need to be reflected in the CMSP Security Guidelines.

Figure 2 features an update cycle that is triggered by (1) lessons learned by CMSPs from applying the CMSP Security Guidelines and (2) changes to the CMSP operational environment, including changes to CMSP threats, technologies and available controls. When these triggers occur, the SEI (or another group) can reapply the SERA Method to update the CMSP Security Guidelines. The feedback loop in the bottom right of Figure 2 represents updating the guidelines based on lessons learned and changes in threats and attack types.

1.3 Study Scope and Limitations

When conducting the study, we started by defining a manageable scope for the underlying security analysis. Two factors heavily influenced the scope of the risk analysis: (1) the selected CMSP architecture and (2) the risks that we analyzed. This section briefly describes each factor.

We analyzed security risks in relation to the CMSP operational environment. To conduct the analysis, we first developed several models (e.g., workflows, architecture, data security attributes) that represent the selected CMSP operational environment. (We present these models in Section 3 of this report.) Most of those models (e.g., workflows, data security attributes) are applicable to most CMSPs. The architecture model was not as universally applicable, however. The CMSP architecture that we selected reflects the type of technology used by larger CMSPs. During our document reviews and discussions with CMSP stakeholders, we noted the existence of alternative CMSP architectures (e.g., using smartphone applications to disseminate WEA messages). The guidelines in this report will not translate directly to alternative architectures. CMSPs that implement different architectures will need to interpret and adjust this report's security guidelines appropriately.

The second factor that affected the scope of the study is the security risk scenarios that we selected for analysis. For our current study, we identified many candidate risks during our initial brainstorming activity. We also uncovered additional risks in our discussions with CMSP SMEs. For the study, we selected four high-priority security risk scenarios to analyze. We developed the CMSP Security Guidelines based on our analysis of those four scenarios. The current version of the guidelines does not address controls that are unique to security risk scenarios not included in the analysis.

1.4 Audience and Document Structure

The primary audience for this report is any CMSP stakeholder responsible for overseeing, operating, maintaining and securing the CMSP WEA infrastructure. CMSP stakeholders consist of personnel from a variety of organizations, including large and small carriers, government organizations and industry groups. A variety of personnel in those organizations will be interested in the content of this report, such as system and software engineers, information technology staff, cybersecurity staff, auditors and compliance personnel.

This report comprises the following sections:

- Part 1. Introduction
  - *Section 1. Background*—provides background information about the WEA alerting pipeline and describes the approach used to conduct the current study.
  - *Section 2. Method*—presents a brief introduction to the SERA Method and how it was used to conduct the study.
- Part 2. Findings
  - *Section 3. CMSP Operational Environment*—presents models (e.g., workflows, architecture, data security attributes) representing the selected CMSP operational environment evaluated in the study.
  - *Section 4. CMSP Risk Scenarios*—presents narrative descriptions for the four security risk scenarios that were analyzed in the study.

- *Section 5. CMSP Security Guidelines*—describes a set of controls that CMSPs can implement to address the four security risk scenarios that were analyzed in the study.

- Part 3. Conclusion: Summary and Next Steps
  - *Section 6. Applying the Results*—explores how CMSPs can apply the security guidelines specified in this report.
  - *Section 7. Next Steps*—outlines several potential next steps for the body of work described in this report.
- Appendices
  - *Appendix A: SERA Method Description*—presents a detailed description of the SERA Method, including illustrative examples.
  - *Appendix B: Risk Data*—provides raw risk data that was generated by the SERA Method for the four security risk scenarios.
  - *Appendix C: Control Summary*—presents a mapping of controls to the four security risk scenarios.
  - *Appendix D: Control Strategy Questionnaire*—provides a control strategy questionnaire that CMSPs can use to evaluate the security posture of their WEA alerting systems.

2 Method

For this study, SERA Method was employed because it is specifically designed to analyze security risks in highly complex operational environments. Traditional security risk-analyses approaches cannot handle the inherent complexity of modern cybersecurity attacks. These traditional approaches are typically based on a simple, linear view of risk that assumes that a single threat actor exploits a single vulnerability in a single system to cause an adverse consequence. In reality, multiple actors often exploit multiple vulnerabilities in multiple systems as part of a complex chain of events. The SERA Method is designed specifically for this type of multi-actor, multisystem risk environment, making it a good candidate for the WEA CMSP study.

2.1 SERA Method

The SERA Method defines a scenario-based approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain. The SERA Method incorporates a variety of models that can be analyzed at any point in the lifecycle to (1) identify security threats and vulnerabilities and (2) construct security risk scenarios. An organization can then use those scenarios to focus its limited resources on controlling the most significant security risks.

The SERA Method can be self-applied by the person or group that is responsible for acquiring and developing a software-reliant system or facilitated by external parties on behalf of the responsible person or group. In either case, a small team of approximately three to five people, called the *Analysis Team*, is responsible for implementing the framework and reporting findings to stakeholders.

An Analysis Team is an interdisciplinary team that requires team members with diverse skill sets. Examples of skills and experience that should be considered when forming a team include: security-engineering risk analysis, systems engineering, software engineering, operational cybersecurity and physical/facility security. The exact composition of an Analysis Team depends on the point in the lifecycle in which the SERA Method is being applied and the nature of the engineering activity being pursued. Table 1 highlights the four tasks that the Analysis Team performs when conducting the method.

Table 1: SERA Method Overview

Task		Description	Outputs
1.	Establish operational context	Task 1 defines the operational context for the analysis. The Analysis Team determines how the application or system supports operations (or is projected to support operations if the system of interest is not yet deployed). The team then (1) selects which operational workflow or mission thread to include in the analysis and (2) documents how the system of interest supports the selected workflow or mission thread.	• System of interest • Selected workflows/mission threads • Operational models

Task		Description	Outputs
2.	Identify risk	The Analysis Team transforms security concerns into distinct, tangible risk scenarios that can be described and measured. The team starts by reviewing the operational models from task 1, then brainstorms threats to the system of interest and selects one of the threats to analyze in detail. The Analysis Team identifies threat components and a sequence of steps for high-priority threats to the systems of interest. Finally, the Analysis Team creates a narrative, or scenario, for each security risk and compiles all data related to the scenario in a usable format.	• Threat components • Threat sequence • Workflow consequences • Stakeholder consequences • Enablers • Amplifiers • Risk scenario • Risk statement
3.	Analyze risk	Task 3 focuses on risk analysis. The Analysis Team evaluates each risk scenario in relation to predefined criteria to determine its probability, impact and risk exposure.	• Probability • Impact • Risk exposure
4.	Develop control plan	Task 4 establishes a plan for controlling a selected set of risks. The Analysis Team prioritizes the security risk scenarios based on their risk measures. The team then determines the basic approach for controlling each risk (i.e., accept or plan) based on predefined criteria and current constraints (e.g., resources and funding available for control activities). Finally, the Analysis Team develops a control plan for each risk that is not accepted.	• Prioritized risk scenarios • Control approach • Control plan

A detailed description of the SERA Method, including example outputs, is provided in Appendix A. The raw data produced by our application of the SERA Method for this study is presented in Appendix B.

2.2 Conducting the CMSP WEA Study

The CMSP WEA study described in this report was conducted by a team of SEI cybersecurity experts (i.e., the authors of this report) who served as the SERA Analysis Team. The following activities were performed during this study:

- *Review WEA documentation*—collected and reviewed several documents that describe WEA processes and technologies. A summary of the documents reviewed is provided in Section 3.
- *Conduct the SERA Method*—the information from the documents was used as input to the SERA Method. The four SERA tasks were completed based on the information provided in the documents.
- *Review initial results with SMEs*—reviewed initial results (operational models and risk data) with a variety of SMEs, including representatives from large and small carriers, FEMA, the FCC, the Communications Security, Reliability and Interoperability Council (CSRIC) and the Competitive Carriers Association (CCA).
- *Update results based on comments received*—based on the feedback provided by the SMEs, the research team updated and refined the operational models and risk data to produce the final results. This report presents those results.

Sections 3–5 present a summary of this study's core findings. Section 3 begins by describing the CMSP operational environment. The research team described seven distinct models, where each model examines a different facet of the CMSP operational environment. Collectively, these models establish a baseline of operational performance for CMSPs. Security risks were then analyzed in relation to this baseline. Section 4 describes four risk scenarios identified and analyzed for this study. Finally, Section 5 presents the CMSP Security Guidelines, comprising 35 high-priority security controls that address the four WEA risk scenarios.

3 CMSP Operational Environment

The first task of the SERA Method is to develop explicit models of the target operational environment. Developing and documenting operational models enable analysts to establish how technologies and processes are supposed to support the operational mission. By understanding how selected technologies and processes are designed to work, analysts can begin to think about ways that others may subvert the intended mission. The SERA Method defines a structured approach for constructing and analyzing complex, cyber-based risk scenarios intended to prevent mission success. Operational models provide the foundation for developing risk scenarios.

This section presents the operational models developed for the CMSP WEA environment. The process of developing operational models starts by reviewing several WEA documents, including

- *Joint ATIS/TIA CMAS Mobile Device Behavior Specification* [ATIS 2009b]
- *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification* [ATIS 2009a]
- *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Text Specification* [ATIS 2011]
- *Commercial Mobile Alert System (CMAS) Concept of Operations (CONOPS) Version 1.0* [FEMA 2009]
- *Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN), v3.07* [FEMA 2014]
- *Commercial Mobile Alert Service Architecture and Requirements, v 1.0* [NPSTC 2007]

The information from the documents was used to develop a set of prototype operational models for the CMSP environment. Once a set of prototype models was completed, the research team met with several SMEs from the following organizations to review the models and receive feedback. The SMEs were from a variety of large and small commercial carriers, FEMA, the FCC, the CSRIC and the CCA. Based on the feedback received, the following models were updated and refined:

- WEA top-level workflow
- WEA system of systems
- CMSP workflow
- selected CMSP architecture
- CMSP dataflow
- data security attributes
- stakeholders

Each model is presented in this section, beginning with the WEA top-level workflow.

3.1 WEA Top-Level Workflow

An *emergency alert* is a message sent by an authorized organization. It provides details of an occurring or pending emergency situation to one or many designated groups of people. Emergency alerts are initiated by many diverse organizations. For example, law enforcement organizations issue America's Missing: Broadcast Emergency Response (AMBER) alerts, and the National Weather Service (NWS) issues weather alerts. Both AMBER alerts and weather alerts are examples of emergency alerts. A *wireless alert* is an emergency alert that is sent to mobile devices, such as cell phones and pagers. Figure 3 shows the top-level workflow model that we developed for the WEA service.

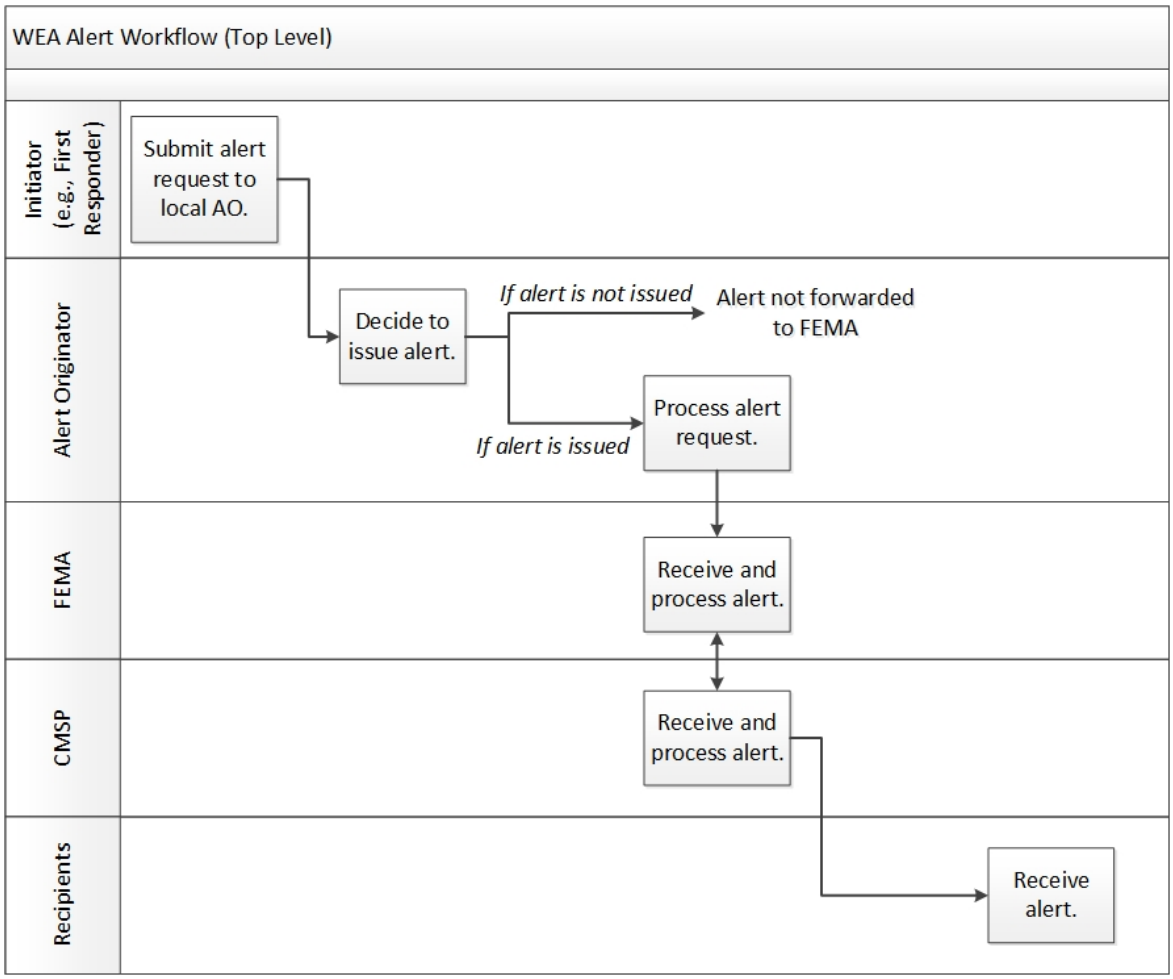

Figure 3: WEA Top-Level Workflow

The figure shows the sequence of activities required to issue a wireless alert. A swim-lane diagram[1] was used to document the workflow. The activities in a swim-lane diagram are grouped visually by placing

[1] A swim-lane diagram provides a visual representation of a workflow or mission thread [Sharp 2001]. It defines the sequence of end-to-end activities that take place to achieve a specific result as well as who performs each activity. Swim-lane diagrams are especially useful for describing workflows or mission threads that cross organizational boundaries, which is a characteristic of system-of-systems environments. Because we are focusing on system of systems environments in our research, we have found swim-lane diagrams to be a useful workflow modeling technique.

them in lanes. Parallel lines divide the diagram into multiple lanes, with one lane for each workflow actor (i.e., person, group or subprocess). Each lane is labeled to show who is responsible for performing the activities assigned to that lane. In Figure 3, the gray boxes with solid borders represent the activities that are performed by each workflow actor. Lines connecting the activities establish the relationships among and sequencing of the activities.

The workflow begins with a request from an initiator, such as law enforcement or the NWS, to submit an alert (*initiator alert request*). A team from the AO organization receives the initiator alert request and decides (1) whether or not to issue the alert and (2) the distribution channels for the alert (e.g., television, radio, roadside signs, and wireless technologies). The workflow in Figure 3 assumes that a wireless alert will be issued.

The emergency alert is sent to FEMA systems, which process and format the alert before sending it to CMSP systems. Then CMSP systems receive the emergency alert and format it for the technologies used in the geographic area covered by the alert. The emergency alert is then sent through the CMSP infrastructure to WEA-enabled mobile devices in the designated geographic area.

3.2 WEA System of Systems

The top-level workflow in Figure 3 provides the anchor for the subsequent security risk analysis. After we develop a workflow model, it is then determined which technologies support that workflow. The systems that support the WEA workflow are shown in Figure 4. In essence, the collection of systems in Figure 4 depicts the WEA system of systems.[2] These systems support the end-to-end WEA workflow and are the starting point for a deep dive into an analysis of WEA support technologies.

The following are highlights of the WEA system of systems depicted in Figure 4:

- *Initiator systems*: Communication of alert information between the initiator and AO can use the following technologies: telecommunications (for verbally communicating requests) and unencrypted email from the initiator's desktop computers.
- *AO systems*: The AO uses three systems: telecommunications, AO desktop computers and the alert originating system (AOS). The AO relies on the following technologies to receive requests to issue an alert: telecommunications (for verbally receiving requests) and unencrypted email sent from an initiator's desktop computer to AO desktop computers.[3] After AO management decides to issue a wireless alert, an AO operator enters the alert into the AOS, which then forwards the CAP-compliant alert message and the AO certificate to the IPAWS-OPEN Gateway (i.e., a FEMA system).
- *FEMA systems:* The IPAWS-OPEN Gateway receives the alert message, validates the sender using the AO certificate and forwards the alert to the WEA Aggregator for processing. The WEA Aggregator processes the wireless alert and transmits it to the Federal Alert Gateway, which then sends the alert message to the CMSP Gateway.

---

[2] A *system of systems* is defined as a set or arrangement of interdependent systems that are related or connected (i.e., networked) to provide a given capability [Levine 2003].

[3] Data from AO desktop computers cannot be sent over the network to the AOS. Operators must use removable media, such as USB drives, to exchange data between these two systems.

- *CMSP systems*: The CMSP Gateway receives the alert message and then forwards it to the CMSP infrastructure (e.g., cell towers). The alert message is transmitted by the CMSP infrastructure to capable wireless devices in the designated area(s).
- *Recipient systems:* People in the designated area(s) who have devices capable of receiving wireless alerts receive the message on their wireless devices.

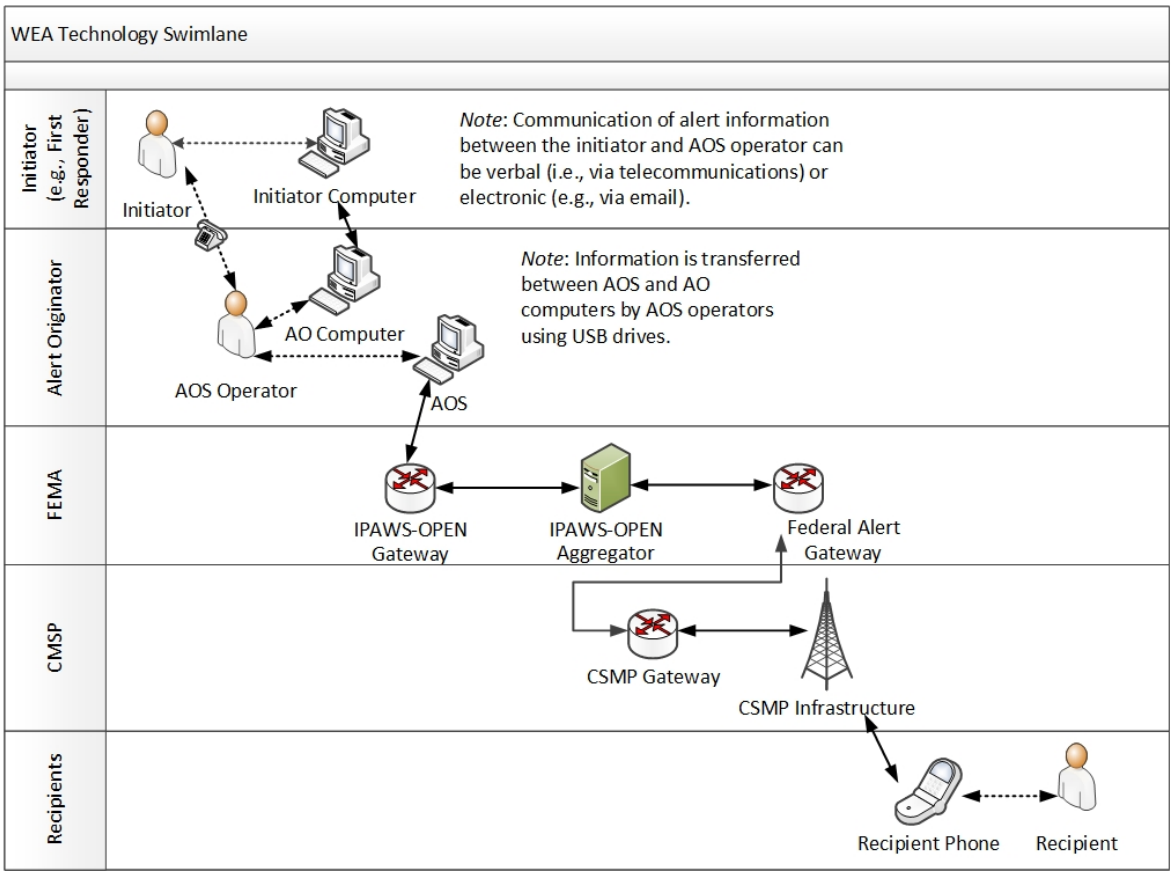

Figure 4: WEA System of Systems

3.3 CMSP Workflow

Figure 5 depicts the CMSP workflow, including the interfaces with FEMA systems and recipients' mobile devices. The CMSP workflow in Figure 5 provides additional details not shown in the top-level workflow of Figure 3. These details are important to understand when identifying threats to the CMSP WEA alerting system. (In the context of this risk analysis, the CMSP WEA alerting system comprises the CMSP Gateway as well as several devices throughout the CMSP infrastructure that support the WEA service.)

The CMSP workflow begins with processing that is performed by FEMA systems. Here, the IPAWS-OPEN Aggregator converts the CAP-compliant alert message into CMAC format. If the conversion fails, the alert is not sent to the CMSP, and the scenario ends. If the conversion is successful, the CMAC alert is then sent to the Federal Alert Gateway, which interfaces directly with the CMSP Gateway. The

Federal Alert Gateway sends the CMAC-formatted alert message to the CMSP Gateway over the designated interface (called Reference Point C).

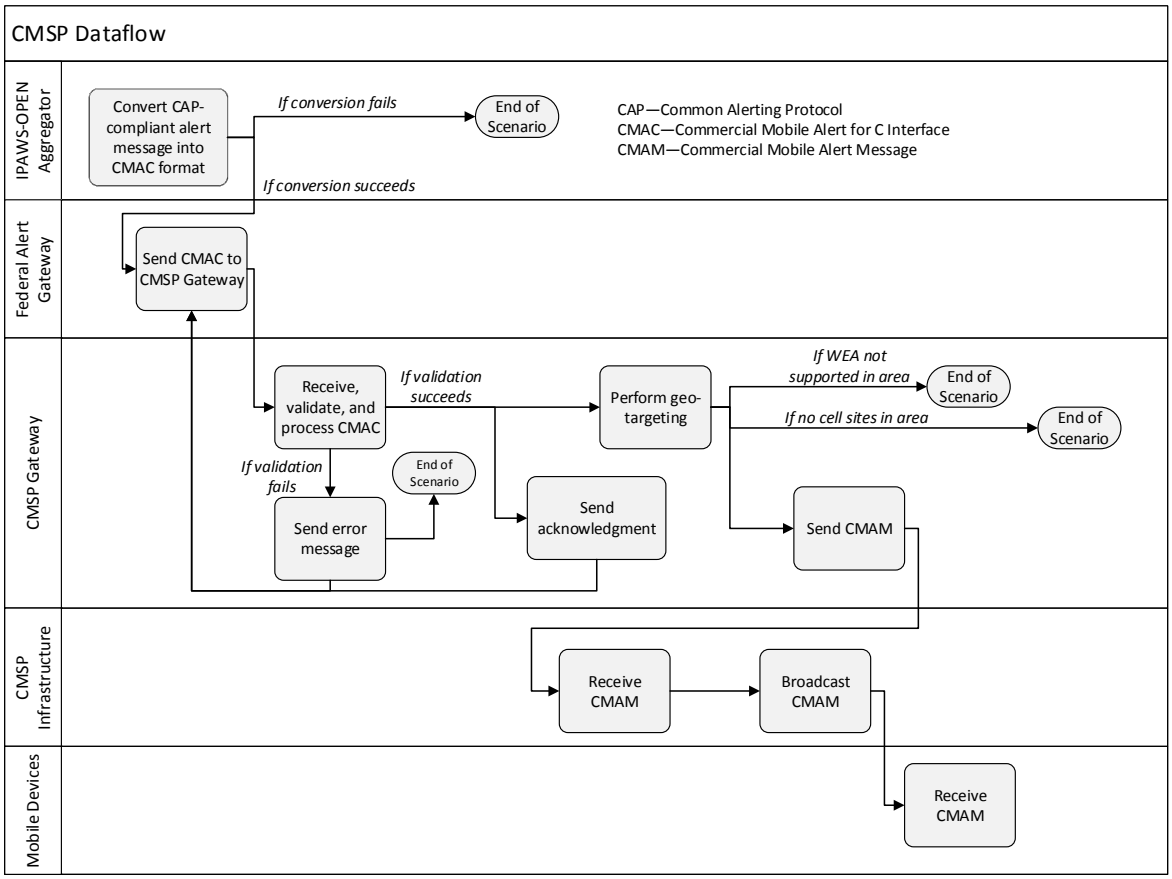

Figure 5: CMSP Workflow

Next, the CMSP Gateway receives and validates the CMAC alert. If the CMAC alert is not validated, the CMSP Gateway sends an error response to the Federal Alert Gateway. At this point, the CMAC alert is not broadcast by the CMSP Gateway, and the scenario ends. If the CMAC alert is validated, the CMSP Gateway sends an acknowledgment to the Federal Alert Gateway and begins processing the alert.

The CMSP Gateway performs geo-targeting to translate the indicated alert area into the associated set of mobile device technologies (e.g., cell towers) in the alert's designated geographic area. If WEA is not supported in the designated geographic area or if the CMSP does not have any cell sites in the area, then an alert is not sent. Otherwise, the CMSP Gateway coverts the alert into Commercial Mobile Alert Message (CMAM) format and sends it to the appropriate technologies in the CMSP infrastructure.

Technologies in the CMSP infrastructure receive the CMAM alert and broadcast it to mobile devices in the designated geographic area. Mobile devices monitor for the broadcast of CMAM alerts. WEA-enabled mobile devices in the geographic area receive the CMAM-formatted alert message and present the alert to the end user. The presentation of an alert includes activation of the WEA audio tone and vibration cadence (if the mobile device has vibration capabilities) for a short duration.

3.4 Selected CMSP Architecture

The technical architecture selected for this analysis is shown in Figure 6. The subsequent security risk analysis is based on the technical architecture illustrated in this figure. This architecture is typical of those implemented by larger carriers. CMSPs that implement different architectures will need to interpret and adjust this report's security guidelines appropriately.

As shown in the architecture diagram, the Federal Alert Gateway interfaces directly with the CMSP Gateway. The interface between the two systems is called the Reference Point C interface [ATIS 2009a]. The Federal Alert Gateway can send emergency alerts (alert,[4] update,[5] cancel[6]) and test messages to the CMSP Gateway. Alert, update and cancel messages are triggered when the Federal Alert Gateway receives a CAP-compliant message. If the CAP-compliant message is validated and translated successfully into the CMAC format, a CMAC message will be sent to the CMSP Gateway.

Nonrepudiation is defined as the ability to ensure proof of the integrity and origin of data. For data security purposes, nonrepudiation requires a mechanism that prevents the sender of a message from later denying having sent the message. The interface between the Federal Alert Gateway and the CMSP Gateway uses Extensible Markup Language (XML) digital signatures to enforce nonrepudiation. The Federal Alert Gateway digitally signs each CMAC message. (The XML signature is not permitted for other types of messages.) The certificate used for this digital signature is issued to the Federal Alert Gateway hardware (i.e., not to a human user). The CMSP Gateway can use the digital signature for nonrepudiation, or it can ignore the digital signature.

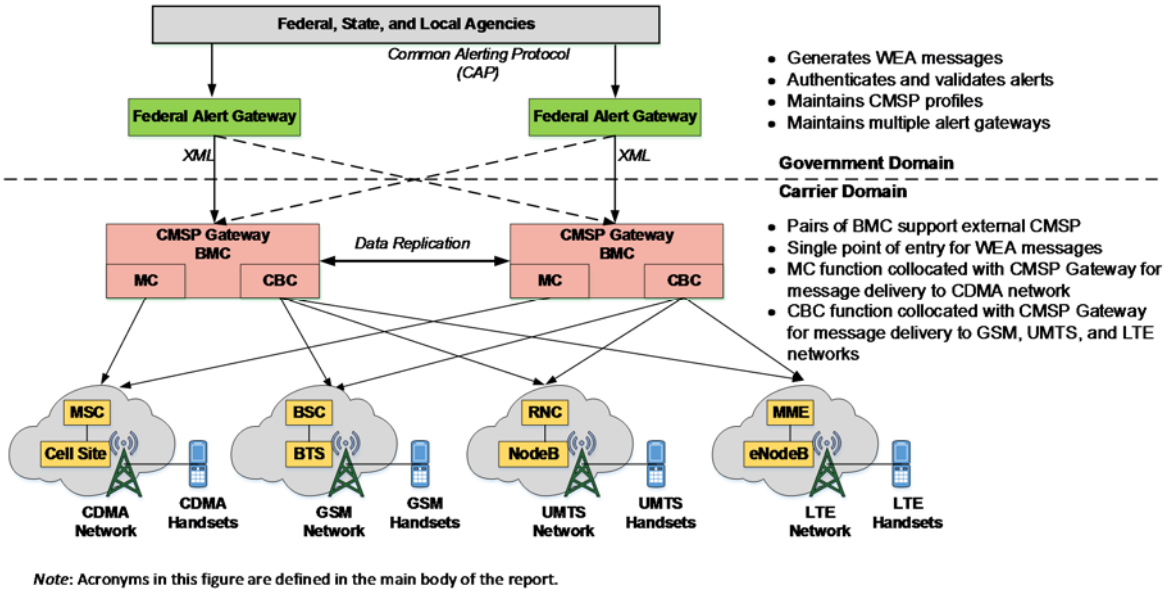

Figure 6: Selected CMSP Architecture

[4] *Alert* indicates that a new alert is being issued.

[5] *Update* indicates that a previously issued alert is being revised or amended.

[6] *Cancel* indicates that a previously issued alert is being withdrawn.

The CMSP Gateway shown in Figure 6 includes a Broadcast Message Center (BMC) application that supports message broadcasts to mobile devices in a specified geographic area. Typically, geographic areas can be defined using a geographic shape (i.e., polygon) or can be mapped to specific broadcast zones containing a group of cells or sectors within the CMSP's network. The CMSP Gateway depicted in the figure includes a mated pair of BMCs, for data replication, that supports the CMSP Gateway functions. Overall, the CMSP Gateway provides a single point of entry for WEA messages for the CMSP network.

The architecture illustrated in Figure 6 supports the following four delivery technologies:

- *Code Division Multiple Access (CDMA) networks*: A Message Center (MC) function is collocated with a CMSP Gateway for message delivery to CDMA networks. The gateway's MC function interfaces with Mobile Switching Centers (MSCs) in CDMA networks. The interface standard between the MC and CDMA networks is the IS-824, IS-637 SMDPP.
- *Global System for Mobile Communications (GSM) networks*: A Cell Broadcast Center (CBC) function is collocated with a CMSP Gateway for message delivery to GSM networks. The gateway's CBC function interfaces with Base Station Controllers (BSCs) in GSM networks. The interface standard between the CBC and GSM networks is 3GPP 23.041 CBS-BSC.
- *Universal Mobile Telecommunications System (UMTS) networks*: A CBC function is collocated with a CMSP Gateway for message delivery to UMTS networks. The gateway's CBC function interfaces with Radio Network Controllers (RNCs) in UMTS networks. The interface standard between the CBC and UMTS networks is 3GPP 25.419 lu-BC.
- *Long-Term Evolution (LTE) networks*: A CBC function is collocated with a CMSP Gateway for message delivery to LTE networks. The gateway's CBC function interfaces with Mobility Management Entities (MMEs) in LTE networks. The interface standard between the CBC and LTE networks is 3GPP 29.168 SBc.

For the application of the SERA Method to CMSPs, the WEA alerting system was identified as the system of interest for the analysis (i.e., the main focus of the security risk analysis). Based on Figure 6, the WEA alerting system comprises (1) the CMSP Gateway and (2) devices throughout the carrier's infrastructure that support the WEA service, including devices in the CDMA, GSM, UMTS and LTE networks.

3.5 CMSP Dataflow

Figure 7 shows data assets that are stored, processed and transmitted during the execution of the CMSP workflow. The following data assets are highlighted in Figure 7:

- *CAP-compliant alert message*—the alert message in CAP format
- *CMAC message*—the alert message in CMAC format (as specified by the interface between the Federal Alert Gateway and the CMSP Gateway)
- *Acknowledgment*—a notification sent from the CMSP Gateway to the Federal Alert Gateway that the CMAC alert has been received and validated
- *CMAM message*—the alert message in CMAM format
- *Geo-targeting data*—the geographic area covered by the alert

- *Validation trigger*—a trigger for the CMSP Gateway to send an acknowledgment to the Federal Alert Gateway that the CMAC alert has been validated
- *Cell sites*—the cell sites in the designated geographic area that will received the CMAM alert

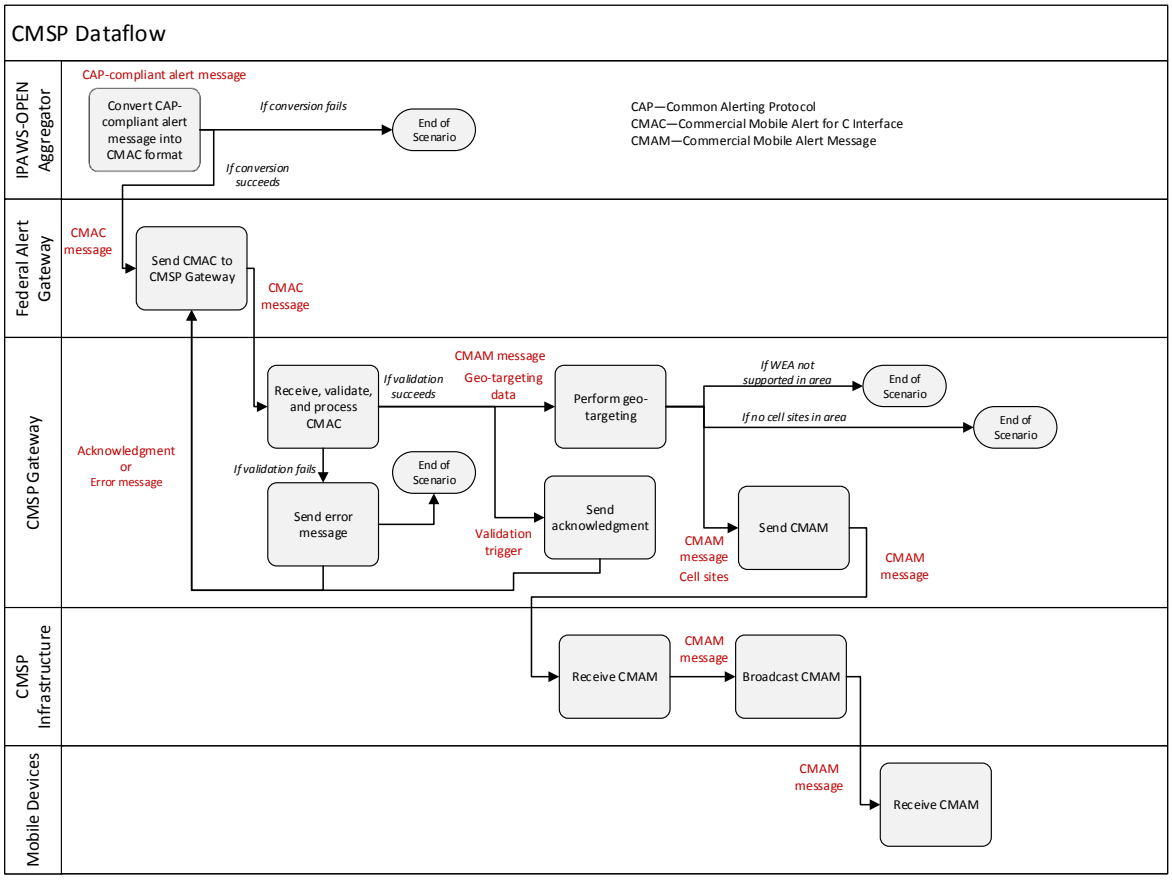

Figure 7: CMSP Dataflow

Based on cybersecurity experience, the following critical data assets were selected as potential targets by a threat actor:

- CAP-compliant alert message
- CMAC message
- CMAM message
- Geo-targeting data

Data security attributes were documented for each critical data asset.

3.6 Data Security Attributes

The SERA Method requires specifying the following security attributes[7] for each critical data asset:

- *Confidentiality*—the requirement of keeping proprietary, sensitive, or personal data private and inaccessible to anyone who is not authorized to see it
- *Integrity*—the authenticity, accuracy, and completeness of a data asset
- *Availability*—the extent to which, or frequency with which, a data asset must be resent or ready for use

Table 2 features the following information for each critical data asset: description of the data asset, the form of the data asset (e.g., electronic or physical) and requirements for confidentiality, integrity and availability.

Table 2: Data Security Attributes

Data Asset	Description	Form	Confidentiality	Integrity	Availability
CAP-compliant alert message	The alert message in CAP format.	Electronic	There are no restrictions on who can view this data asset (public data).	The data asset must be correct and complete (high data integrity).	This data asset must be available when needed (high availability).
CMAC message	The alert message in CMAC format (as specified by the interface between the Federal Alert Gateway and the CMSP Gateway).	Electronic	There are no restrictions on who can view this data asset (public data).	The data asset must be correct and complete (high data integrity).	This data asset must be available when needed (high availability).
CMAM message	The alert message in CMAM format.	Electronic	There are no restrictions on who can view this data asset (public data).	The data asset must be correct and complete (high data integrity).	This data asset must be available when needed (high availability).
Geo-targeting data	The geographic area covered by the alert.	Electronic	There are no restrictions on who can view this data asset (public data).	The data asset must be correct and complete (high data integrity).	This data asset must be available when needed (high availability).

Data security attributes indicate what qualities of a data asset are important to protect. Security attributes also provide insight into a cyber attacker's goal. Table 2 indicates that confidentiality is not considered to be an important attribute of the four critical data assets because these data assets are considered to be public information. Integrity and availability are important attributes of the data assets, however. As a result, threat actors that target the CMSP WEA alerting system will likely focus on violating the integrity and availability attributes of the critical data assets.

[7] The definitions for confidentiality, integrity and availability come from *Managing Information Security Risks: The OCTAVE℠ Approach* [Alberts 2002].

3.7 Stakeholders

As used in this report, a *stakeholder* is a person, group or organization that is interested in or concerned about a workflow or mission thread and its associated objectives. Table 3 defines the mission interests of selected WEA stakeholders. The immediate, or direct, outcome (i.e., consequence) of a threat describes how a critical data asset is affected (i.e., how its security attributes have been violated). Examples of direct outcomes or consequences include data disclosure, data modification, insertion of false data, destruction of data and interruption of access to data.

Table 3: Stakeholders

Stakeholder	Mission Interest
FEMA	Transmit alert messages to carriers within a required time frame and maintain trust in WEA and the overall EAS
Carrier	Deliver alert messages to customers as rapidly as possible without adversely affecting customer satisfaction Implement best security practices to reduce risk of security incidents (and avoid additional mandated security regulations)
Recipients	Receive and act on WEA messages

The direct consequence of a threat can also trigger a range of indirect consequences. These indirect consequences typically affect (1) selected workflows or mission threads and (2) interested stakeholders. Workflow consequences are determined by analyzing workflow models (such as the CMSP workflow shown in Figure 5). Stakeholder consequences are determined by considering the mission interests of stakeholder groups and determining how those interests might not be met, based on the projected consequences to the workflow or mission thread. As a result, stakeholder models (such as the one shown in Table 3) are an important input when analyzing the consequences of security risks.

The models featured in this section were used to establish a baseline of operational performance. Security risks were then identified and analyzed in relation to this baseline. The next section highlights the four risk scenarios analyzed during this study.

4 CMSP Risk Scenarios

This section presents four risk scenarios that we included in the study. Once each scenario was developed, it was then analyzed it to determine its probability of occurrence and impact on the WEA service if the scenario were realized. This information was used to prioritize the risks and determine which need to be controlled. This prioritized ranking of the risk scenarios provides a basis for implementing administrative, technical and physical security controls.

Appendix A describes the SERA Method used to identify and analyze cybersecurity risk scenarios for the CMSP WEA alerting system. A complete set of data for each risk scenario is presented in Appendix B. This section summarizes the results of applying the method, focusing on the four risk scenarios. Based on the team's collective cybersecurity experience and expertise, the following risk scenarios were selected to analyze in detail:

- Risk 1: Insider Sends False Alerts
- Risk 2: Inherited Replay Attack
- Risk 3: Malicious Code in the Supply Chain
- Risk 4: Denial of Service

These scenarios provide a broad cross section of the types of issues likely to affect the CMSP WEA alerting system. The underlying threats that trigger these four risks include an insider (Risk 1), the consequences of an upstream attack on an AO (Risk 2), malicious code inserted in the CMSP supply chain (Risk 3) and a denial-of-service attack (Risk 4). Although not exhaustive, the resulting analysis provides a broad range of mitigation requirements that CMSPs should consider. The remainder of this section describes each risk scenario in detail and highlights the SEI team's ranking of those scenarios based on the results of the risk analysis.

4.1 Risk 1: Insider Sends False Alerts

An insider is employed by a wireless carrier. The insider is a software developer and is responsible for developing applications that support the company's wireless infrastructure. The insider is upset that he will not receive a bonus this year and also has been passed over for a promotion. Both of these perceived slights anger the insider. As a result, he begins to behave aggressively and abusively toward his coworkers. For example, he downplays their achievements, brags about his own abilities, takes credit for the work of others and delays progress on projects. The insider's anger builds over time until he finally convinces himself to take action against the carrier.

His plan is to plant a logic bomb in the CMSP Gateway, hoping to send "custom" WEA messages to all WEA-capable wireless devices supported by the carrier. His ultimate goal is to bring negative publicity to the company. As a function of his job, the insider has unlimited access to the company's software code and is able to modify the company's code at will. While on site and during work hours, the insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.

The insider shares an office with another software developer, who often leaves her workstation unlocked when she is out of the office. The insider uses his colleague's workstation to check in the

modified code with the logic bomb. Seven months later, the insider voluntarily leaves the company for a position in another organization. Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically. The malicious code causes the carrier's WEA service to send a nonsense WEA message repeatedly to people across the country.

Many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier's customer service operators. A large number of recipients turn off the WEA function on their phones in response to the attack.

The carrier responds to the attack by taking the infected CMSP Gateway offline. The broadcast of the illegitimate messages stops. The carrier then responds aggressively to the attack by investigating the source of the attack, locating the malicious code and removing that code from its infrastructure. Once the malicious code is removed from the CMSP Gateway, the carrier brings the CMSP Gateway back online. The cost to recover from the attack is considerable.[8]

As a result of the attack, some customers leave their carrier for other carriers. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

The overall risk exposure of this scenario is low. This scenario has a remote probability of occurrence because it is reasonably complex and requires considerable preparation to execute. A disgruntled insider must have physical access to a workstation that can update CMSP production code, which limits the number of potential attackers. In addition, the disgruntled insider must have the technical skills needed to execute the attack and must be familiar with the CMSP Gateway. Field experience indicates that the number of cyber attacks by disgruntled insiders continues to grow across all sectors, however. As a result, an insider attack like this is not considered to be a rare event.

The consequences of this risk scenario are moderate in severity. Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of business. Carriers already maintain help desk capabilities to respond to customer complaints, which helps with the response to this attack. In addition, tech-savvy customers can turn off the WEA service and eliminate the annoyance.

4.2 Risk 2: Inherited Replay Attack

An attacker targets an AO to capture legitimate WEA messages (unencrypted) and their associated AO certificates (encrypted) during transmission. She intends to resend a legitimate alert repeatedly at a later time (i.e., a replay attack), hoping to annoy people who use the WEA service. The attacker captures multiple WEA messages and selects one that will affect a large number of people, based on the geographic area targeted by the alert message.

[8] The experience of SMEs related to malicious code indicate that the typical costs to find and remove malicious code from a networked environment are *considerable*, a term used in this report to refer to all of the external and internal costs to recover from a cyber attack. External cost factors can include business disruption, information loss or theft, revenue loss and equipment damages. Internal cost factors can include funds required for detection, investigation and escalation, containment, recovery and subsequent efforts to ward off future attacks.

At a later time, the attacker executes a replay attack using the captured WEA message (i.e., now considered to be an illegitimate alert). She sends the illegitimate alert (unencrypted) and associated AO certificate (encrypted) to IPAWS-OPEN, which then performs the following activities:

- accepts the illegitimate alert
- confirms the source as legitimate using the AO certificate
- processes the illegitimate alert
- forwards the illegitimate alert to the CMSP Gateway along with the appropriate certificate

The attacker then repeatedly sends the same illegitimate alert to IPAWS-OPEN, which processes each alert and forwards it to the CMSP Gateway. Each illegitimate alert is accepted by the CMSP Gateway and validated as being legitimate.

The CMSP Gateway converts each illegitimate message to CMAM format, performs geo-targeting of each message and sends each illegitimate message to designated cell sites. Each illegitimate CMAM message is received by cell sites, which then broadcast the CMAM message to mobile devices. As a result of this attack, people receive the same illegitimate alert repeatedly on their mobile devices.

Many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier's customer service operators. A large number of recipients turn off the WEA function on their phones in response to the attack.

The carrier responds to the attack by restricting messages temporarily from the Federal Alert Gateway. The carrier works with FEMA and the AO to resolve the upstream issues that led to the attack. Once the upstream issues are addressed, the carrier allows messages from the Federal Alert Gateway to be received and processed.

As a result of the attack, some customers leave their carrier for other carriers. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

The overall risk exposure of this scenario is low. This scenario has a remote probability of occurrence because the triggering attack (i.e., the attack on the AO) is moderately complex, requires technical skills and requires moderate preparation to execute. The large number of AOs across the country provide numerous targets for the triggering attack, however. In addition, AOs have varying degrees of security controls in place. Some AOs (and their AOS vendors) likely have implemented effective security controls, while others likely have not. An attacker can look for a weak link with respect to security controls (and most likely find one).

The consequences of this risk scenario are medium in severity. Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of business. Carriers already maintain help desk capabilities to respond to customer complaints, which helps with the response to this attack. In addition, tech-savvy customers can turn off the WEA service. Field experience indicates that the costs required to recover from this attack will not be excessive.

4.3 Risk 3: Malicious Code in the Supply Chain

An employee at a subcontractor of a carrier's WEA alerting system vendor has followed the pursuits of the attacker community for some period of time. He gets excited thinking about executing attacks like those that he follows online. One day, the subcontractor's employee becomes upset at a perceived slight from some of the carrier's employees during a technical exchange. He does not believe that that the carrier's technical staff has shown him the respect that he is due. As a result, he decides to execute an attack against the carrier.

The subcontractor's employee (hereafter referred to as the actor) performs reconnaissance to obtain subcontractor and vendor artifacts that describe the carrier's WEA alerting system, such as requirements specifications, architecture and design documents, and source code. The actor gains access to artifacts that provide technical details of the carrier's WEA alerting system. He studies the documents in great detail, looking for any weaknesses that he can exploit. Finally, the actor develops an attack strategy. He intends to develop malicious code designed to (1) disseminate an alert as broadly as possible (i.e., override the system's geo-targeting capability) and (2) change the priority of all alerts into Presidential alerts. After much effort, he successfully develops the malicious code.

The actor intends to plant the malicious code in a software update that the subcontractor is developing for the carrier's WEA alerting system. Hoping to cover his tracks when executing the attack, the actor intends to plant the malicious code using credentials (e.g., user ID and password) that he will steal from a colleague. The actor uses password cracker software (such as L0phtCrack) to retrieve passwords for user accounts on the subcontractor's development system. The actor then accesses the development system using a colleague's user ID and password that he has stolen. He inserts the malicious code into a software update for the carrier's WEA alerting system.

The subcontractor's technical staff completes development and testing of the software update, with the inserted malicious code, and delivers it to the vendor. Technical staff from the vendor's development team do not detect the malicious code during testing and accept the software update. The vendor then integrates the subcontractor's software update into the latest version of the WEA alerting software. Acceptance testing by the carrier does not detect the malicious code, and the latest version of the WEA alerting software, with the malicious code, is deployed in the carrier's infrastructure.

The malicious code waits until the carrier receives an alert from the CMSP Gateway. When an alert is received, the malicious code expands the region receiving the alert as broadly as possible and changes the priority of the alert into a Presidential alert.

Recipients receive and read the alert on their wireless devices. Recipients outside of the region covered by the actual alert become annoyed at receiving an alert designated for another geographic area. In addition, some recipients become alarmed by receiving a Presidential alert. Many recipients try to turn off the WEA function on their phones. This does not work because people cannot opt out of receiving a Presidential alert. Thus, many people continually receive Presidential alerts related to severe weather affecting other counties or states. Many recipients complain to the carrier's customer service operators.

The carrier responds to the attack by taking the infected WEA alerting system offline. The broadcast of the Presidential alerts stops. The carrier then responds aggressively to the attack by investigating the source of the attack, locating the malicious code and removing that code from its infrastructure. Once

the carrier has removed the malicious code from its WEA alerting system, the carrier brings the system back online. The cost to recover from the attack is considerable.

As a result of the attack, some customers leave their carrier for other carriers. Because of the high-profile nature of the attack (i.e., issuing illegitimate Presidential alerts), the media covers the attack extensively. The media coverage of the attack helps to amplify the public's loss of trust in the WEA service.

The overall risk exposure of this scenario is minimal. This risk scenario has a rare probability of occurrence because the scenario is considered to be uncommon or unusual. This is a very sophisticated, complex attack that requires significant technical skills and considerable preparation to execute. Not many people have the combination of technical skills and motivation to conduct this type of attack.

The consequences of this risk scenario are medium in severity. The organization will be able to recover from the attack by investing organizational capital and resources.

4.4 Risk 4: Denial of Service

An outside actor with malicious intent is planning a physical (i.e., terrorist) attack on a crowd that is gathered in a public place (e.g., for a sporting event or concert). She plans to conduct a simultaneous denial-of-service (DoS) attack on a carrier's WEA alerting system to prevent the dissemination of a WEA message about the attack. The goal is to prevent people from learning about the physical attack as long as possible to maximize the physical harm inflicted upon the crowd.

Because the carrier is known to employ rigorous cybersecurity practices, the actor decides to target one of the carrier's business partners with trusted access to the carrier's internal network. She performs reconnaissance on the carrier to determine which business partners might make good targets for an attack. This involves examining publicly available information about the carrier and its business partners, as well as attempts to gain information from the carrier's employees through social engineering.

Based on the information acquired through various reconnaissance activities, the actor decides to target a third-party contractor that has legitimate access to the carrier's internal network. She performs additional reconnaissance on the contractor's infrastructure to obtain information needed to gain access. The contractor is not vigilant about its cybersecurity practices, making it a relatively easy target for an attacker.

The actor exploits several well-known vulnerabilities in the contractor's perimeter security and gains access to a computer in the contractor's internal network. She then uses this access to perform additional reconnaissance of the contractor's internal network. Jumping from computer to computer until she gains access to a specific contractor system that has trusted access to the carrier's infrastructure, the actor uses the contractor's trusted access to bypass the carrier's perimeter security controls. She performs reconnaissance on the carrier's internal network to obtain information needed for targeting the WEA alerting system. The actor scans the carrier's internal network for vulnerable computers and then exploits vulnerabilities to gain access to those computers. She installs malicious code on the vulnerable computers that will be used to initiate the DoS attack. The cyber component of the attack is ready.

The actor initiates the physical attack. At the same time, the actor instructs the infected computers to send a flood of requests to the carrier's WEA alerting system, which consumes the system's available bandwidth. An AO (e.g., from law enforcement) enters a legitimate WEA message into its AOS. The

legitimate WEA message is transmitted to the carrier's computing infrastructure from the CMSP Gateway. The carrier's WEA alerting system is unable to process the legitimate alert because the system's bandwidth is consumed by the DoS attack, however.

People are put in harm's way from the physical attack, leading to injuries and death. The carrier tries to mount a response to the attack. It eventually disseminates the alert through other available channels. Because of the DoS attack, however, people do not receive the WEA message in a timely manner. As a result, people at the event are unaware of what is happening and do not react, leading to additional harm.

After the attack, the carrier removes the malicious code from its infrastructure. As part of its recovery plan, the carrier terminates its relationship with the contractor that was responsible for the DoS attack. The carrier also begins more rigorous auditing of the security practices of all organizations with whom it has contractual relationships. The carrier updates its contracting language to be more specific about the security obligations of its contractors.

The cost to recover from the attack is considerable. Media outlets learn about the DoS attack's role in amplifying the impact of the incident and publicize this fact in their reports. The carrier receives more than its share of the blame for the consequences of the attack. Ultimately, the court system could hold the carrier liable for financial penalties. In addition, the reputation of the carrier could be damaged with the general public, leading to a loss of business. Finally, many people lose trust in the WEA service.

The overall risk exposure of this scenario is medium. This risk scenario has a rare probability of occurrence. This is a very sophisticated, complex attack that requires significant technical skills and considerable preparation to execute. Not many people have the combination of technical skills and motivation to conduct this type of attack. It also must be timed to coincide with a physical attack. All of these reasons make it a rare event.

The consequences of this risk scenario are maximum in severity due to health and safety issues and loss of life. The carrier may be subject to significant financial penalties (e.g., legal awards) as a result of this attack.

4.5 Prioritized CMSP Risk Scenarios

Under the SERA Method, once the risk scenarios are identified and analyzed, the next step is to prioritize them based on their risk measures (i.e., impact, probability and risk exposure). The following guidelines were used for prioritizing the list of CMSP WEA risk scenarios:

- Impact was the primary factor for prioritizing security risks. Risks with the largest impacts are deemed to be of highest priority.
- Probability was the secondary factor for prioritizing security 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.

The prioritized risk spreadsheet is shown in Table 4.

Table 4: Prioritized Risk Spreadsheet with Control Decisions

ID	Risk Statement	Impact	Probability	Risk Exposure	Control Approach
R4	**Denial of Service** **IF** an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, **THEN** people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Maximum	Rare	Medium	Plan
R1	**Insider Sends False Alerts** **IF** an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Remote	Low	Plan
R2	**Inherited Replay Attack** **IF** the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, **THEN** customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Remote	Low	Plan
R3	**Malicious Code in the Supply Chain** **IF** malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Rare	Minimal	Plan

The table also includes the control approach for each risk scenario. Here, we determined how to handle each risk scenario. If a scenario is accepted, its consequences will be tolerated; no proactive action to address the risk will be taken. If a decision is made to take action to control a risk, a control plan will be developed for that risk scenario. The following guidelines were used to determine when to develop a control plan: *any risk with an impact of medium or greater should be controlled*. As a result, control plans for all four risk scenarios were developed.

The detailed control plan for each risk scenario is documented in Appendix B. The next section presents the CMSP Security Guidelines derived from the four control plans.

5 CMSP Security Guidelines

CMSP Security Guidelines are a set of high-priority security controls that a CMSP should consider implementing to protect its WEA alerting system. These guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study. Security controls in the following areas were identified:

- human resources
- training
- contracting
- physical security
- change management
- access control
- information management
- vulnerability management
- system architecture
- system configuration
- code analysis
- technical monitoring
- independent reviews
- incident response
- disaster recovery

While this section provides an overview of the CMSP Security Guidelines, additional details related to the guidelines are located in the appendices of this report. Appendix B, examines how the controls can be used to address all threat steps and consequences for each risk scenario. Appendix C overviews which controls map to each risk scenario. Finally, Appendix D contains a control strategy questionnaire that a CMSP can use to evaluate the security posture of its WEA alerting system. The remainder of this section presents high-priority security controls for each identified area, beginning with human resources.

5.1 Human Resources

The human resources function of an organization is responsible for finding, screening, recruiting and training job applicants. It also administers employee-benefit programs, conducts performance appraisals and oversees performance-based rewards. From a security perspective, human–resource controls are important for mitigating risks from malicious insiders. CMSPs should consider implementing the following human-resource controls:

- The carrier’s managers are trained to provide constructive feedback on performance issues.
- The carrier’s managers recognize inappropriate behavior when it occurs and respond appropriately.

- The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
- Selected employees receive training that is focused on interacting with people from other organizations.

5.2 Training

Training is the process by which an individual is taught the skills needed to perform designated job duties. Security training focuses on teaching personnel about appropriate organizational security practices. As a result, an effective training program can help mitigate a wide variety of security risks. CMSPs should consider implementing the following high-priority training controls:

- All employees are required to attend security awareness training, which addresses the topic of social engineering.
- Selected employees participate in training simulations that include social engineering attacks.

5.3 Contracting

Contracting is the process of developing a formal agreement with a third party to provide a product or service. Security standards and practices should be explicitly defined in an organization's contracting processes. In addition, an organization might decide to contract with a third party for security services. Overall, contracting controls are an important aspect of managing an organization's supply chain. CMSPs should consider implementing the following contracting controls:

- All contracts with third parties specify security standards that must be met across the supply chain.
- All contracts with third parties require third parties to participate in independent security audits when requested.
- All contracts require third parties to immediately notify the carrier when a security incident is detected.
- All contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities.
- All contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code.

5.4 Physical Security

Physical security is the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to an organization and its mission. Physical security countermeasures are designed to protect an organization from threats that require an attacker to gain physical access to an organization's facilities and assets. These threats can include fire, natural disasters, burglary, theft, vandalism and terrorism. CMSPs should consider implementing the following physical-security control:

The carrier implements physical access controls for workstations and workspaces.

5.5 Change Management

Change management is a process of requesting, analyzing, planning, implementing and evaluating changes to a system. If changes to a software-reliant system's code base are not managed appropriately, attackers might be able to insert malicious code into the system's code base undetected. CMSPs should consider implementing the following change-management control:

The carrier implements/improves a change-management/configuration-management system.

5.6 Access Control

Access control is the limiting of access to system and network resources. It grants authenticated users access to specific resources based on organizational policies and the permission level assigned to the user or user group. For restricting access to system and network resources, CMSPs should consider implementing the following control:

The carrier controls access to sensitive information based on organizational role.

5.7 Information Management

As used in this report, information management refers to (1) the collection and management of information from one or more sources and (2) the distribution of that information to one or more audiences. Here, information is viewed as an organizational resource. From a cybersecurity perspective, information should be restricted to specific audiences based on its sensitivity. For example, an organization can designate information as public, for official use only, secret or top secret. Information management includes the definition, use and distribution of information within an organization whether processed by computer or not. CMSPs should consider implementing the following information-management control:

The carrier restricts the dissemination of information based on risk.

5.8 Vulnerability Management

A vulnerability is a flaw or weakness in a software-reliant system that leaves the system open to the potential for exploitation in the form of unauthorized access or malicious behavior (e.g., viruses, worms, Trojan horses and other forms of malware). Vulnerability management is the practice of identifying, classifying, remediating and mitigating cybersecurity vulnerabilities. CMSPs should consider implementing the following controls related to vulnerability management:

- The carrier patches all systems and network devices as appropriate.
- The carrier performs periodic vulnerability assessments.
- The carrier acts on the results of vulnerability assessments (i.e., addresses vulnerabilities).

5.9 System Architecture

System architecture is a conceptual model that defines the structure and behavior of a system. An architectural description is a formal representation of a system organized in a way that enables reasoning about the structures and behaviors of the system. Some security risks can be addressed by designing security controls into a system's architecture. When developing the system architecture, CMSPs should consider implementing the following practices:

- Security controls are implemented in systems and network devices based on cybersecurity risk.
- The carrier's WEA alerting system has a backup capability that uses a separate communication channel.

5.10 System Configuration

In the context of security, system configuration addresses software and system-configuration settings that (1) deal with known security risks and (2) comply with an organization's security policies. CMSPs should consider implementing the following system-configuration control:

The carrier configures its systems and network devices securely

5.11 Code Analysis

Code analysis includes methods, tools and techniques for analyzing code for the presence of security vulnerabilities and malicious code. Examples of code analysis methods, tools, and techniques include static analysis,[9] dynamic analysis[10] and peer reviews.[11] CMSPs should consider implementing the following controls related to code analysis:

- The carrier's technical staff conducts security reviews of source code.
- The carrier's technical staff looks for malicious code in software by running static and dynamic analysis tools prior to accepting software from third parties.

5.12 Technical Monitoring

Technical monitoring refers to the collection and analysis of system and network data to identify suspicious or unusual behavior. Monitoring activities look for a variety of suspicious or unusual behaviors, including unauthorized access, misuse, modification and denial of computer network and network-accessible resources. CMSPs should consider implementing the following technical-monitoring controls:

- The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.

---

[9] *Static analysis* is the examination of software performed without actually executing programs. Static analysis can be performed on either the source code or the object code. It is usually performed by an automated tool, augmented by subsequent human analysis of the tool's output.

[10] *Dynamic analysis* is the examination of software performed by executing programs on a real or virtual processor. Effective dynamic analysis requires the target program to be executed with sufficient test inputs to produce interesting behaviors.

[11] A *peer review* of code is the systematic examination of source code to find and fix mistakes overlooked in the initial development phase.

- The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
- The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.
- The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
- The carrier monitors trusted connections for abnormal activity and responds appropriately.

5.13 Independent Reviews

An independent review is an activity performed by an objective third party to provide insight into an activity's progress, current performance and risks. Independent reviews can be used to assess organizational activities in relation to accepted practice or community standards. They can also be used to assess a product, service or system to ensure that it meets its requirements and fulfills its intended purpose. With respect to cybersecurity, CMSPs should consider implementing the following control for independent reviews:

> The carrier has third parties perform periodic cybersecurity audits to evaluate whether the carrier demonstrates due diligence with respect to cybersecurity.

5.14 Incident Response

Incident response is an organizational practice for detecting, analyzing and responding to cybersecurity events and incidents. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. CMSPs should consider implementing the following incident-response controls:

- The carrier implements an incident response capability to minimize the consequences of the event.
- The carrier switches to a backup WEA alerting system (that uses a separate communication channel) to issue the alert.
- Recipients can disable the WEA service on their mobile devices.
- The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages.

5.15 Disaster Recovery

Disaster recovery is an activity that enables the recovery or continuation of critical technology infrastructures and systems following a natural or human-induced disaster. It defines a practice for returning an organization to a state of normality after the occurrence of a disastrous event. CMSPs should consider implementing the following controls related to disaster recovery:

- The carrier implements a recovery plan to minimize the consequences of the event.
- The carrier is insured for damages produced by cybersecurity breaches.

6 Applying the Results

This section describes how CMSPs can apply the results of this study. The CMSP Security Guidelines are the major output of this study. These guidelines comprise 35 high-priority security controls that a CMSP should consider implementing to protect its WEA alerting system. CMSPs can use these to improve their current security controls. This section begins by exploring the CMSP improvement cycle and then examines how a CMSP can assess itself against the guidelines.

6.1 CMSP Improvement Cycle

A CMSP can use the security guidelines introduced in Section 5 to assess its current security controls and chart a course for improvement. This concept is illustrated in Figure 8.[12]

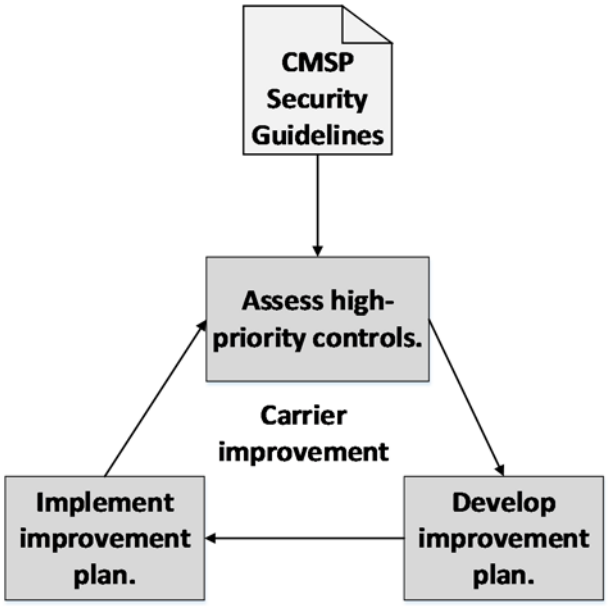

Figure 8: CMSP Improvement Cycle

The CMSP improvement cycle comprises three activities:

1. *Assess high-priority controls:* The CMSP evaluates the extent to which it implements each control specified in the CMSP Security Guidelines.
2. *Develop improvement plan*: The CMSP selects which controls to address (based on resources available and current risk exposure) and then develops an improvement plan for the selected controls.
3. *Implement improvement plan*: The CMSP implements its improvement plan and reduces its exposure to the four risk scenarios featured in this document.

[12] Figure 8 is an excerpt of the big-picture diagram illustrated in Figure 2 of this report.

The remainder of this section focuses on assessing the high-priority controls featured in the CMSP Security Guidelines.

6.2 CMSP Control Survey Questionnaire

Appendix D provides a control strategy questionnaire that CMSPs can use to assess themselves against the CMSP Security Guidelines. Table 5 shows two example questions from that survey. The two examples in the table were derived from two contracting controls included in the guidelines. Each contracting control has been phrased as a yes-no question in the figure. (The survey in Appendix D includes a yes-no question for each of the 35 high-priority controls.)

Table 5: CMSP Survey Question

Category	Control Question	Response			Rationale and Evidence
		Yes	Partial	No	
Contracting	10. Do all contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities?	❑	❑	❑	
	11. Do all contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code?	❑	❑	❑	

The questionnaire establishes relative strengths and weaknesses among the 35 high-priority controls identified for the four risks analyzed in this study. The questions should be answered by an interdisciplinary team with knowledge of the WEA alerting system, the process it supports and the security controls that the CMSP currently implements. The team may not be able to answer all the questions at once. Some investigation and research into available materials and evidence may be needed to reach a correct answer.

The team performs a set of prescribed steps when completing the questionnaire. It starts by selecting a question to answer. Team members then read the question carefully and consider the following responses:

- *Yes*—The answer to the question is yes. The vast majority of the evidence points to an answer of yes. Little or no evidence points to an answer of no.
- *Partial*—The answer to the question is ambiguous. Some evidence points to an answer of yes, while other evidence points to an answer of no. The answer is not a clear-cut yes or no.
- *No*—The answer to the question is no. The vast majority of the evidence points to an answer of no. Little or no evidence points to an answer of yes.

Team members should then discuss the answer to the question. The team selects the most appropriate response (yes, partial or no) and checks the corresponding box in the survey. Next, the team documents the rationale for its response and also documents any supporting evidence. The *rationale* is defined as the underlying reason or basis for the response to the question. *Evidence* is defined as the data on which the rationale is based. When assessing security controls, the team can use different types of evidence, such as the following:

- *Observation*—the action or process of watching someone carefully or in order to gain insight or information. Team members can watch how people perform an activity to determine whether they execute the activity correctly and completely.
- *Artifacts*—any tangible data that is produced when activities are performed. Examples of artifacts include reports from tools (e.g., code analysis tools), security audit reports and tangible project artifacts (e.g., policy statements, project documents, architecture diagrams).
- *Expert opinion*—a view or judgment formed by someone who has expertise and experience in a given field (e.g., cybersecurity). An expert opinion is not necessarily based on facts or data that have been gathered.

Table 6 shows example answers for the two questions from Table 5, including rationale and evidence for each question. The rationales for the two questions are similar. The team has determined that the contract with the vendor for the WEA alerting system does not enable the CMSP to participate in the following activities:

- code reviews
- security testing activities
- reviews of the outputs produced by static and dynamic analysis tools

The evidence cited for both questions is the contract with the vendor. The vendor contract is an example of an artifact that is being used as evidence. It provides tangible, objective data that supports the rationale.

Table 6: Completed CMSP Survey Question

Category	Control Question	Response			Rationale and Evidence
		Yes	Partial	No	
Contracting	10. Do all contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities?	❑	❑	☑	Rationale: The contract with the vendor for our WEA alerting system does not enable us to participate in code reviews and security testing activities performed by the vendor. Evidence: Language in vendor contract
	11. Do all contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code?	❑	❑	☑	Rationale: The contract with the vendor for our WEA alerting system does not enable us to review the results of static and dynamic analysis tools run by the vendor. Evidence: Language in vendor contract

The team should proceed to answer all questions in the survey. When documenting the rationale for its response to a question, the team should make sure to include any minority opinions that (1) may need to be investigated later or (2) could influence any decisions about selecting which controls to improve. Overall, a CMSP can use the results obtained by completing the questionnaire to identify gaps in the security controls that it currently implements. The team can select which controls to address based on resources available and current risk exposure. It can then develop and implement an improvement plan for the selected controls. The team should use the CMSP's existing planning and improvement processes to address weaknesses in its selected security controls.

7 Next Steps

This report presents the results of a study of the CMSP WEA alerting system conducted by the CERT Division of the SEI. The goal of this study is to provide members of the CMSP community with practical guidance that they can use to better manage their cybersecurity risk exposure. The SEI team applied the SERA Method to perform the security risk analysis that provided the basis of this study. The SERA Method defines a scenario-based approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain.

The centerpiece of these findings is the CMSP Security Guidelines, which was developed using the results of the SERA Method. The CMSP Security Guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study. CMSPs should consider implementing these guidelines to protect their WEA alerting systems. (See Section 5 for more details about the CMSP Security Guidelines.)

By implementing the CMSP Security Guidelines, a CMSP's stakeholders will be able to establish confidence that the organization's exposure to the four security risk scenarios analyzed in this study is within an acceptable tolerance. Ultimately, these stakeholders will be able to demonstrate their due diligence with respect to assuring the CMSP WEA infrastructure by implementing the guidelines specified in this report.

This study builds on work that we completed in 2013, which focused on AOs [SEI 2014]. The 2013 study examined the AO WEA infrastructure and produced a cybersecurity risk management strategy for AOs. The AO strategy was focused on designing cybersecurity controls into the AO WEA infrastructure prior to the deployment of the WEA service. For the current study, much of the information from the 2013 study related to the end-to-end WEA workflow was leveraged (as documented in Section 3).

The purpose of this section is to describe potential next steps for expanding our analysis of the WEA service. Several possible next steps have been identified for this work. Some of these proposed steps focus on expanding the scope of the analysis described in this report. Others look at ways to expand or extend the analysis beyond CMSPs. A variety of candidate follow-on activities are explored in the remainder of this section, beginning with analyzing additional security risk scenarios.

Analyzing Additional Security Risk Scenarios. Four security risk scenarios were analyzed in this study. A future study could expand the number of scenarios. The new scenarios would be analyzed using the SERA Method to identify additional security controls and update the CMSP Security Guidelines. Other candidate threats were identified during the initial brainstorming activity. (A list of brainstormed threats is included in Appendix A.) Additional threats were uncovered during discussions with CMSP SMEs. Security risk scenarios could be constructed based on these threats, and the resulting scenarios analyzed. Finally, as the use of the WEA service continues to expand, new threats and weaknesses may arise. Security risk scenarios for those threats when appropriate can be developed and analyzed.

Expanding Questionnaire Guidance. The control strategy questionnaire in Appendix D could be expanded to include more detailed guidance and specific examples in terms of how to

- complete the questionnaire
- draw conclusions from the results
- determine relative priorities for security controls
- integrate the results into improvement plans

Example workflows and architectures for the WEA service could be used to demonstrate how to set control priorities based on risk exposure and resources (e.g., budget, number of cybersecurity SMEs). Some CMSPs might already have an effective security risk-management program in place. These cyber-savvy carriers should be able to use the control strategy questionnaire as is (i.e., with little or no additional guidance). CMSPs with less cybersecurity experience, however, would probably benefit from having additional guidance and examples available to them.

Conducting Additional CMSP Studies. Additional studies could be conducted to investigate alternative CMSP architectures, such as using smartphone applications to disseminate WEA messages. These additional studies would likely identify new risks and controls unique to those alternative architectures. For example, a WEA application on a smartphone could be attacked or spoofed. A control strategy questionnaire (including detailed guidance and specific examples) could be developed to address cybersecurity risks that are unique to each alternative CMSP architecture.

Updating AO Security Guidelines. As mentioned above, the 2013 AO study examined the AO WEA infrastructure and produced a cybersecurity risk-management strategy for AOs. That strategy was focused on analyzing cybersecurity risks to the AO WEA infrastructure prior to the deployment of the WEA service, however. Here, the goal was to make sure that proper security controls were designed into AO WEA alerting systems. The 2013 AO strategy could be updated and refreshed based on operational data and experience related to issuing WEA messages. Analysis of additional risks using the SERA Method would provide similar detailed risk data, control tables and a set of security guidelines aimed at AOs.

Addressing Continuous Risk Management. Detailed guidance could be developed and vetted for WEA-affiliated organizations (e.g., CMSPs, AOs or other WEA participants) in the area of continuous risk management. Here, cybersecurity risks associated with end-to-end WEA workflow could be identified and managed in real time, as opposed to waiting for formal cybersecurity assessments or audits to be performed. Many larger and more advanced WEA-affiliated organizations could already be addressing aspects of continuous risk management. It is likely that many small organizations (e.g., small CMSPs and AOs) would benefit from continuous risk-management guidance that is tailored to their specific needs and constraints, however. The guidance could be vetted with larger, more advanced organizations for accuracy and relevance and then tailored to the needs and constraints of smaller organizations.

Transitioning the SERA Method to WEA Stakeholders. Appendix A documents a basic description of the SERA Method used to produce the results of this study. The SERA Method was applied to produce the CMSP Security Guidelines described in Section 5 and the associated questionnaire presented in Appendix D. The guidelines and questionnaire reflect the current CMSP operational environment. Over

time, it is expected that the CMSP environment will experience many changes as

- New threats will arise over time.
- CMSP architectures and technologies will continue to change.
- The WEA service evolves over time.

As a result, the CMSP Security Guidelines should be refreshed periodically to reflect changes in the environment. The SERA Method could be transitioned to designated CMSP stakeholders, who would be responsible for applying the method and updating the guidelines when needed. Effective transition requires several mechanisms, including enhanced guidance, training, automated tools for the method and support and assistance from SERA SMEs. Once developed, these transition mechanisms could be used to teach other WEA stakeholder groups, such as AOs and FEMA, how to apply the SERA Method.

Overall, the CMSP Security Guidelines presented in this report provide a place for a CMSP to start when improving the security posture of its WEA alerting system. It is important for us to note that these guidelines are only a starting point. Improvement is an ongoing process. In this section, several additional activities were identified that could be explored in the future. These next steps are intended to build on and expand the body of work described in this report, with the ultimate goal of enabling CMSPs and other WEA stakeholders to continually improve their cyber defenses.

Appendix A SERA Method Description

Software is a growing component of modern business- and mission-critical systems. As organizations become more dependent on software, security-related risks to their organizational missions also increase. In addition, the costs required to control security risks increase significantly when organizations wait until systems are deployed to address those risks. It is more cost effective to address software security risks as early in the lifecycle as possible.

Traditional security-engineering approaches rely on addressing security risks during the operation and maintenance of software-reliant systems. These approaches 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 ineffective for analyzing complex cybersecurity attacks. A new approach for addressing cybersecurity risks earlier in the lifecycle is needed.

Researchers from the CERT Division of the Software Engineering Institute (SEI) have developed the Security Engineering Risk Analysis (SERA) Method, a model-based approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain. The overarching goals of the SERA Method are to (1) build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design), (2) reduce residual cybersecurity risk in deployed systems, and (3) ensure consistency with the National Institute of Standards and Technology (NIST) Risk Management Framework [NIST 2010] and other Department of Defense (DoD) and industry policies for software assurance (e.g., NIST 800-53, DoD 5000-2 and the Building Security In Maturity Model).

This appendix describes the SERA Method and how it was used to analyze commercial mobile service provider (CMSP) security risks. It starts by defining key risk-management terms and concepts in Section A.1. The information presented in Section A.1 provides the conceptual foundation for the SERA Method. In Section A.2, the four tasks of the SERA Method are described. Here, details are provided for each SERA task, along with selected examples.

A.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.[13]
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.*[14]

A.1.1 Security Risk

Security risk is a measure of (1) the likelihood that a threat will exploit a vulnerability to produce an adverse consequence, or loss, and (2) the magnitude of the loss. Figure 9 illustrates the three core components of security 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 security 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)

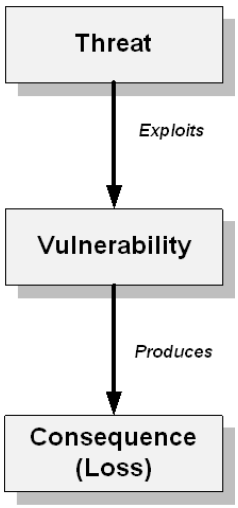

Figure 9: Components of Security Risk

---

[13] 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). Because uncertainty is a fundamental attribute of risk, however, this report does not differentiate between decision-making under risk and decision-making under uncertainty.

[14] This definition is derived from the *Continuous Risk Management Guidebook* [Dorofee 1996].

From the security 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. By itself, however, 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 the book titled *Managing Information Security Risks: The OCTAVE[SM] Approach* [Alberts 2002]).

Consider the following example of a security risk. To ensure quick processing of data, an organization does not encrypt customer data as they are transmitted between systems on the internal network. Malware (e.g., a sniffer), which has been installed in an organization's infrastructure, collects unencrypted customer data (i.e., personally identifiable information) and sends the data to designated staging points across the globe. As a result of this breach in data confidentiality, the organization could suffer significant financial, legal and reputation consequences.

The components of this security risk are

- *Threat*—malware collects unencrypted customer data (i.e., personally identifiable information) and sends the data to designated staging points across the globe.
- *Vulnerability*—the organization does not encrypt customer data as they are transmitted between systems on the internal network.
- *Consequence*—the organization could suffer significant financial loss, legal fees, and reputation damage.

In this example, malware exploits a single vulnerability, the unencrypted transmission of data between systems. If no threat actor (i.e., malware in this example) attempts to exploit the vulnerability and carry out the attack, however, then no adverse consequences will occur. The security vulnerability (e.g., unencrypted data) lies dormant until a threat actor (e.g., malware) attempts to exploit it to produce an adverse consequence or loss.

A.1.2 Risk Measures

In general, three measures are associated with any risk: (1) probability, (2) impact and (3) risk exposure.[15] *Probability* is 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.

A.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

[15] 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.

Figure 10 illustrates the three core risk-management activities:

1. Assess risk—Transform the concerns people have into distinct, tangible security risks that are explicitly documented and analyzed.
2. Plan for controlling risk—Determine an approach for addressing each security risk; produce a plan for implementing the approach.
3. Control risk—Deal with each security risk by implementing its defined control plan and tracking the plan to completion.

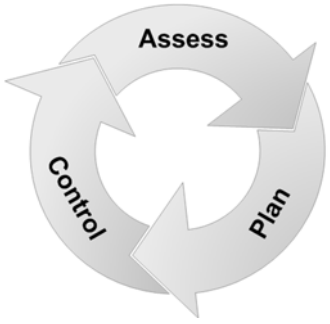

Figure 10: Risk-Management Activities

A.1.4 Controlling Security Risks

The strategy for controlling a risk is based on the measures for the risk - that is, probability, impact and risk exposure - which are established during the risk assessment. Decision-making criteria, such as 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 security 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:

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

Thus far in this section, a simplified view of security risk is provided where a single threat actor exploits a single vulnerability in a single system to cause an adverse consequence. Most traditional security risk-analysis methods are based on this simplified view of risk. In reality, however, multiple actors exploit multiple vulnerabilities in multiple systems as part of a complex chain of events. This next section addresses the inherent complexity of security risk.

A.1.5 Complexity of Security Risk

Consider the following example of a complex risk scenario. In this scenario, an individual (i.e., the perpetrator) intends to steal personally identifiable information about an organization's customer base. The individual's goal is to steal the identities of customers for financial gain. To carry out this risk scenario successfully, the individual performs the following actions:

- The individual performs reconnaissance on the organization's systems and networks.
- The individual also performs reconnaissance on partners and collaborators that work with the organization and have trusted access to the organization's systems and networks.
- Reconnaissance indicates that the organization has strong perimeter security controls in place. As a result, the individual targets a third-party collaborator that (1) has legitimate, trusted access to the organization's internal network and (2) has relatively weak perimeter security controls in place.
- The individual gains access to the third-party collaborator's internal network by exploiting several common vulnerabilities.
- The individual uses the collaborator's trusted access to the organization's internal network to bypass the organization's perimeter security controls and gain access to its network.
- Additional reconnaissance indicates that the organization does not encrypt customer data as they are transmitted between an order entry system and an inventory system (to ensure quick processing of the data). In addition, the organization does not employ rigorous monitoring in its systems and networks. The organization's strategy is to focus primarily on its perimeter security. The individual decides to exploit these vulnerabilities and installs malware (i.e., a sniffer) that is designed to
  - steal unencrypted customer data as it is being transmitted between systems on the internal network
  - send the stolen data to staging points at multiple external locations
- Once installed, the malware collects unencrypted data and sends the data to the staging points. This data exchange is timed to occur during peak business hours to mask the attack.

The crux of this scenario is similar to the risk highlighted in Section A.1.1; however, the risk scenario presented in this section is considerably more complex. This risk scenario better represents the inherent complexity of modern security attacks, where multiple actors exploit multiple vulnerabilities in multiple systems as part of a complex chain of events. In the scenario, both the individual who initiates the attack and the malicious code are considered to be threat actors. Vulnerabilities in the scenario include lack of monitoring to detect the actor's reconnaissance activities; allowing trusted access to the organization's internal network by a third-party collaborator that employs poor security practices; the organization's lack of rigorous monitoring of its systems and networks; and lack of data encryption between the order entry and inventory systems. Systems involved in the attack include systems owned by the third-party collaborator, order entry system, inventory system, perimeter security systems and devices, and various networking systems and devices. As a result of this scenario, the organization could suffer significant financial, legal and reputation consequences.

Traditional methods are often ineffective for analyzing complex security attacks. This research addresses this deficiency in traditional security risk-analysis methods. The next section describes the product of this research: the SERA Method.

A.2 SERA Method

The SERA Method comprises the following four tasks:

1. Establish operational context.
2. Identify risk.
3. Analyze risk.
4. Develop control plan.

The SERA Method can be self-applied by the person or group that is responsible for acquiring and developing a software-reliant system or facilitated by external parties on behalf of the responsible person or group.[16] In either case, a small team of approximately three to five people, called the *Analysis Team*, is responsible for implementing the framework and reporting findings to stakeholders.

An Analysis Team is an interdisciplinary team that requires team members with diverse skill sets. Examples of skills and experience that should be considered when forming a team include security-engineering risk analysis, systems engineering, software engineering, operational cybersecurity and physical/facility security. The exact composition of an Analysis Team depends on the point in the lifecycle in which the SERA Method is being applied and the nature of the engineering activity being pursued.

This section describes the SERA Method. For each SERA task that must be completed, this describes the task as well as the steps that must be conducted for that task. In addition, examples are provided for each step. Our analysis of the Wireless Emergency Alerts (WEA) service provides the basis for all examples in this section. The authors of this report served as the Analysis Team for this application of the SERA Method and generated the WEA examples by applying the SERA Method to the CMSP workflow that supports the WEA service. The description of the SERA Method begins with Task 1.

A.2.1 Establish Operational Context (Task 1)

Task 1 defines the operational context for the analysis. Here, the Analysis Team begins its work by focusing on the environment in which the software application or software-reliant system will be deployed. During Task 1, the team determines how the application or system supports operations (or is projected to support operations if the system of interest 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 system of interest supports the selected workflow or mission thread. This establishes a baseline of operational performance for the system of interest. The team then analyzes security risks in relation to this baseline.

[16] A facilitated assessment still requires participation from groups that are responsible for acquiring and developing the system of interest. The person facilitating the assessment has expertise in conducting security risk analysis. The facilitator includes others on the team with skills and experience in other areas, such as systems engineering, software engineering, operational cybersecurity and physical/facility security.

The Analysis Team completes the following steps during Task 1:

- Determine system of interest (Step 1.1).
- Select workflow/mission thread (Step 1.2).
- Establish operational views (Step 1.3).

The SERA Method begins by establishing the system of interest of the analysis.

A.2.1.1 Determine System of Interest (Step 1.1)

In Step 1.1, the Analysis Team identifies the system of interest for the analysis. The *system of interest* is defined as the software application or system that is the focus of the analysis. Selecting the system of interest starts to define the scope of the subsequent analysis.

Example: The Analysis Team has been asked to conduct a cybersecurity risk analysis of a carrier's WEA alerting environment. As a result, the team selected the carrier's *WEA alerting system* as the system of interest.

A.2.1.2 Select Workflow/Mission Thread (Step 1.2)

A *workflow* is a collection of interrelated work tasks that achieves a specific result [Sharp 2001]. A workflow includes all tasks, procedures, organizations, people, technologies, tools, data, inputs and outputs required to achieve the desired objectives. The business literature uses several terms synonymously with workflow, including work process, business process and process. *Mission thread* is essentially the term that the military uses in place of workflow. A mission thread is a sequence of end-to-end activities and events that takes place to accomplish the execution of a military operation. In this document, the terms *workflow* and *mission thread* are used synonymously.

In Step 1.2, the Analysis Team selects which workflows or mission threads to include in the analysis. A system of interest might support multiple workflows or mission threads during operations. Selecting relevant workflows or mission threads helps to refine the scope of the analysis further.

Example: The Analysis Team selected the WEA alerting system as the system of interest in Step 1.1. In the context of this risk analysis, the WEA alerting system includes the CMSP Gateway as well as several devices throughout the carrier's infrastructure that support the WEA service. The workflow supported by the WEA alerting system is the carrier's WEA alerting process. As a result, the team selects the WEA alerting process as the workflow that will provide the touchstone for the subsequent cybersecurity risk analysis.

A.2.1.3 Establish Operational Views (Step 1.3)

In the final step of Task 1, the Analysis Team establishes a common view of the operational environment in which the system of interest must function. Most traditional risk-identification methods do not explicitly describe the operational environment. As a result, each participant must rely on his or her mental model of the environment when identifying and analyzing security risks. Field experience indicates that people's tacit assumptions about an operational environment tend to be incorrect, incomplete or in conflict with the assumptions of other participants. This incomplete view of the environment is especially problematic when participants attempt to identify security risks early in the lifecycle. The environment might not be well described or documented, which makes people's perspectives vary widely.

To counteract this lack of a common perspective, the SERA Method requires the Analysis Team to develop models that describe the operational environment in which the system of interest will be deployed. Table 7 provides a description of key operational views that are typically documented during Step 1.3 of the SERA Method. Each view is characterized using one or more models.

Table 7: Operational View

View	Description
Workflow/Mission Thread	The sequence of end-to-end activities and events that take place to achieve a specific result.
Stakeholder	The set of people with an interest or concern in (1) the workflow/mission thread and (2) the outcomes (e.g., products, services) produced by it.
Data	The data items required when executing the workflow/mission and their associated security attributes (e.g., confidentiality, integrity, availability).
Technology	The projected technologies that constitute the system of interest. The technology view can include multiple models, such as system architecture and network topology.
Physical	The projected physical layout of the facilities in which components of the system of interest are located.
Use Case	A description of a set of steps that define the interactions between a role/actor and a system to achieve a goal. (The actor can be a human or an external system.)

Developing and documenting operational models enables the Analysis Team to address aspects of complexity that are inherent in the security risk environment. Models representing the views from Table 7 can be analyzed to establish the following key aspects of a threat:

- *Critical data*: Important information highlighted in workflow/mission thread, use case and technology models. By examining these models, analysts can identify which data elements are most critical to the workflow/mission thread and its associated mission.
- *Access path*: How a threat actor can gain access to data and violate its security attributes (i.e., create breaches of data confidentiality, integrity and availability). The technology and physical models provide insights into potential cyber and physical access paths for an attack.
- *Threat outcome*: The direct consequence caused by the threat. A direct consequence describes which security attributes of critical data have been breached. Examples of outcomes include data disclosure, data modification, insertion of false data, destruction of data and interruption of access to data. The data model is used to identify the immediate consequence of a threat.

A threat ends with a description of its direct consequence or outcome. A cybersecurity risk analysis must also take into account any indirect consequences triggered by the occurrence of a threat, however. For example, if false data are inserted into a workflow or mission thread, then the Analysis Team must answer the following questions related to indirect consequences:

- How is the workflow/mission thread affected?
- How are the mission's objectives affected?
- How are mission's stakeholders affected?

The indirect consequences are used to (1) measure the impact of a security risk and (2) establish a risk's priority for decision makers. The Analysis Team determines indirect consequences using models that represent the workflow/mission thread and stakeholder views. These views provide team members with

the information they need to begin identifying risk scenarios in Task 2. In the remainder of this subsection, we feature two operational models that we developed as part of our risk analysis: (1) CMSP workflow model and (2) data model. (The complete set of models is provided in Part 2 of this report, *CMSP Operational Environment.*)

Example (CMSP Workflow): An *emergency alert* is a message sent by an authorized organization that provides details of an occurring or pending emergency situation to one or many designated groups of people. Emergency alerts are initiated by many diverse organizations. For example, law enforcement organizations issue America's Missing: Broadcast Emergency Response (AMBER) alerts, and the National Weather Service (NWS) issues weather alerts. Both AMBER alerts and weather alerts are examples of emergency alerts. A *wireless alert* is an emergency alert that is sent to mobile devices, such as cell phones and pagers.

The following organizations play a role in sending wireless alerts:

- *Initiator*—starts the process of issuing an emergency alert (e.g., law enforcement, NWS).
- *Alert Originator (AO)*—receives the initiator alert request and decides (1) whether or not to issue the alert and (2) the distribution channels for the alert (e.g., television, radio, roadside signs, wireless technologies, others).
- *Federal Emergency Management Agency (FEMA)*—operates Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN), which is a collection of systems that receives a wireless alert from an AO, processes the alert and forwards it to the CMSPs (i.e., carriers).
- *CMSPs*—operate systems that process and format the alert message and then distribute it to recipients' smartphones.
- *Recipients*—receive and read the wireless alert on their smartphones.

In Step 1.2, the Analysis Team identified the carrier's WEA alerting process as the key workflow supported by the WEA alerting system. As a result, the team will use the WEA alerting process as the touchstone for the subsequent cybersecurity risk analysis. Figure 11 depicts the WEA alerting process (also referred to as the CMSP workflow). The figure shows the sequence of activities performed by a carrier to issue a wireless alert. It also shows interfaces to the Federal Alert Gateway and the recipients' mobile devices.

The Analysis Team used a swim-lane diagram to document the workflow. The activities in a swim-lane diagram are grouped visually by placing them in *lanes*. Parallel lines divide the diagram into multiple lanes, with one lane for each workflow actor (i.e., person, group or subprocess). Each lane is labeled to show who is responsible for performing the activities assigned to that lane. In Figure 11, the gray boxes with solid borders represent the activities that are performed by each workflow actor. Lines between the activities establish the relationships among and sequencing of the activities. Finally, the red text represents data items that flow between the activities.

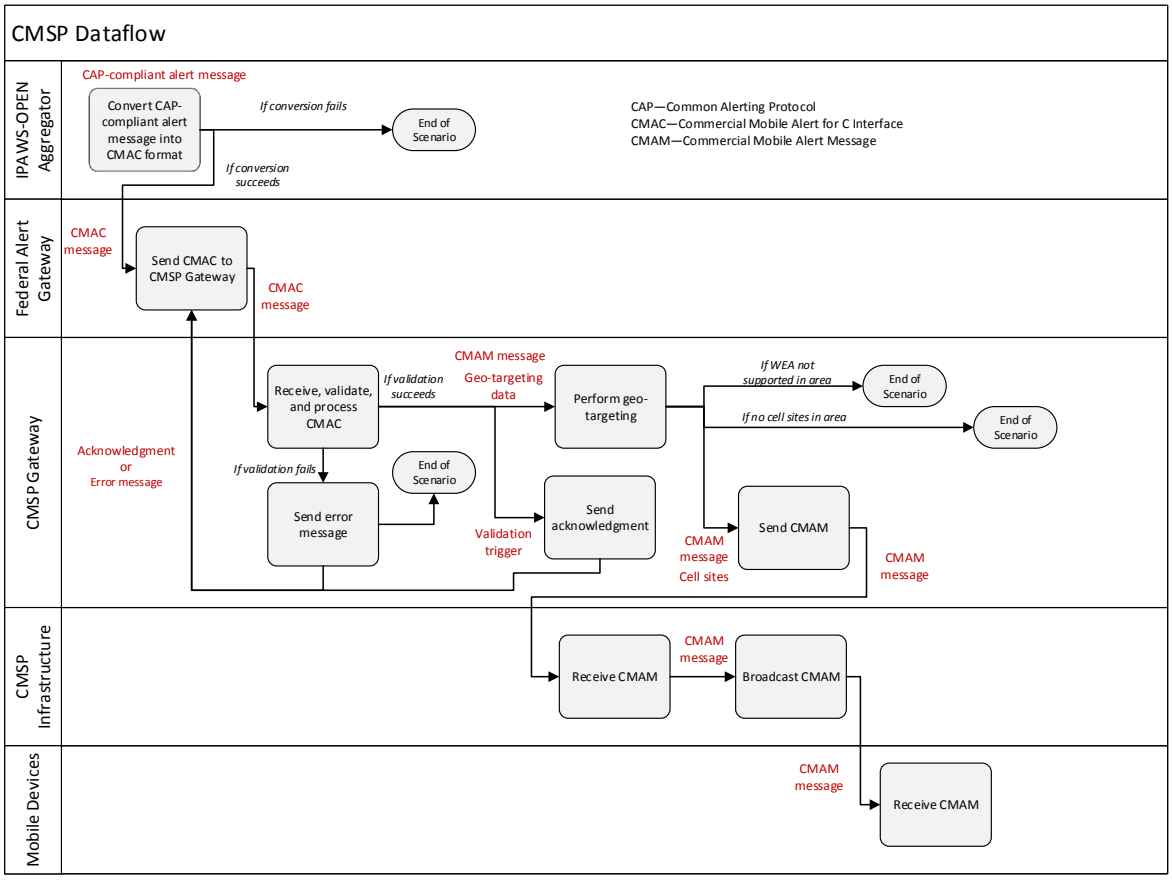

Figure 11: CMSP Workflow Model with Dataflow

The process in Figure 11 begins with the IPAWS-OPEN Aggregator converting a Common Alerting Protocol (CAP)-compliant message into Commercial Mobile Alert for C Interface (CMAC) format. The CMAC message (i.e., the alert message in CMAC format) is forwarded to the Federal Alert Gateway, which interfaces directly with the CMSP Gateway. The Federal Alert Gateway forwards the CMAC message to the CMSP Gateway. Next, the CMSP Gateway sends an acknowledgment that it has received the CMAC message to the Federal Alert Gateway. The CMSP Gateway then validates and processes the CMAC message and performs geo-targeting to determine which cell sites need to broadcast the alert. The CMSP Gateway sends the alert message in Commercial Mobile Alert Message (CMAM) format to targeted cell sites within the CMSP infrastructure. Finally, the CMAM message is broadcast to WEA-capable mobile devices in the targeted area.

Example (Data Model): From analyzing the workflow Figure 11, the Analysis Team identified the following critical data items (i.e., critical assets) for the CMSP workflow:

- *CAP-compliant alert message*—the alert message in CAP format
- *CMAC*—the alert message in CMAC format (as specified by the interface between the Federal Alert Gateway and the CMSP Gateway)
- *CMAM*—the alert message in CMAM format
- *Geo-targeting data*—the geographic area covered by the alert

Table 8 presents the security attributes (i.e., confidentiality, integrity and availability) for the four critical data items.

Table 8: CMSP Data Model

Data Element	Form	Confidentiality	Integrity	Availability
CAP-compliant alert message	Electronic	There are no restrictions on who can view this data element (public data).	The data element must be correct and complete (high data integrity).	This data element must be available when needed (high availability).
CMAC	Electronic	There are no restrictions on who can view this data element (public data).	The data element must be correct and complete (high data integrity).	This data element must be available when needed (high availability).
CMAM	Electronic	There are no restrictions on who can view this data element (public data).	The data element must be correct and complete (high data integrity).	This data element must be available when needed (high availability).
Geo-targeting data	Electronic	There are no restrictions on who can view this data element (public data).	The data element must be correct and complete (high data integrity).	This data element must be available when needed (high availability).

A.2.2 Identify Risk (Task 2)

Task 2 focuses on risk identification. In this task, the Analysis Team transforms security concerns into distinct, tangible risk scenarios that can be described and measured. The team starts by reviewing the operational models from Task 1. It then brainstorms threats to the system of interest and then selects one of the threats to analyze in detail. The Analysis Team identifies threat components and a sequence of steps for a subset of the brainstormed list of threats. The team continues analyzing all high-priority threats to the systems of interest. Team members must use their professional judgment when determining which threats to analyze in detail.

For each selected threat, the team continues its risk identification activities by establishing the following elements of security risk:

- *Consequences*—the operational effects or impacts produced by the occurrence of a threat
- *Enablers*—conditions and circumstances that facilitate a threat's occurrence
- *Amplifiers*—conditions and circumstances that increase the consequences triggered by the occurrence of a threat

Finally, the Analysis Team creates a narrative, or scenario, for each security risk and compiles all data related to the scenario in a usable format.

A.2.2.1 Identify Threat (Step 2.1)

The Analysis Team first analyzes the operational models from Task 1 to identify critical data, which is transmitted, stored, and processed by the system of interest (i.e., critical assets). The team then examines how threat actors might violate the security attributes (i.e., confidentiality, integrity and availability) of the critical data. For threats that the team will analyze further, it documents the components of the threat and the sequence of steps required to execute the threat (i.e., threat sequence).

Threat components describe different facets of a threat. They provide details about a threat that are not part of a risk statement and might not be conveyed in the security risk scenario. Threat components include the following items:

- *Threat*—a statement that describes the cyber-based act, occurrence or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss; the threat statement provides the content for the *if* portion of the risk statement
- *Actor*—who or what is attempting to violate the security attributes of critical data
- *Motive*—the intentions of a threat actor, which can be deliberate and malicious or accidental
- *Goal*—the end toward which the threat actor's effort is directed; the goal succinctly describes the key indirect consequence (i.e., impact on stakeholders) that the actor is trying to produce
- *Outcome*—the direct consequence of the threat (i.e., disclosure of data, modification of data, insertion of false data, destruction of data, interruption of access to data)
- *Means*—the resources the actor uses when executing the threat
- *Threat complexity*—the degree of difficulty associated with executing the threat
- *Additional context*—any additional, relevant contextual information related to the threat

The threat sequence describes the series of actions taken by the actor(s) when executing the threat. It describes how the actor(s) will carry out the threat and ultimately produce a desired outcome.

Example (Brainstormed List of Threats): The Analysis Team brainstormed the following threats to the carrier's WEA alerting system:

- An outside actor with malicious intent obtains a valid certificate through social engineering and uses it to send an illegitimate alert message by spoofing the Federal Alert Gateway.
- Malicious code prevents the CMSP Gateway from processing an alert.
- An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages.
- An outside actor with malicious intent launches a distributed denial-of-service (DDoS) attack against the CMSP Gateway.
- An attacker in the mobile-device supply chain inserts malicious code into mobile devices sold by carriers. The malicious code captures legitimate WEA messages and replays them repeatedly at a later time (supply-chain attack).
- An upstream replay attack targets an AO and sends repeated messages to a geographic area, which could result in a denial of service for the carriers.
- An outside actor with malicious intent spoofs a cell tower and transmits an illegitimate message to mobile devices in a local area.

The team selected the following threat to analyze first: *An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages*. The remainder of this appendix examines the analysis of this risk (hereafter referred to as *Risk 1*).

Example (Threat Components): Table 9 illustrates the threat components that the Analysis Team documented for Risk 1.

Table 9: Threat Components for Risk 1

Component	Description
Threat	An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages.
Actor	A person with insider knowledge of the organization.
Motive	The threat is a deliberate/malicious act. The actor is disgruntled (e.g., has been passed over for promotion or has been notified of performance issues). The actor has visibly expressed frustration/anger.
Goal	The actor seeks to erode trust in the carrier. If this is a major carrier, the attack will also erode trust in the WEA service (e.g., people will turn off alerts) due to the large impact.
Outcome	Illegitimate alerts are sent to the carrier's mobile devices, which will trigger alert sounds (integrity issue).
Means	The actor needs access to the carrier's systems, access to public documents that describe the WEA service and access to documents that describe the CMAM format.
Threat complexity	The attack is moderately complex, requires technical skills and requires moderate preparation to execute.
Attack summary	The insider inserts a logic bomb, which is designed to replay a nonsense or inflammatory CMAM message repeatedly.
Additional context	The timing of the attack could cause critical alerts to be ignored. This threat incorporates current SEI/CERT research on insider threat [http://www.cert.org/insider-threat/].

Example (Threat Sequence): The threat sequence for Risk 1 is shown in Table 10.

Table 10: Threat Sequence for Risk 1

Step	
T1.	The insider is upset upon learning that he will not receive a bonus this year and has been passed over for a promotion.
T2.	The insider begins to behave aggressively and abusively toward his coworkers.
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.
T4.	The insider uses a colleague's workstation to check in the modified code with the logic bomb to the CMSP Gateway code base.
T5.	Seven months later, the insider voluntarily leaves the company for a position in another organization.
T6.	Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.
T7.	The malicious code causes the carrier's CMSP Gateway to send a nonsense WEA message repeatedly to people across the country.

A.2.2.2 Establish Consequences (Step 2.2)

The next step in the analysis is to establish the consequences of each threat identified during the previous step. In Step 2.2, the Analysis Team analyzes the workflow/mission thread and stakeholder models from Task 1 to determine how the workflow/mission thread and stakeholders could be affected by that threat.

A threat produces a direct consequence, which is called the outcome of the threat. A threat's outcome indicates how the security attributes of critical data are violated; it does not indicate the potential impact on the objectives of the workflow or mission thread. To fully analyze a threat's impact, the Analysis Team must look beyond the direct consequence and examine how the threat might affect the projected operational environment. This process begins by examining how the outcome (i.e., direct consequence) might affect the objectives of the workflow or mission thread (i.e., indirect consequence of the threat's occurrence).

Analyzing workflow consequences is a necessary part of a security risk analysis; however, it is not sufficient. To conduct a thorough security risk analysis, the Analysis Team must look beyond a threat's effect on the workflow or mission thread and examine how the stakeholders of that workflow or mission thread might be affected.

Example (Workflow Consequences): The workflow consequences for Risk 1 are shown in Table 11.

Table 11: Workflow Consequences for Risk 1

Consequence	Workflow Actor
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices

Example (Stakeholder Consequences): The Analysis Team identified the consequences in Table 12 for WEA stakeholders.

Table 12: Stakeholder Consequences for Risk 1

Consequence	Stakeholder
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.	Recipients
Many recipients complain to the carrier's customer service operators.	Recipients
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	FEMA Carrier
The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable.	Carrier
People leave the carrier for another carrier because of the incident.	Carrier
People lose trust in the WEA service.	FEMA Carrier

Stakeholders can experience a variety of risk-relevant consequences, including health, safety, legal, financial and reputation consequences. Ultimately, the Analysis Team uses the stakeholder consequences when evaluating the impact of a security risk.

A.2.2.3 Identify Enablers and Amplifiers (Step 2.3)

Enablers are the conditions and circumstances that lead to the occurrence of a risk. Enablers include

- vulnerabilities (i.e., design weaknesses, coding errors, configuration errors) that a threat actor could exploit to produce an adverse consequence or loss
- any additional conditions or circumstances that are needed for the risk to occur

Amplifiers are conditions and circumstances that propagate or increase the consequences triggered by the occurrence of a threat. Amplifiers include

- conditions or circumstances that allow consequences to propagate though a workflow or mission thread
- conditions or circumstances that facilitate or increase the consequence experienced by a set of stakeholders.

Example (Enablers): The Analysis Team identified the enablers in Table 13 for each step in the threat sequence.

Table 13: Threat Sequence with Enablers for Risk 1

Step		Enabler
T1.	The insider is upset upon learning that he will not receive a bonus this year and has been passed over for a promotion.	A lack of proper feedback provided to an employee can result in the employee being unaware of performance issues that could affect his or her career.
T2.	The insider begins to behave aggressively and abusively toward his coworkers.	An employee's inappropriate behavior can be an indicator of more serious actions.
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.	An employee who has technical skills can use those skills to inflict damage on information systems.
T4.	The insider uses a colleague's workstation to check in the modified code with the logic bomb to the CMSP Gateway code base.	Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.
		An insufficient change-management/configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.
T5.	Seven months later, the insider voluntarily leaves the company for a position in another organization.	Insufficient monitoring of an employee's actions and behavior before he or she leaves the organization can prevent the carrier from knowing if the employee is abusing his or her access to information and systems.
T6.	Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.	An insufficient change-management/configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.
T7.	The malicious code causes the carrier's CMSP Gateway to send a nonsense WEA message repeatedly to people across the country.	Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.
		Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).

Example (Amplifiers): Table 14 shows the amplifiers for each workflow consequence.

Table 14: Workflow Consequences with Amplifiers for Risk 1

Consequence	Workflow Actor	Amplifier
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.

The Analysis Team identified the amplifiers in Table 15 for each stakeholder consequence.

Table 15: Stakeholder Consequences with Amplifiers for Risk 1

Consequence	Stakeholder	Amplifier
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.
Many recipients complain to the carrier's customer service operators.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	FEMA Carrier	People's ability to disable the WEA service on their mobile devices helps them deal with the attack. They might decide not to (or might forget to) re-enable the WEA service after the attack.
The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable.	Carrier	An insufficient change-management/configuration-management capability can increase the time it takes to identify unauthorized changes and recover from the attack. This can amplify the recovery costs.
People leave the carrier for another carrier because of the incident.	Carrier	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.
People lose trust in the WEA service.	FEMA Carrier	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.

A.2.2.4 Develop Risk Scenario (Step 2.4)

In Step 2.4, the Analysis Team documents a narrative description of the security risk based on the information generated in Steps 2.1 through 2.3. Finally, the team documents a risk statement that provides a succinct and unique description of the security risk scenario that is used for tracking purposes.

Many traditional risk assessments use if-then statements to represent a security risk. Those assessments rely on the if-then structure to convey all relevant information about a security risk. In contrast, the SERA Method uses a risk statement as a shorthand description of a security risk scenario. The Analysis Team uses the security risk scenario and supporting data structures (i.e., not the summary if-then statement) when analyzing security risks and making decisions about how to control them. Risk statements are used to facilitate the tracking of multiple security risk scenarios during analysis and control.

Example (Risk Scenario): The Analysis Team documented the following scenario for Risk 1:

> An insider is employed by a wireless carrier. The insider is a software developer and is responsible for developing applications that support the company's wireless infrastructure. The insider is upset that he will not receive a bonus this year and also has been passed over for a promotion. Both of these perceived slights anger the insider. As a result, he begins to behave aggressively and abusively toward his coworkers. For example, he downplays their achievements, brags about his own abilities, takes credit for the work of others and delays progress on projects. The insider's anger builds over time until he finally convinces himself to take action against the carrier.
>
> His plan is to plant a logic bomb in the CMSP Gateway, hoping to send "custom" WEA messages to all WEA-capable wireless devices supported by the carrier. His ultimate goal is to bring negative publicity to the company. As a function of his job, the insider has unlimited access to the company's software code and is able to modify the company's code at will. While on site and during work hours, the insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.
>
> The insider shares an office with another software developer, who often leaves her workstation unlocked when she is out of the office. The insider uses his colleague's workstation to check in the modified code with the logic bomb. Seven months later, the insider voluntarily leaves the company for a position in another organization. Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically. The malicious code causes the carrier's WEA service to send a nonsense WEA message repeatedly to people across the country.
>
> Many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier's customer service operators. A large number of recipients turn off the WEA function on their phones in response to the attack.
>
> The carrier responds to the attack by taking the infected CMSP Gateway offline. The broadcast of the illegitimate messages stop. The carrier then responds aggressively to the attack by investigating the source of the attack, locating the malicious code and removing that code from its infrastructure. Once the malicious code is removed from the CMSP Gateway, the carrier brings the CMSP Gateway back online. The cost to recover from the attack is considerable.
>
> As a result of the attack, some customers leave their carrier for other carriers. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

Example (Risk Statement): The Analysis Team documented the following risk statement in if-then format for Risk 1:

> **IF** an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

A.2.3 Analyze Risk (Task 3)

Task 3 focuses on risk analysis. The following three measures are associated with risk:

1. *Probability*—the likelihood that the risk will occur
2. *Impact*—the loss that occurs when a risk is realized
3. *Risk exposure*—the magnitude of a risk based on current values of probability and impact

During Task 3, the Analysis Team evaluates each risk scenario in relation to predefined criteria to determine its probability, impact and risk exposure.

A.2.3.1 Establish Probability (Step 3.1)

In Step 3.1, the Analysis Team evaluates and documents the probability of occurrence for the security risk scenario. The team first reviews the probability evaluation criteria[17] that they established for the analysis. Next, the Analysis Team estimates the probability for the security risk scenario by assigning a probability measure (e.g., frequent, probable, occasional, remote, rare) to the scenario and documenting the rationale for selecting that measure.

Example (Probability Evaluation Criteria): Table 16 provides the criteria that the Analysis Team used to evaluate probability.

Table 16: Probability Criteria

Value	**Definition**	**Guidelines/Context/Examples** *How often would an event occur for each value? How many times in a given year?*
Frequent (5)	The scenario occurs on numerous occasions or in quick succession. It tends to occur quite often or at close intervals.	≥ 1 time per month ≥ 12 times per 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.”	~ 1 time per 6 months ~ 2 times per 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 occurs infrequently and is considered to be uncommon or unusual. It is not frequently experienced.	≤ 1 time every 3 years ≤ .33 times per year

[17] The Analysis Team defines a set of probability evaluation criteria when it is preparing to conduct the SERA Method. Probability evaluation criteria establish a set of qualitative measures (e.g., frequent, probable, occasional, remote, rare) for assessing the likelihood that the risk will occur.

Example (Probability Evaluation): Table 17 shows the probability evaluation for Risk 1.

Table 17: Probability Evaluation for Risk 1

Probability Value	Rationale
Remote	This attack can occur, but it is not likely to occur often. It has "an outside chance" of occurring. Reasons for categorizing the probability as remote include the following: • The attack is moderately complex and requires moderate preparation to execute. • The disgruntled insider must have physical access to a workstation with access to CMSP production code. • The disgruntled insider must have the technical skills needed to execute the attack. • The disgruntled insider must be familiar with the CMSP Gateway. • The number of cyber attacks by disgruntled insiders continues to grow (i.e., an insider attack like this is not a rare event). • Public data do not indicate that the probability is higher than remote.

A.2.3.2 Establish Impact (Step 3.2)

In Step 3.2, the Analysis Team evaluates and documents the impact for the security risk scenario. The team first reviews the impact evaluation criteria[18] that they established for the analysis. Next, the Analysis Team estimates the impact for the security risk scenario by assigning an impact measure (e.g., frequent, probable, occasional, remote, rare) to the scenario and documenting the rationale for selecting that measure.

Example (Impact Evaluation Criteria): Table 18 provides the criteria that the Analysis Team used to evaluate impact.

Table 18: Impact Criteria

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. The organization experiences significant problems and disruptions. 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 time. Recovery will require a significant investment of organizational capital and resources.
Medium (3)	The impact on the organization is moderate. The organization experiences several problems and disruptions. 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.

[18] The Analysis Team defines a set of impact evaluation criteria when it is preparing to conduct the SERA Method. Impact evaluation criteria establish a set of qualitative measures (e.g., maximum, high, medium, low, minimal) for assessing the loss that will occur if the risk is realized.

Value	Definition
Low (2)	The impact on the organization is relatively small, but noticeable. The organization experiences minor problems and disruptions. 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. The organization can accept any damages without affecting operations or the mission being pursued. No stakeholders will be affected. Any costs incurred by the organization will be incidental.

Example (Impact Evaluation): Table 19 shows the impact evaluation for Risk 1.

Table 19: Impact Evaluation for Risk 1

Impact Value	Rationale
Medium	The impact on the organization is moderate. The organization will be able to recover from the attack. Recovery will require a moderate investment of organizational capital and resources. Reasons for categorizing the impact as medium include the following: • Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of business. • Carriers already have help desk capabilities in place to respond to customer complaints. • Tech-savvy customers can turn off the WEA service. • The costs required to recover from this attack (e.g., remove the malicious code, perform public relations outreach) will not be excessive. • Public data indicate that the impact of this type of attack is generally moderate.

A.2.3.3 Determine Risk Exposure (Step 3.3)

Finally, in Step 3.3, the Analysis Team determines and documents the risk exposure for the security risk scenario. The team uses the risk exposure matrix[19] that they established for the analysis. The team maps the current values of probability and impact to the measurement scales on the matrix. The cell in the matrix at the interstation of the current probability and impact values defines the risk exposure for the scenario.

[19] The Analysis Team defines a risk exposure matrix when it is preparing to conduct the SERA Method. The matrix provides a way of estimating the magnitude of a risk (e.g., maximum, high, medium, low, minimal) based on current values of probability and impact.

Example (Risk Exposure Matrix): The matrix that the Analysis Team used to evaluate risk exposure is shown in Table 20.

Table 20: Risk Exposure Matrix

Impact	Probability: Rare (1)	Remote (2)	Occasional (3)	Probable (4)	Frequent (5)
Maximum (5)	**Medium (3)**	**Medium (3)**	**High (4)**	**Maximum (5)**	**Maximum (5)**
High (4)	**Low (2)**	**Low (2)**	**Medium (3)**	**High (4)**	**Maximum (5)**
Medium (3)	**Minimal (1)**	**Low (2)**	**Low (2)**	**Medium (3)**	**High (4)**
Low (2)	**Minimal (1)**	**Minimal (1)**	**Minimal (1)**	**Low (2)**	**Medium (3)**
Minimal (1)	**Minimal (1)**	**Minimal (1)**	**Minimal (1)**	**Minimal (1)**	**Low (2)**

Example (Risk Exposure Evaluation): The risk exposure evaluation for Risk 1 is *Low*. As shown in Table 21, the Analysis Team established the risk exposure for Risk 1 using the current values of impact and probability.

Table 21: Risk Exposure for Risk 1

Impact	Probability: Rare (1)	Remote (2)	Occasional (3)	Probable (4)	Frequent (5)
Maximum (5)	Medium (3)	Medium (3)	High (4)	Maximum (5)	Maximum (5)
High (4)	Low (2)	Low (2)	Medium (3)	High (4)	Maximum (5)
Medium (3)	Minimal (1)		Low (2)	Medium (3)	High (4)
Low (2)	Minimal (1)	Minimal (1)	Minimal (1)	Low (2)	Medium (3)
Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)	Low (2)

A.2.4 Develop Control Plan (Task 4)

Task 4 establishes a plan for controlling a selected set of risks. First, the Analysis Team prioritizes the security risk scenarios based on their risk measures. Once they have established priorities, the team determines the basic approach for controlling each risk (i.e., accept or plan[20]) based on predefined criteria and current constraints (e.g., resources and funding available for control activities).

For each risk that is not accepted, the Analysis Team develops a control plan that indicates

- how the threat can be monitored and the actions to take when it occurs (recognize and respond)
- which protection measures can be implemented to reduce vulnerability to the threat and minimize any consequences that might occur (resist)
- how to recover from the risk if the consequences or losses are realized (recover)

Completing Task 4 marks the conclusion of the SERA Method. At this point, the Analysis Team has actionable control plans that it can begin to implement.

---

[20] The SERA Method examines control approaches in Steps 4.2 and 4.3. During Step 4.2, the Analysis Team determines which risks will be accepted and no longer considered and which will have control plans. At this point in applying the method, the Analysis Team does not identify specific strategies for transferring, avoiding and mitigating risks. Those strategies are addressed in Step 4.3. As noted earlier in this appendix, security risk scenarios comprise multiple threat steps (as defined in the threat sequence), many enablers and a range of indirect consequences. An Analysis Team might employ multiple strategies for addressing a given security risk scenario. For example, some steps in the threat sequence might be avoided by restructuring the workflow/mission thread or changing the network architecture. Certain financial consequences might be transferred to third parties by purchasing insurance. The probability of occurrence for some steps in the threat sequence or some types of consequences might be reduced by implementing mitigation controls. Specific control strategies (e.g., transfer, avoid, mitigate) are considered when the control plan is being developed.

A.2.4.1 Prioritize Risks (Step 4.1)

The Analysis Team prioritizes all security risk scenarios in Step 4.1 based on their impact, probability and risk exposure measures. The team documents the ranked risk scenarios in a tracking spreadsheet.

Example (Prioritized Risks): The Analysis Team used the following guidelines for prioritizing the list of WEA risks:

- Impact was the primary factor for prioritizing security risks. Risks with the largest impacts are deemed to be of highest priority.
- Probability was the secondary factor for prioritizing security 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.

The prioritized risk spreadsheet developed by the Analysis Team is shown in Table 22.

Table 22: Prioritized Risk Spreadsheet

ID	Risk Statement	Impact	Probability	Risk Exposure
R4	**IF** an outside actor with malicious intent uses a denial-of-service (DoS) attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, **THEN** people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Maximum	Rare	Medium
R1	**IF** an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Remote	Low
R2	**IF** the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, **THEN** customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Remote	Low
R3	**IF** malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Medium	Rare	Minimal

A.2.4.2 Select Control Approach (Step 4.2)

In Step 4.2, the Analysis Team determines how it will handle each risk. If a risk is accepted, its consequences will be tolerated; no proactive action to address the risk will be taken. If the team decides to

take action to control a risk, it will develop a control plan for that risk in Step 4.3. The team documents its control approach and the rationale for selecting that approach.

Example (Control Approach): The Analysis Team decided to develop a control plan for Risk 1. The team's decision and rationale are shown in Table 23.

Table 23: Control Approach for Risk 1

Control Approach	Rationale
Plan	This risk will be actively controlled. Reasons for developing a control plan include the following: • A motivated insider with the right set of technical skills could easily execute this attack. An effective set of controls will reduce the probability of occurrence. • The impact of this risk (i.e., moderate) is high enough to warrant taking action. An effective set of controls will reduce the impact of and recovery costs for this risk. • This risk affects the customer base and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

A.2.4.3 Establish Control Actions (Step 4.3)

In the final step of the SERA Method, the Analysis Team defines and documents a plan for all risks that are being controlled. A control plan establishes a range of actions needed to

- recognize and respond to threats
- resist the threat and potential consequences
- recover from consequences when they occur

At this point, the team can begin to prioritize controls (across all control plans) and begin to implement the highest priority actions.

Example (Control Actions): Table 24 provides the candidate controls that the Analysis Team developed for Risk 1. Table 24 depicts controls that are mapped to the enablers of each threat step. The team also developed controls for the workflow and stakeholder consequences. A complete set of controls for Risk 1 is provided in Appendix B.

Table 24: Control Actions for Risk 1's Threat Enablers

Step		Enabler	Candidate Control
T1.	The insider is upset upon learning that he will not receive a bonus this year and has been passed over for a promotion.	A lack of proper feedback provided to an employee can result in the employee being unaware of performance issues that could affect his or her career.	The carrier's managers are trained to provide constructive feedback on performance issues.
T2.	The insider begins to behave aggressively and abusively toward his coworkers.	An employee's inappropriate behavior can be an indicator of more serious actions.	The carrier's managers recognize inappropriate behavior when it occurs and respond appropriately.
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.	An employee who has technical skills can use those skills to inflict damage on information systems.	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.

Step		Enabler	Candidate Control
T4.	The insider uses a colleague's workstation to check in the modified code with the logic bomb to the CMSP Gateway code base.	Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.	The carrier implements physical access controls for workstations and workspaces.
		An insufficient change-management/ configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.	The carrier implements/improves a change-management/configuration-management system.
			The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T5.	Seven months later, the insider voluntarily leaves the company for a position in another organization.	Insufficient monitoring of an employee's actions and behavior before he or she leaves the organization can prevent the carrier from knowing if the employee is abusing his or her access to information and systems.	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T6.	Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.	An insufficient change-management/ configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.	The carrier implements/improves a change-management/configuration-management system.
T7.	The malicious code causes the carrier's CMSP Gateway to send a nonsense WEA message repeatedly to people across the country.	Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.	The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
		Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
			The carrier implements an incident response capability plan to minimize the consequences of the event.

Appendix B Security Risk Data

This appendix documents the detailed information for each risk generated using the Security Engineering Risk Analysis (SERA) Method. For each risk, the following data was recorded:

- *Security Risk Scenario*—a narrative description of the security risk
- *Risk Statement*—a short and unique description of a security risk scenario in if-then format
- *Threat Components*—different facets of a threat, including threat description, actor, motive, goal, outcome, means, threat complexity and additional context
- *Threat Sequence Table*—the series of actions taken by the actor(s) when executing the threat this table also includes enablers of each threat action and candidate controls
- *Workflow Consequences Table*—the effects of a threat on the workflow or mission thread; this table also includes consequence amplifiers and candidate controls
- *Stakeholder Consequences Table*—the effects of a threat on stakeholders; this table also includes consequence amplifiers and candidate controls
- *Risk Measures*—estimates of the values of probability, impact and risk exposure; this table also includes the rationales for the estimates of probability and impact
- *Control Approach*—the decision about how to handle each risk (accept or plan)

The following four risks were analyzed using the SERA Method:

- Risk 1: Insider Sends False Alerts
- Risk 2: Inherited Replay Attack
- Risk 3: Malicious Code in the Supply Chain
- Risk 4: Denial of Service.

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

B.1 Insider Sends False Alerts (Risk 1)

B.1.1 Security Risk Scenario

An insider is employed by a wireless carrier. The insider is a software developer and is responsible for developing applications that support the company's wireless infrastructure. The insider is upset that he will not receive a bonus this year and also has been passed over for a promotion. Both of these perceived slights anger the insider. As a result, he begins to behave aggressively and abusively toward his coworkers. For example, he downplays their achievements, brags about his own abilities, takes credit for the work of others and delays progress on projects. The insider's anger builds over time until he finally convinces himself to take action against the carrier.

His plan is to plant a logic bomb in the commercial mobile service provider (CMSP) Gateway, hoping to send "custom" Wireless Emergency Alerts (WEA) messages to all WEA-capable wireless devices supported by the carrier. His ultimate goal is to bring negative publicity to the company. As a function of his job, the insider has unlimited access to the company's software code and is able to modify the

company's code at will. While on site and during work hours, the insider develops a logic bomb designed to replay a nonsense Commercial Mobile Alert Message (CMAM) message repeatedly.

The insider shares an office with another software developer, who often leaves her workstation unlocked when she is out of the office. The insider uses his colleague's workstation to check in the modified code with the logic bomb. Seven months later, the insider voluntarily leaves the company for a position in another organization. Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically. The malicious code causes the carrier's WEA service to send a nonsense WEA message repeatedly to people across the country.

Many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier's customer service operators. A large number of recipients turn off the WEA function on their phones in response to the attack.

The carrier responds to the attack by taking the infected CMSP Gateway offline. The broadcast of the illegitimate messages stop. The carrier then responds aggressively to the attack by investigating the source of the attack, locating the malicious code, and removing that code from its infrastructure. Once the malicious code is removed from the CMSP Gateway, the carrier brings the CMSP Gateway back online. The cost to recover from the attack is considerable.

As a result of the attack, some customers leave their carrier for other carriers. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

B.1.2 Risk Statement

IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

B.1.3 Threat Components

Component	Description
Threat	An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages.
Actor	The actor is a person with insider knowledge of the organization
Motive	The threat is a deliberate/malicious act. The actor is disgruntled (e.g., has been passed over for promotion or has been notified of performance issues). The actor has visibly expressed frustration/anger.
Goal	The actor seeks to erode trust in the carrier. If this is a major carrier, the attack will also erode trust in the WEA service (e.g., people will turn off alerts) due to the large impact.
Outcome	Illegitimate alerts are sent to the carrier's mobile devices, which will trigger alert sounds (integrity issue).
Means	The actor needs access to the carrier's systems, access to public documents that describe the WEA service and access to documents that describe the CMAM format.
Threat complexity	The attack is moderately complex, requires technical skills and requires moderate preparation to execute.
Attack summary	The insider inserts a logic bomb, which is designed to replay a nonsense or inflammatory CMAM message repeatedly.
Additional context	The timing of the attack could cause critical alerts to be ignored. This threat incorporates current SEI/CERT research on Insider Threat [http://www.cert.org/insider-threat/].

B.1.4 Threat Sequence Table

Threat Step		Focus	Enabler	Candidate Control
T1.	The insider is upset upon learning that he will not receive a bonus this year and has been passed over for a promotion.	Organization Carrier—human resource practices	A lack of proper feedback provided to an employee can result in the employee being unaware of performance issues that could affect his or her career.	The carrier's managers are trained to provide constructive feedback on performance issues.
T2.	The insider begins to behave aggressively and abusively toward his coworkers.	Organization Carrier—human resource practices	An employee's inappropriate behavior can be an indicator of more serious actions.	The carrier's managers recognize inappropriate behavior when it occurs and respond appropriately.
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.	Technology CMSP Gateway (focus of the logic bomb)	An employee who has technical skills can use those skills to inflict damage on information systems.	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T4.	The insider uses a colleague's workstation to check in the modified code with the logic bomb to the CMSP Gateway code base.	Organization Carrier's physical security practices Technology Workstation security (e.g., screen locking) CMSP Gateway Change-management/configuration-management system	Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.	The carrier implements physical access controls for workstations and workspaces.
			An insufficient change-management/configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.	The carrier implements/improves a change-management/configuration-management system.
				The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T5.	Seven months later, the insider voluntarily leaves the company for a position in another organization.	Organization Carrier—human resource practices Technology System and network monitoring	Insufficient monitoring of an employee's actions and behavior before he or she leaves the organization can prevent the carrier from knowing if the employee is abusing his or her access to information and systems.	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T6.	Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.	Technology CMSP Gateway	An insufficient change-management/configuration-management capability can prevent the carrier from knowing if software has been modified inappropriately.	The carrier implements/improves a change-management/configuration-management system.

Threat Step		Focus	Enabler	Candidate Control
T7.	The malicious code causes the carrier's CMSP Gateway to send a nonsense WEA message repeatedly to people across the country.	Organization Carrier—system and network monitoring practices Technology CMSP Gateway System and network monitoring technologies	Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.	The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
			Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
				The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
				The carrier implements an incident response capability to minimize the consequences of the event.

B.1.5 Workflow Consequences Table

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
			The carrier implements an incident response capability to minimize the consequences of the event.
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.	Recipients can disable the WEA service on their mobile devices.

B.1.6 Stakeholder Consequences Table

Consequence	Stakeholder	Amplifier	Candidate Control
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	The carrier implements an incident response capability to minimize the consequences of the event.
			The carrier controls access to sensitive information based on organizational role.
Many recipients complain to the carrier's customer service operators.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	The carrier implements a recovery plan to minimize the consequences of the event.
			The carrier controls access to sensitive information based on organizational role.
			The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages.
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	Federal Emergency Management Agency (FEMA) Carrier	People's ability to disable the WEA service on their mobile devices helps them deal with the attack. They might decide not to (or might forget to) re-enable the WEA service after the attack.	The carrier implements a recovery plan to minimize the consequences of the event.
The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable.	Carrier	An insufficient change-management/configuration-management capability can increase the time it takes to identify unauthorized changes and recover from the attack. This can amplify the recovery costs.	The carrier implements/improves a change-management/configuration-management system.
			The carrier implements an incident response capability to minimize the consequences of the event.
People leave the carrier for another carrier because of the incident.	Carrier	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	The carrier implements a recovery plan to minimize the consequences of the event.
			The carrier controls access to sensitive information based on organizational role
People lose trust in the WEA service.	FEMA Carrier	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.	The carrier implements a recovery plan to minimize the consequences of the event.

B.1.7 Risk Measures

Measure	Value	Rationale
Probability	Remote	This attack can occur, but it is not likely to occur often. It has "an outside chance" of occurring. Reasons for categorizing the probability as remote include the following: • The attack is moderately complex and requires moderate preparation to execute. • The disgruntled insider must have physical access to a workstation with access to CMSP production code. • The disgruntled insider must have the technical skills needed to execute the attack. • The disgruntled insider must be familiar with the CMSP Gateway • The number of cyber attacks by disgruntled insiders continues to grow (i.e., an insider attack like this is not a rare event). • Public data do not indicate that the probability is higher than remote.
Impact	Medium	• The impact on the organization is moderate. The organization will be able to recover from the attack. Recovery will require a moderate investment of organizational capital and resources. Reasons for categorizing the probability as remote include the following: • Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of business. • Carriers already maintain help desk capabilities to respond to customer complaints. • Tech-savvy customers can turn off the WEA service. • The costs required to recover from this attack (e.g., remove the malicious code, perform public relations outreach) will not be excessive • Public data indicate that the impact of this type of attack is generally moderate.
Risk exposure	Low	

B.1.8 Control Approach

Approach	Rationale
Plan	This risk will be actively controlled. Reasons for developing a control plan include the following: • A motivated insider with the right set of technical skills could easily execute this attack. An effective set of controls will reduce the probability of occurrence. • The impact of this risk (i.e., moderate) is high enough to warrant taking action. An effective set of controls will reduce the impact of and recovery costs for this risk. • This risk affects the customer base and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

B.2 Inherited Replay Attack (Risk 2)

B.2.1 Security Risk Scenario

An attacker targets an alert originator (AO) to capture legitimate WEA messages (unencrypted) and their associated AO certificates (encrypted) during transmission. She intends to resend a legitimate alert repeatedly at a later time (i.e., a replay attack), hoping to annoy people who use the WEA service. The

attacker captures multiple WEA messages and selects one that will affect a large number of people, based on the geographic area targeted by the alert message.

At a later time, the attacker executes a replay attack using the captured WEA message (i.e., now considered to be an illegitimate alert). She sends the illegitimate alert (unencrypted) and associated AO certificate (encrypted) to Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN), which then performs the following activities:.

- accepts the illegitimate alert
- confirms the source as legitimate using the AO certificate
- processes the illegitimate alert
- forwards the illegitimate alert to the CMSP Gateway along with the appropriate certificate

The attacker then repeatedly sends the same illegitimate alert to IPAWS-OPEN, which processes each alert and forwards it to the CMSP Gateway. Each illegitimate alert is accepted by the CMSP Gateway and validated as being legitimate.

The CMSP Gateway converts each illegitimate message to CMAM format, performs geo-targeting of each message, and then sends each illegitimate message to designated cell sites. Each illegitimate CMAM message is received by cell sites, which then broadcast the CMAM message to mobile devices. As a result of this attack, people receive the same illegitimate alert repeatedly on their mobile devices.

Many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier's customer service operators. A large number of recipients turn off the WEA function on their phones in response to the attack.

The carrier responds to the attack by restricting messages temporarily from the Federal Alert Gateway. The carrier works with FEMA and the AO to resolve the upstream issues that led to the attack. Once the upstream issues are addressed, the carrier allows messages from the Federal Alert Gateway to be received and processed.

As a result of the attack, some customers leave their carrier for other carriers. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

B.2.2 Risk Statement

IF the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, **THEN** customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

B.2.3 Threat Components

Component	Description
Threat	The carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area.
Actor	The actor is a person with an outsider's knowledge of the WEA service.
Motive	The threat is a deliberate and malicious act. In this attack, the attacker is considered to be a prankster or vandal.
Goal	The actor seeks to gain notoriety in the community of cyber attackers by executing an attack that gains media publicity. If this is a major carrier, the attack will also erode trust in the carrier as well as the WEA service (e.g., people will turn off alerts) due to the large impact.
Outcome	Illegitimate alerts are sent to the carrier's mobile devices, which will trigger alert sounds (integrity issue).
Means	The actor needs only a networked computer and the expertise to capture an alert in transit so that it can be replayed.
Threat complexity	The attack is moderately complex, requires technical skills and requires moderate preparation to execute.
Attack summary	The attacker exploits a weak point in the WEA service—AO security. From the CMSP perspective, carriers inherit this risk from an upstream exploit. The attacker repeatedly replays a previous alert to annoy recipients of the WEA service by repeatedly sending an outdated alert to recipients' mobile devices. This attack tests a carrier's ability to detect and respond to problems that originate upstream. A carrier will need a robust capability to monitor the behavior of its network to determine when the volume of messages exceeds accepted thresholds.
Additional context	Replay attacks are fairly common. Mobile devices could be sent an alert repeatedly unless there is an upstream detection and filtering capability.

B.2.4 Threat Sequence Table

Threat Step		Focus	Enabler	Candidate Control
T1.	An attacker captures an alert and associated certificate from an AO.	Organization AO—alert transmission process Technology Alert originating system (AOS)	AO is vulnerable to a replay attack. [Multiple enablers in the AO organization and infrastructure.]	[Upstream activity. Beyond a carrier's control.]
T2.	At a later time, the attacker repeatedly sends the captured alert (i.e., illegitimate alert) and AO certificate to IPAWS-OPEN.	Technology IPAWS-OPEN	AO certificates do not expire.	[Upstream activity. Beyond a carrier's control.]
T3.	IPAWS-OPEN accepts the illegitimate alerts, confirms the source as legitimate (using the AO certificate), processes the illegitimate alerts and forwards them to the CMSP Gateway.	Technology IPAWS-OPEN	Insufficient network monitoring practices within IPAWS-OPEN can enable the replay attack. [Multiple enablers in the FEMA organization and infrastructure.]	[Upstream activity. Beyond a carrier's control.]
T4.	CMSP Gateway accepts illegitimate alerts and converts them to CMAM format.	Technology CMSP Gateway	Lack of monitoring for abnormal traffic patterns or volume (e.g., spikes in traffic) could allow the replayed alerts to be processed.	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			Insufficient monitoring of alert content for duplicate messages could allow duplicate alerts to be processed.	The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
T5.	CMSP Gateway performs geo-targeting of illegitimate messages.	Technology CMSP Gateway	The CMSP Gateway performs geo-targeting automatically based on data in the alert message it receives from the Federal Alert Gateway.	N/A
T6.	CMSP Gateway sends illegitimate messages to selected cell sites.	Technology CMSP Gateway	The CMSP Gateway sends illegitimate messages to selected cell sites automatically.	N/A

B.2.5 Workflow Consequences Table

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
			The carrier implements an incident response capability to minimize the consequences of the event.
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.	Recipients can disable the WEA service on their mobile devices.

B.2.6 Stakeholder Consequences Table

Consequence	Stakeholder	Amplifier	Candidate Control
Recipients of the alert messages quickly become annoyed at receiving the same alert repeatedly.	Recipients	Knowledge of the Common Alerting Protocol (CAP)-compliant format can enable the attacker to determine the geographic area being targeted by each alert. The attacker can select an alert message that affects a large number of recipients for the replay attack.	The carrier implements an incident response capability to minimize the consequences of the event.
Many recipients complain to the carrier's customer service operators.	Recipients	Knowledge of the CAP-compliant format can enable the attacker to determine the geographic area being targeted by each alert. The attacker can select an alert message that affects a large number of recipients for the replay attack.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages.
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	FEMA Carrier	People's ability to disable the WEA service on their mobile devices helps them deal with the attack. They might decide not to (or might forget to) re-enable the WEA service after the attack.	The carrier implements an incident response capability to minimize the consequences of the event.
The carrier responds to the attack. The carrier traces the Federal Alert Gateway that is sending the replay attack to the CMSP Gateway and restricts messages from that gateway. The carrier works with FEMA and the AO to resolve upstream issues. Once upstream issues are addressed, the carrier allows messages from the affected Federal Alert Gateway.	Carrier FEMA AO	The attacker is located in the affected geographic region and is monitoring the WEA messages on a mobile device. When the alerts stop, the attacker could attempt to send messages through another AO. Note: Disallowing messages from a Federal Alert Gateway could prevent the receipt of a legitimate alert from that gateway. This is a risk.	The carrier implements a recovery plan to minimize the consequences of the event.
People leave the carrier for another carrier because of the incident.	Carrier	Knowledge of the CAP-compliant format can enable the attacker to determine the geographic area being targeted by each alert. The attacker can select an alert message that affects a large number of recipients for the replay attack.	The carrier implements a recovery plan to minimize the consequences of the event.
People lose trust in the WEA service.	FEMA Carrier	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.	The carrier implements a recovery plan to minimize the consequences of the event.

B.2.7 Risk Measures

Measure	Value	Rationale
Probability	Remote	This attack can occur, but it is not likely to occur often. It has "an outside chance" of occurring. Reasons for categorizing the probability as remote include the following: • The triggering attack (i.e., the attack on the AO) is moderately complex, requires technical skills, and requires moderate preparation to execute. • A large number of AOs across the country provide many targets for the triggering attack. • AOs have varying degrees of security controls in place. Some AOs (and their AOS vendors) likely have implemented effective security controls, while others likely have not. An attacker can look for a weak link with respect to security controls. • Public data with respect to similar attacks do not indicate that the probability is higher than remote.
Impact	Medium	The impact on the organization is moderate. The organization will be able to recover from the attack. Recovery will require a moderate investment of organizational capital and resources. Reasons for categorizing the probability as remote include the following: • Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of revenue. • Carriers already maintain help desk capabilities to respond to customer complaints. • Tech-savvy customers can turn off the WEA service. • The costs required to recover from this attack (e.g., public relations outreach) will not be excessive. • Public data indicate that the impact of this type of attack is generally moderate.
Risk exposure	Low	

B.2.8 Control Approach

Approach	Rationale
Plan	This risk will be actively controlled. Reasons for developing a control plan include the following: • A motivated attacker with the right set of technical skills could easily trigger this attack by targeting an AO. Effective monitoring at the CMSP Gateway will reduce the probability of occurrence (from the carrier's perspective). • The impact of this risk (i.e., moderate) is high enough to warrant taking action. An effective set of controls will reduce the recovery costs for this risk. • This risk affects the customer base and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

B.3 Malicious Code in the Supply Chain (Risk 3)

B.3.1 Security Risk Scenario

An employee at a subcontractor of a carrier's WEA alerting system vendor has followed the pursuits of the attacker community for some period of time. He gets excited thinking about executing attacks like those that he follows online. One day, the subcontractor's employee becomes upset at a perceived slight from some of the carrier's employees during a technical exchange. He does not believe that that the carrier's technical staff has shown him the respect that he is due. As a result, he decides to execute an attack against the carrier.

The subcontractor's employee (hereafter referred to as the actor) performs reconnaissance to obtain subcontractor and vendor artifacts that describe the carrier's WEA alerting system, such as requirements specifications, architecture and design documents and source code. The actor gains access to artifacts that provide technical details of the carrier's WEA alerting system. He studies the documents in great detail, looking for any weaknesses that he can exploit. Finally, the actor develops an attack strategy. He intends to develop malicious code designed to (1) disseminate an alert as broadly as possible (i.e., override the system's geo-targeting capability) and (2) change the priority of all alerts into Presidential alerts. After much effort, he successfully develops the malicious code.

The actor intends to plant the malicious code in a software update that the subcontractor is developing for the carrier's WEA alerting system. Hoping to cover his tracks when executing the attack, the actor intends to plant the malicious code using credentials (e.g., user ID and password) that he will steal from a colleague. The actor uses password cracker software (such as L0phtCrack) to retrieve passwords for user accounts on the subcontractor's development system. The actor then accesses the development system using a colleague's user ID and password that he has stolen. He inserts the malicious code into a software update for the carrier's WEA alerting system.

The subcontractor's technical staff completes development and testing of the software update, with the inserted malicious code, and delivers it to the vendor. The technical staff from the vendor's development team does not detect the malicious code during testing and accept the software update. The vendor then integrates the subcontractor's software update into the latest version of the WEA alerting software. Acceptance testing by the carrier does not detect the malicious code, and the latest version of the WEA alerting software, with the malicious code, is deployed in the carrier's infrastructure.

The malicious code waits until the carrier receives an alert from the CMSP Gateway. When an alert is received, the malicious code expands the region receiving the alert as broadly as possible and changes the priority of the alert into a Presidential alert.

Recipients receive and read the alert on their wireless devices. Recipients outside of the region covered by the actual alert become annoyed at receiving an alert designated for another geographic area. In addition, receiving a presidential alert can alarm some recipients. Many recipients try to turn off the WEA function on their phones. This does not work because people cannot opt out of receiving a Presidential alert. Thus, many people continually receive Presidential alerts related to severe weather affecting other counties or states. Many recipients complain to the carrier's customer service operators.

The carrier responds to the attack by taking the infected WEA alerting system offline. The broadcast of the Presidential alerts stop. The carrier then responds aggressively to the attack by investigating the

source of the attack, locating the malicious code and removing that code from its infrastructure. Once the carrier has removed the malicious code is removed from its WEA alerting system, the carrier brings the system back online. The cost to recover from the attack is considerable.

As a result of the attack, some customers leave their carrier for other carriers. Because of the high-profile nature of the attack (i.e., issuing illegitimate Presidential alerts), the media covers the attack extensively. The media coverage of the attack helps to amplify the public's loss of trust in the WEA service.

B.3.2 Risk Statement

IF malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, **THEN** customers could become annoyed with the carrier. The carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

B.3.3 Threat Components

Component	Description
Threat	An employee at a subcontractor of the carrier's WEA alerting system vendor inserts malicious code into a software update for the alerting system. The malicious code (1) disseminates the alert as broadly as possible (i.e., overrides the system's geo-targeting capability) and (2) changes the priority of all alerts into Presidential alerts.
Actor	The actor is an employee at a subcontractor of the carrier's WEA alerting system vendor.
Motive	The threat is a deliberate and malicious act. The actor is disgruntled (e.g., upset at a perceived slight from some of the carrier's employees during a technical exchange).
Goal	The actor seeks to erode trust in the carrier. The attack will also erode trust in the vendor and subcontractor. If this is a major carrier, the attack will also erode trust in the WEA service (e.g., people will turn off alerts) due to the large impact.
Outcome	Modified alerts (in terms of coverage and priority) are sent to the carrier's wireless devices (integrity issue).
Means	The actor works for a subcontractor in the carrier's supply chain. The actor requires access to subcontractor and vendor artifacts (e.g., requirements, architecture, design, source code) that describe the carrier's WEA alerting system.
Threat complexity	The attack is complex, requires technical skills, and requires significant preparation to execute.
Attack summary	An employee at a subcontractor of the carrier's WEA alerting system vendor (i.e., the actor) inserts malicious code into a software update for the WEA alerting system. The vendor integrates the software update, with the malicious code, into a new version of WEA alerting system's software. Acceptance testing by the carrier does not detect the malicious code and the updated WEA alerting software is deployed in the carrier's infrastructure. Once it is installed on the carrier's WEA alerting system, the malicious code waits until the carrier receives an alert from the CMSP Gateway. The malicious code then expands the region receiving the alert as broadly as possible and changes the priority of the alert into Presidential alerts.
Additional context	N/A

B.3.4 Threat Sequence Table

Threat Step		Focus	Enabler	Candidate Control
T1.	An employee at a subcontractor of the carrier's WEA alerting system vendor (i.e., the actor) becomes upset at a perceived slight from some of the carrier's employees during a technical exchange.	Organization Subcontractor, vendor and carrier interaction	Poor communication during the technical exchange.	Selected employees receive training that is focused on interacting with people from other organizations.
T2.	The actor performs reconnaissance to obtain subcontractor and vendor artifacts (e.g., requirements, architecture, design, source code) that describe the carrier's WEA alerting system.	Technology Subcontractor's systems and networks Vendor's systems and networks	Insufficient access controls in the subcontractor's systems and networks [subcontractor]. Insufficient monitoring of the subcontractor's systems and networks [subcontractor]. Insufficient access controls in the vendor's systems and networks [vendor]. Insufficient monitoring of the vendor's systems and networks [vendor].	[Vendor and subcontractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the organization when a security incident is detected.
T3.	The actor develops malicious code designed to disseminate an alert as broadly as possible (i.e., overriding the system's geo-targeting capability) and change the priority of all alerts into Presidential alerts.	Technology Malicious code development	Availability of technical details (e.g., requirements, architecture, design, source code) about the carrier's WEA alerting system [subcontractor and vendor].	[Vendor and subcontractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the organization when a security incident is detected.

Threat Step		Focus	Enabler	Candidate Control
T4.	The actor uses password cracker software (e.g., L0phtCrack) to retrieve passwords for user accounts on the subcontractor's development system.	Technology Subcontractor's systems and networks	Insufficient authentication controls (e.g., lack of encryption of user credentials) [subcontractor].	[Subcontractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the organization when a security incident is detected.
T5.	The actor accesses the subcontractor's development system using a colleague's user id and password.	Technology Subcontractor's development system	Insufficient authentication controls (e.g., lack of encryption of user credentials) [subcontractor].	[Subcontractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the organization when a security incident is detected.
T6.	The actor inserts the malicious code into a software update for the WEA alerting system.	Technology Subcontractor software update for the WEA alerting system	An insufficient change-management/configuration-management capability can prevent the organization from knowing if software has been modified inappropriately [subcontractor].	[Vendor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the organization when a security incident is detected.

Threat Step		Focus	Enabler	Candidate Control
T7.	The subcontractor completes development and testing of the software update and delivers it to the vendor.	Technology Subcontractor software update for the WEA alerting system	Subcontractor testing practices do not look for malicious code [subcontractor].	[Subcontractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities. All contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code. All contracts require third parties to immediately notify the organization when a security incident is detected.
T8.	The vendor does not detect the malicious code during testing and accepts the software module.	Technology Subcontractor software update for the WEA alerting system	Software code reviews do not look for malicious code [vendor]. Unit acceptance testing practices do not look for malicious code [vendor].	[Vendor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities. All contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code. All contracts require third parties to immediately notify the organization when a security incident is detected.
T9.	The vendor integrates the software update with the malicious code into a new version of its WEA alerting system's software.	Technology New version of WEA alerting software	Software code reviews do not look for malicious code [vendor]. Integration testing practices do not look for malicious code [vendor].	[Vendor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of supply-chain security standards and requirements in contracts with vendors.	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities. All contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code. All contracts require third parties to immediately notify the organization when a security incident is detected.

Threat Step		Focus	Enabler	Candidate Control
T10.	Acceptance testing by the carrier does not detect the malicious code and the updated WEA alerting software is deployed in the carrier's infrastructure.	Technology WEA alerting system	Acceptance testing practices do not look for malicious code.	The carrier's technical staff conducts security reviews of source code. The carrier's technical staff looks for malicious code in software by running static and dynamic analysis tools prior to accepting software from third parties.
T11.	Once it is installed on the carrier's WEA alerting system, the malicious code waits until an alert is received from the CMSP Gateway. The malicious code then expands the region receiving the alert as broadly as possible and changes the priority of the alert into a Presidential alert.	Technology Malicious code Carrier's WEA alerting software	Insufficient monitoring of the WEA alerting system for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.
			Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.	The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately. The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.

B.3.5 Workflow Consequences Table

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure forwards the illegitimate Presidential alert to mobile devices in the expanded geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
			The carrier implements an incident response capability to minimize the consequences of the event.
People with WEA-capable mobile devices supported by the carrier receive the illegitimate Presidential alert.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.	N/A

B.3.6 Stakeholder Consequences Table

Consequence	Stakeholder	Amplifier	Candidate Control
Recipients receive and read the alert on their wireless devices.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients. Knowledge of the system's alert prioritization capability can enable the attacker to increase the priority of an alert to a Presidential alert.	N/A
Recipients outside of the region covered by the alert become annoyed at receiving the alert.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	The carrier implements an incident response capability to minimize the consequences of the event.
Receiving a presidential alert alarms some recipients.	Recipients	Knowledge of the system's alert prioritization capability can enable the attacker to increase the priority of an alert to a Presidential alert.	The carrier implements an incident response capability to minimize the consequences of the event.
A large number of recipients try to turn off the WEA function on their phones. This does not work because people cannot opt out of receiving a Presidential alert.	Recipients FEMA Carrier	People cannot disable Presidential alerts on their mobile devices.	The carrier implements a recovery plan to minimize the consequences of the event.

Consequence	Stakeholder	Amplifier	Candidate Control
Many recipients complain to the carrier's customer service operators.	Carrier	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients. People cannot disable Presidential alerts on their mobile devices.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages.
The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable.	Carrier	An insufficient change-management/configuration-management capability can increase the time it takes to identify unauthorized changes and recover from the attack. This can amplify the recovery costs.	The carrier implements/improves a change-management/configuration-management system. The carrier implements an incident response capability to minimize the consequences of the event.
People leave the carrier for other carriers because of the incident.	Carrier	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients. Knowledge of the system's alert prioritization capability can enable the attacker to increase the priority of an alert to a Presidential alert.	The carrier implements a recovery plan to minimize the consequences of the event.
People lose trust in the WEA service.	FEMA Carrier	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.	The carrier implements a recovery plan to minimize the consequences of the event.

B.3.7 Risk Measures

Measure	Value	Rationale
Probability	Rare	The scenario is considered to be uncommon or unusual. This is a very sophisticated, complex attack that requires significant technical skills and considerable preparation to execute. Not many people have the combination of technical skills and motivation to conduct this type of attack.
Impact	Medium	The impact on the organization is moderate. The organization will be able to recover from the attack. Recovery will require a moderate investment of organizational capital and resources.
Risk exposure	Minimal	

B.3.8 Control Approach

Approach	Rationale
Plan	This risk will be actively controlled. A control plan will be developed for risks that have medium or higher impacts. Reasons for developing a control plan include the following: • The impact of this risk (i.e., moderate) is high enough to warrant taking action. An effective set of controls will reduce the response and recovery costs for this risk. • This risk affects the customer base and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

B.4 Denial of Service (Risk 4)

B.4.1 Security Risk Scenario

An outside actor with malicious intent is planning a physical (i.e., terrorist) attack on a crowd that is gathered in a public place (e.g., for a sporting event or concert). She plans to conduct a simultaneous denial-of-service (DoS) attack on a carrier's WEA alerting system to prevent the dissemination of a WEA message about the attack. The goal is to prevent people from learning about the physical attack as long as possible in order to maximize the physical harm inflicted upon the crowd.

Because the carrier is known to employ rigorous cybersecurity practices, the actor decides to target one of the carrier's business partners that has trusted access to the carrier's internal network. She performs reconnaissance on the carrier to determine which business partners might make good targets for an attack. This involves examining publicly available information about the carrier and its business partners, as well as attempts to gain information from the carrier's employees through social engineering.

Based on the information acquired through various reconnaissance activities, the actor decides to target a third-party contractor that has legitimate access to the carrier's internal network. She performs additional reconnaissance on the contractor's infrastructure to obtain information needed to gain access. The contractor is not vigilant about its cybersecurity practices and is a relatively easy target for an attacker.

The actor exploits several well-known vulnerabilities in the contractor's perimeter security and gains access to a computer in the contractor's internal network. She then uses this access to perform additional reconnaissance of the contractor's internal network. Jumping from computer to computer until she gains access to a specific contractor system that has trusted access to the carrier's infrastructure, the

actor uses the contractor's trusted access to bypass the carrier's perimeter security controls. She performs reconnaissance on the carrier's internal network to obtain information needed for targeting the WEA alerting system. The actor scans the carrier's internal network for vulnerable computers and then exploits vulnerabilities to gain access to those computers. She installs malicious code on the vulnerable computers that will be used to initiate the DoS attack. The cyber component of the attack is ready.

The actor initiates the physical attack. At the same time, the actor instructs the infected computers to send a flood of requests to the carrier's WEA alerting system, which consumes the system's available bandwidth. An AO (e.g., from law enforcement) enters a legitimate WEA message into its AOS. The legitimate WEA message is transmitted to the carrier's computing infrastructure from the CMSP Gateway. The carrier's WEA alerting system is unable to process the legitimate alert because the system's bandwidth is consumed by the DoS attack, however.

People are put in harm's way from the physical attack, leading to injuries and death. The carrier tries to mount a response to the attack. It eventually disseminates the alert through other available channels. Because of the DoS attack, however, people do not receive the WEA message in a timely manner. As a result, people at the event are unaware of what is happening and do not react, leading to additional harm.

After the attack, the carrier removes the malicious code from its infrastructure. As part of its recovery plan, the carrier terminates its relationship with the contractor that was responsible for the DoS attack. The carrier also begins more rigorous auditing of the security practices of all organizations with whom it has contractual relationships. The carrier updates its contracting language to be more specific about the security obligations of its contractors.

The cost to recover from the attack is considerable. Media outlets learn about the role of the DoS attack in amplifying the impact of the incident and publicize this fact in their reports. The carrier receives more than its share of the blame for the consequences of the attack. Ultimately, the court system could hold the carrier liable for financial penalties. In addition, the reputation of the carrier could be damaged with the general public, leading to a loss of business. Finally, many people lose trust in the WEA service.

B.4.2 Risk Statement

IF an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, **THEN** people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

B.4.3 Threat Components

Component	Description
Threat	An outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack.
Actor	The actor is a person or group with an outsider's knowledge of the WEA service and the carrier's infrastructure and its contractors.
Motive	The threat is a deliberate and malicious act (i.e., a terrorist attack).
Goal	To inflict physical injury on a large number of people (e.g., people gathered for a sporting event or concert)
Outcome	A legitimate alert is prevented from reaching constituents (availability issue).
Means	For the cyber part of the attack, the actor needs only a networked computer and access to public documents that describe the WEA service.
Threat complexity	The attack is complex and requires significant preparation to execute.
Attack summary	The actor plans a physical attack on a crowd that is gathered in a public place (e.g., for a sporting event or concert). The actor plans to conduct a simultaneous DoS attack on the carrier's WEA alerting system. As the physical attack is launched, the actor initiates the DoS attack on the carrier's WEA alerting system. Most people at the venue do not have access to other means of receiving alert information and are unaware of the attack. People do not take evasive action, which helps to maximize the damage to people's health and safety.
Additional context	The actor must time the attack to coincide with an event where a large crowd will gather.

B.4.4 Threat Sequence Table

Threat Step		Focus	Enabler	Candidate Control
T1.	The actor performs reconnaissance on the carrier and its business partners. This involves examining publicly available information about the carrier and its business partners as well as attempts to gain information from the carrier's employees through social engineering.	Technology Web servers with information about the carrier Third-party websites with information about the carrier's business dealings Organization Knowledge of carrier employees	The carrier's website includes detailed information about its business relationships.	The carrier restricts the dissemination of information based on risk.
			Third-party websites (e.g., news websites) provide information about the carrier's business relationships [contractor].	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
			The carrier's employees are vulnerable to social engineering.	All employees are required to attend security awareness training, which addresses the topic of social engineering. Selected employees participate in training simulations that include social engineering attacks.
T2.	The actor decides to target a third-party contractor that has legitimate access to the carrier's network. The actor performs reconnaissance on the contractor's infrastructure to get information needed to gain access.	Technology Contractor's systems and networks	Lack of security patching on contractor systems and network devices [contractor] Insufficient security controls implemented in contractor systems and network devices [contractor] Insufficient monitoring of contractor systems and network devices [contractor]	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]

Threat Step		Focus	Enabler	Candidate Control
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
T3.	The actor breaks through the contractor's perimeter security and gains access to a computer in the contractor's internal network.	Technology Contractor's systems and networks	Lack of security patching on contractor perimeter security devices [contractor] Insufficient security controls implemented on contractor perimeter security devices [contractor] Insufficient monitoring of contractor internal systems and network devices [contractor]	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
T4.	The actor performs additional reconnaissance of the contractor's internal network.	Technology Contractor's systems and networks	Lack of security patching on contractor systems and network devices [contractor] Insufficient security controls implemented in contractor internal systems and network devices [contractor] Insufficient monitoring of contractor internal systems and network devices [contractor]	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]

Threat Step		Focus	Enabler	Candidate Control
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
T5.	The actor moves from computer to computer until she gains access to the contractor system that has legitimate access to the carrier's infrastructure.	Technology Contractor's systems and networks	Lack of security patching on contractor systems and network devices [contractor] Insufficient security controls implemented in contractor internal systems and network devices [contractor] Insufficient monitoring of contractor internal systems and network devices [contractor]	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
T6.	The actor uses the contractor's trusted access to the carrier's infrastructure to bypass the carrier's perimeter security controls.	Technology Contractor's systems and networks Carrier's systems and networks	Trusted access of the carrier's computing infrastructure by the contractor	The carrier monitors trusted connections for abnormal activity and responds appropriately.
			Insufficient monitoring of contractor internal systems and network devices [contractor]	[Contractor should implement security controls to address enablers in infrastructure. This is beyond a carrier's direct control.]

Threat Step		Focus	Enabler	Candidate Control
			Insufficient specification of security standards and requirements in contracts with contractors	All contracts with third parties specify security standards that must be met across the supply chain. All contracts with third parties require third parties to participate in independent security audits when requested. All contracts require third parties to immediately notify the carrier when a security incident is detected.
			Insufficient monitoring of the carrier network for suspicious or abnormal activity can result in unauthorized access to systems	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
T7.	The actor performs reconnaissance on the carrier's internal network to obtain information needed for targeting the WEA alerting system.	Technology Carrier's systems and networks	Insufficient monitoring of the carrier network for suspicious or abnormal activity can enable unauthorized users to collect network and system data	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
T8.	The actor scans the carrier's internal network for vulnerable computers.	Technology Computers in the carrier's infrastructure	Lack of or inconsistent security patching on carrier systems and network devices	The carrier patches all systems and network devices as appropriate.
			Insufficient security controls implemented in carrier internal systems and network devices leads to vulnerabilities	Security controls are implemented in systems and network devices based on cybersecurity risk. The carrier configures its systems and network devices securely.
			Insufficient monitoring of carrier internal systems and network devices	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
T9.	The actor exploits vulnerabilities on targeted computers to gain access to those computers.	Technology Vulnerable computers in the carrier's infrastructure	Vulnerabilities in carrier computers	The carrier performs periodic vulnerability assessments. The carrier acts on the results of vulnerability assessments (i.e., addresses vulnerabilities).
T10.	The actor installs malicious code on the vulnerable computers.	Technology Vulnerable computers in the carrier's infrastructure	Vulnerabilities in carrier computers	The carrier performs periodic vulnerability assessments. The carrier acts on the results of vulnerability assessments (i.e., addresses vulnerabilities).

Threat Step		Focus	Enabler	Candidate Control
			Insufficient monitoring of carrier internal systems and network devices	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
T11.	The actor instructs the infected computers to send a flood of requests to the carrier's WEA alerting system, which consumes the system's available bandwidth.	Technology Vulnerable computers connected to the internet Carrier's WEA alerting system	Insufficient monitoring of carrier internal systems and network devices	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately. The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
T12.	The actor initiates the physical attack.	Public Event Crowd that is gathered in a public place (e.g., for a sporting event or concert)	N/A	N/A
T13.	An AO enters a legitimate WEA message into its AOS.	Organization AO Technology AOS	N/A	N/A
T14.	The legitimate WEA message is transmitted to the carrier's computing infrastructure from the CMSP Gateway.	Technology CMSP Gateway Carrier's computing infrastructure	N/A	N/A
T15.	The carrier's WEA alerting system is unable to process the legitimate alert because the system's bandwidth is consumed by the DoS attack.	Technology Carrier's WEA alerting system	The bandwidth of the WEA alerting system is consumed by the DoS attack.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier's WEA alerting system has a backup capability that uses a separate communication channel. The carrier switches to a backup WEA alerting system (that uses a separate communication channel) to issue the alert. The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.

B.4.5 Workflow Consequences Table

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure is unable to forward the WEA message to mobile devices in the targeted geographic area.	Carrier infrastructure	Dissemination of WEA messages through the carrier's infrastructure is a push process. The carrier's infrastructure can only process alerts that are forwarded by the carrier's WEA alerting system.	N/A
People with WEA-capable mobile devices in the targeted geographic area supported by the carrier do not receive the alert.	Mobile devices	Dissemination of WEA messages to mobile devices in the targeted geographic area is a push process. Mobile devices can only receive alerts that are forwarded by the carrier's infrastructure.	N/A

B.4.6 Stakeholder Consequences Table

Consequence	Stakeholder	Amplifier	Candidate Control
People are put in harm's way from the physical attack, leading to injuries and death.	Public	The impact on people's health and safety correlates with the delay in disseminating the alert to the public.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
		The impact of this consequence will increase as more people come to use the WEA service as the primary source for receiving emergency alert messages (i.e., people trust the WEA service).	The carrier implements an incident response capability to minimize the consequences of the event. The carrier's WEA alerting system has a backup capability that uses a separate communication channel. The carrier switches to a backup WEA alerting system (that uses a separate communication channel) to issue the alert.
People are unaware of what is happening and do not react, leading to additional harm.	Public	Lack of timely notification keeps people unaware of health and safety issues.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.

Consequence	Stakeholder	Amplifier	Candidate Control
		This consequence will increase if the actor targets multiple carriers.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
The carrier responds to the attack. It takes action to disseminate the alert through other channels (if they exist).	Carrier	An insufficient monitoring capability can increase the time it takes to identify and recover the DoS attack.	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately. The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
		Lack of a backup channel for disseminating alerts can amplify the consequences of the attack.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier's WEA alerting system has a backup capability that uses a separate communication channel. The carrier switches to a backup WEA alerting system (that uses a separate communication channel) to issue the alert.
The carrier recovers from the attack. It conducts an investigation and removes the malicious code from its infrastructure. The cost to do so is considerable.	Carrier	An insufficient monitoring capability can increase the time it takes to identify and recover the DoS attack. This can amplify the recovery costs. Insufficient disaster recovery planning can slow recover activities and amplify the recovery costs.	The carrier implements a recovery plan to minimize the consequences of the event.
The carrier could be held liable for damages.	Carrier	The carrier is shown to be negligent in its cybersecurity practices.	The carrier has third parties perform periodic cybersecurity audits to evaluate whether the carrier demonstrates due diligence with respect to cybersecurity. The carrier is insured for damages produced by cybersecurity breaches. The carrier implements a recovery plan to minimize the consequences of the event.

Consequence	Stakeholder	Amplifier	Candidate Control
		The carrier responds slowly to the event. This negligence could be considered when legal penalties are awarded to affected parties.	The carrier implements an incident response capability to minimize the consequences of the event. The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately. The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
The reputation of the carrier could be damaged.	Carrier	The media's publicizing of the WEA attack and the attack on the carrier can erode trust in the carrier.	The carrier implements a recovery plan to minimize the consequences of the event.
The reputation of WEA could be damaged.	FEMA Carrier AOs	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.	The carrier implements a recovery plan to minimize the consequences of the event.
People leave the carrier for another carrier because of the incident.	Carrier	The media's publicizing of the WEA attack and the attack on the carrier can erode trust in the carrier.	The carrier implements a recovery plan to minimize the consequences of the event.
People lose trust in the WEA service.	FEMA Carrier AOs	The media's publicizing of the WEA attack and the resulting problems with mobile devices can erode the public's trust in the WEA service.	The carrier implements a recovery plan to minimize the consequences of the event.

B.4.7 Risk Measures

Measure	Value	Rationale
Probability	Rare	The scenario is considered to be uncommon or unusual. This is a very sophisticated, complex attack that requires significant technical skills and considerable preparation to execute. Not many people have the combination of technical skills and motivation to conduct this type of attack. It also must be timed to coincide with a physical attack.
Impact	Maximum	The impact on the organization is severe due to health and safety issues and loss of life. The carrier may be subject to significant financial penalties.
Risk exposure	Medium	

B.4.8 Control Approach

Approach	Rationale
Plan	This risk will be actively controlled. A control plan will be developed for risks that have medium or higher impacts. Reasons for developing a control plan include the following: • The impact of this risk (i.e., maximum) warrants taking action. An effective set of controls will reduce the response and recovery costs for this risk. • This risk affects the health and safety of customers and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

Appendix C Control Summary

This appendix provides a summary of the controls identified for the four commercial mobile service provider (CMSP) Wireless Emergency Alerts (WEA) alerting risks. Our application of the Security Engineering Risk Analysis (SERA) Method produced a set of controls for each security risk scenario. In all, we identified 35 controls across the four risk scenarios.

Table 25 describes the 35 controls identified during this study. The table provides the following information regarding controls and the related risks:

- *Control category* (Column 1): The category to which a control belongs. Examples of control categories include human resources, physical security, technical monitoring and incident response.
- *Control* (Column 2): A specific control that was identified during the risk analysis.
- *Risks R1 through R4* (Columns 3–6): Risk scenarios analyzed during the study. An "X" in the cell representing the intersection of a row (control) and column (risk scenario) indicates that the given control was identified for that particular risk scenario. A blank cell indicates that the control does not apply to that risk scenario.

The mapping in Table 25 is useful for determining which controls mitigate more than one risk. The table can be used by CMSPs when setting their priorities for allocating resources for controlling security risks. Common controls provide opportunities for CMSP decision makers to leverage resources across multiple risks. Based on the information provided in Table 25, the following controls mitigate two or more security risk scenarios:

- *Technical monitoring*: The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately (four scenarios).
- *Technical monitoring*: The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately (four scenarios).
- *Incident response*: The carrier implements an incident response capability to minimize the consequences of the event (four scenarios).
- *Disaster recovery*: The carrier implements a recovery plan to minimize the consequences of the event (four scenarios).
- *Technical monitoring*: The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately (three scenarios).
- *Incident response*: The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages (three scenarios).
- *Contracting*: All contracts with third parties specify security standards that must be met across the supply chain (two scenarios).
- *Contracting*: All contracts with third parties require third parties to participate in independent security audits when requested (two scenarios).
- *Contracting*: All contracts require third parties to immediately notify the carrier when a security incident is detected (two scenarios).

- *Change management*: The carrier implements/improves a change-management/configuration-management system (two scenarios).
- *Incident response*: Recipients can disable the WEA service on their mobile devices (two scenarios).

Table 25: Control Map

Control Category	Control	Risk 1: Insider Sends False Alerts	Risk 2: Inherited Replay Attack	Risk 3: Malicious Code in the Supply Chain	Risk 4: Denial of Service
Human Resources	The carrier's managers are trained to provide constructive feedback on performance issues.	X			
	The carrier's managers recognize inappropriate behavior when it occurs and respond appropriately.	X			
	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.	X			
	Selected employees receive training that is focused on interacting with people from other organizations.			X	
Training	All employees are required to attend security awareness training, which addresses the topic of social engineering.				X
	Selected employees participate in training simulations that include social engineering attacks.				X
Contracting	All contracts with third parties specify security standards that must be met across the supply chain.			X	X
	All contracts with third parties require third parties to participate in independent security audits when requested.			X	X
	All contracts require third parties to immediately notify the carrier when a security incident is detected.			X	X
	All contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities.			X	
	All contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code.			X	
Physical Security	The carrier implements physical access controls for workstations and workspaces.	X			
Change Management	The carrier implements/improves a change-management/configuration-management system.	X		X	
Access Control	The carrier controls access to sensitive information based on organizational role.	X			

Control Category	Control	Risk 1: Insider Sends False Alerts	Risk 2: Inherited Replay Attack	Risk 3: Malicious Code in the Supply Chain	Risk 4: Denial of Service
Information Management	The carrier restricts the dissemination of information based on risk.				X
Vulnerability Management	The carrier patches all systems and network devices as appropriate.				X
	The carrier performs periodic vulnerability assessments.				X
	The carrier acts on the results of vulnerability assessments (i.e., addresses vulnerabilities).				X
System Architecture	Security controls are implemented in systems and network devices based on cybersecurity risk.				X
	The carrier's WEA alerting system has a backup capability that uses a separate communication channel.				X
System Configuration	The carrier configures its systems and network devices securely.				X
Code Analysis	The carrier's technical staff conducts security reviews of source code.			X	
	The carrier's technical staff looks for malicious code in software by running static and dynamic analysis tools prior to accepting software from third parties.			X	
Technical Monitoring	The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.	X	X	X	
	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.	X	X	X	X
	The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.			X	
	The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.	X	X	X	X
	The carrier monitors trusted connections for abnormal activity and responds appropriately.				X
Independent Reviews	The carrier has third parties perform periodic cybersecurity audits to evaluate whether the carrier performs due diligence with respect to cybersecurity.				X
Incident Response	The carrier implements an incident response capability to minimize the consequences of the event.	X	X	X	X

Control Category	Control	Risk 1: Insider Sends False Alerts	Risk 2: Inherited Replay Attack	Risk 3: Malicious Code in the Supply Chain	Risk 4: Denial of Service
	The carrier switches to a backup WEA alerting system (that uses a separate communication channel) to issue the alert.				X
	Recipients can disable the WEA service on their mobile devices.	X	X		
	The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA messages.	X	X	X	
Disaster Recovery	The carrier implements a recovery plan to minimize the consequences of the event.	X	X	X	X
	The carrier is insured for damages produced by cybersecurity breaches.				X

Appendix D Control Strategy Questionnaire

This appendix provides a control strategy questionnaire that a carrier can use to evaluate the security posture of its Wireless Emergency Alerts (WEA) alerting system. This questionnaire establishes relative strengths and weaknesses among the 35 high-priority controls identified for the four risks analyzed in this study. An interdisciplinary team with knowledge of the WEA alerting system, the process it supports and the security controls that are currently implemented should answer the questions. The team may not be able to answer all the questions at once. Some investigation and research into available materials and evidence may be needed to reach a correct answer.

To use this questionnaire, respondents should complete the following steps for each question in the survey:

1. Read the question carefully and consider the following responses:
   - **Yes—**The answer to the question is *yes*. The vast majority of the evidence points to an answer of *yes*. Little or no evidence points to an answer of *no*.
   - **Partial—**The answer to the question is ambiguous. Some evidence points to an answer of *yes*, while other evidence points to an answer of *no*. The answer is not a clear-cut *yes* or *no*.
   - **No—**The answer to the question is *no*. The vast majority of the evidence points to an answer of *no*. Little or no evidence points to an answer of *yes.*
2. Discuss the answer to the question.
3. Select the most appropriate response (yes, partial or no), and check the corresponding box in the survey.
4. Document the rationale for the selected response. Also, document any evidence that supports the response. Examples of evidence include reports from tools (e.g., code analysis tools), security audit reports and tangible project artifacts (e.g., policy statements, project documents, architecture diagrams). Also document any minority opinions that may need to be investigated later or that may influence any decisions on prioritizing controls.

The results of this survey can be used to identify gaps in controls in the carrier's WEA alerting system. The carrier can implement missing or incomplete controls to improve the system's security posture.

Category	Control Question		Response			Rationale and Evidence
			Yes	Partial	No	
Human Resources	1.	Are the carrier's managers trained to provide constructive feedback on performance issues?	❑	❑	❑	
	2.	Do the carrier's managers recognize inappropriate behavior when it occurs and respond appropriately?	❑	❑	❑	
	3.	Does the carrier perform targeted monitoring of individuals with suspected behavioral issues and respond appropriately?	❑	❑	❑	
	4.	Do selected employees receive training that is focused on interacting with people from other organizations?	❑	❑	❑	
Training	5.	Are all employees required to attend security awareness training that addresses the topic of social engineering?	❑	❑	❑	
	6.	Do selected employees participate in training simulations that include social engineering attacks?	❑	❑	❑	
Contracting	7.	Do all contracts with third parties specify security standards that must be met across the supply chain?	❑	❑	❑	
	8.	Do all contracts with third parties require third parties to participate in independent security audits when requested?	❑	❑	❑	

Category	Control Question		Response			Rationale and Evidence
			Yes	Partial	No	
	9.	Do all contracts require third parties to immediately notify the carrier when a security incident is detected?	❑	❑	❑	
	10.	Do all contracts with third parties enable carrier technical staff to participate in code reviews and security testing activities?	❑	❑	❑	
	11.	Do all contracts with third parties enable carrier technical staff to review results of static and dynamic analysis of code?	❑	❑	❑	
Physical Security	12.	Does the carrier implement physical access controls for workstations and workspaces?	❑	❑	❑	
Change Management	13.	Does the carrier implement a change-management or configuration-management system?	❑	❑	❑	
Access Control	14.	Does the carrier control access to sensitive information based on organizational role?	❑	❑	❑	
Information Management	15.	Does the carrier restrict the dissemination of information based on risk?	❑	❑	❑	
Vulnerability Management	16.	Does the carrier patch all systems and network devices as appropriate?	❑	❑	❑	

Category	Control Question		Response			Rationale and Evidence
			Yes	Partial	No	
	17.	Does the carrier perform periodic vulnerability assessments?	❑	❑	❑	
	18.	Does the carrier act on the results of vulnerability assessments (i.e., address vulnerabilities)?	❑	❑	❑	
System Architecture	19.	Are security controls implemented in system and network devices based on cybersecurity risk?	❑	❑	❑	
	20.	Does the carrier's WEA alerting system have a backup capability that uses a separate communication channel?	❑	❑	❑	
System Configuration	21.	Does the carrier configure its systems and network devices securely?	❑	❑	❑	
Code Analysis	22.	Does the carrier's technical staff conduct security reviews of source code?	❑	❑	❑	
	23.	Does the carrier's technical staff look for malicious code in software by running static and dynamic analysis tools prior to accepting software from third parties?	❑	❑	❑	
Technical Monitoring	24.	Does the carrier monitor messages for suspicious content (e.g., illegitimate messages, duplicate messages) and respond appropriately?	❑	❑	❑	

Category	Control Question		Response			Rationale and Evidence
			Yes	Partial	No	
	25.	Does the carrier monitor its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and respond appropriately?	❑	❑	❑	
	26.	Does the carrier monitor the WEA alerting system for abnormal activity and respond appropriately?	❑	❑	❑	
	27.	Does the carrier maintain situational awareness of the WEA environment and respond to any issues appropriately?	❑	❑	❑	
	28.	Does the carrier monitor trusted connections for abnormal activity and respond appropriately?	❑	❑	❑	
Independent Reviews	29.	Does the carrier have third parties perform periodic cybersecurity audits to demonstrate that the carrier is showing due diligence with respect to cybersecurity?	❑	❑	❑	
Incident Response	30.	Does the carrier implement an incident response capability to minimize the consequences of the event?	❑	❑	❑	
	31.	Can the carrier switch to a backup WEA alerting system (that uses a separate communication channel) when needed to issue an alert?	❑	❑	❑	
	32.	Can recipients disable the WEA service on their mobile devices?	❑	❑	❑	

Category	Control Question		Response			Rationale and Evidence
			Yes	Partial	No	
	33.	Are the carrier's customer service operators trained in handling complaints about incorrect or errant WEA messages?	❑	❑	❑	
Disaster Recovery	34.	Has the carrier implemented a recovery plan to minimize the consequences of the event?	❑	❑	❑	
	35.	Is the carrier insured for damages produced by cybersecurity breaches?	❑	❑	❑	

References

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

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE[SM] Approach*. Addison-Wesley, 2002. http://www.sei.cmu.edu/library/abstracts/books/0321118863.cfm

[ATIS 2009a]
Alliance for Telecommunications Industry Solutions. *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification* (Draft Version, ATIS-TIA-J-STD-101). Alliance for Telecommunications Industry Solutions, 2009.

[ATIS 2009b]
Alliance for Telecommunications Industry Solutions. *Joint ATIS/TIA CMAS Mobile Device Behavior Specification* (Draft Version, ATIS-TIA-J-STD-100). Alliance for Telecommunications Industry Solutions, 2009.

[ATIS 2011]
Alliance for Telecommunications Industry Solutions. *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Text Specification* (Draft Version, ATIS-TIA-J-STD-102). Alliance for Telecommunications Industry Solutions, 2009.

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

[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*. Federal Emergency Management Agency, 2009.

[FEMA 2014]
Federal Emergency Management Agency. *Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN), v3.07*. Federal Emergency Management Agency, 2014.

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

[Levine 2003]
Levine, Linda; Meyers, B. Craig; Morris, Ed; Place, Patrick R. H.; & Plakosh, Daniel. *Proceedings of the System of Systems Interoperability Workshop (February 2003)* (CMU/SEI-2003-TN-016). Software Engineering Institute, Carnegie Mellon University, 2003. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6469

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

[NIST 2013]
National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53 Revision 4). National Institute of Standards and Technology, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[NPSTC 2007]
National Public Safety Telecommunications Council. *Commercial Mobile Alert Service Architecture and Requirements, v 1.0*. National Public Safety Telecommunications Council, 2007.

[SEI 2014]
Software Engineering Institute, WEA Project Team. *Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators* (CMU/SEI-2013-SR-018). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=70071

[Sharp 2001]
Sharp, Alec & McDermott, Patrick. *Workflow Modeling: Tools for Process Improvement and Application Development*. Artech House, 2001.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	June 2016	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Wireless Emergency Alerts Commercial Service Provider (CMSP) Cybersecurity Guidelines	FA8721-05-C-0003

6. AUTHOR(S)
Christopher Alberts, Audrey Dorofee, Carol Woody, PhD

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2016-SR-009

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	n/a

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 is a collaborative partnership that enables local, tribal, state, territorial, and federal public safety officials to disseminate geographically targeted emergency alerts to users of capable mobile devices in an affected geographic area. The end-to-end WEA alerting pipeline comprises the following four major elements: (1) alert originators, (2) Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN), (3) commercial mobile service providers (CMSPs), and (4) alert recipients. This report presents the results of a study of the CMSP element of the WEA pipeline conducted by researchers at the Software Engineering Institute (SEI). The goal of the study is to provide members of the CMSP community with practical guidance that they can use to better manage their cybersecurity risk exposure. To conduct the study, the SEI research team used the Security Engineering Risk Analysis (SERA) Method to assess high-priority cybersecurity risks in the CMSP WEA infrastructure. The research team used the results of the risk analysis to develop a set of cybersecurity guidelines tailored to the needs of CMSPs.

14. SUBJECT TERMS	15. NUMBER OF PAGES
commercial mobile service provider, CMSP, alert originator service provider, AO, threat enabler, risk	119

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