Security Engineering Risk Analysis (SERA)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-1054

Topics

Introduction

Security Engineering Risk Analysis (SERA) Method

Summary

Security Engineering Risk Analysis (SERA)

Introduction

Systems Security Engineering (SSE)

"An element of Systems Engineering (SE) that applies scientific and engineering principles in a standardized, repeatable, and efficient manner to identify security vulnerabilities, requirements, and methods of verifications that minimize risks."[1]

- SSE processes are used to design systems that are resilient to cyber-attacks.
- SSE delivers systems that satisfy stakeholder security needs for weapon system operation in today's cyber-contested environments.

1. United States Air Force Weapon System Program Protection / Systems Security Engineering Guidebook, Version 2.0

USAF Program Protection (PP) and Systems Security Engineering (SSE) Guidebook

The USAF Weapon System PP/SSE Guidebook defines an integrating process for implementing security countermeasures in weapon systems:

- Anti-counterfeit practices
- Anti-tamper (AT)
- Cybersecurity
- Exportability features
- Hardware assurance (HwA)
- Procurement strategies
- Secure system design
- Security management / information protection (IP)
- Software assurance (SwA)
- Supply chain risk management (SCRM)

Key gap: Software security engineering is not addressed sufficiently in the USAF Weapon System PP/SSE Guidebook.

Situational Awareness (SA) CSE Assessments

Assessments are a key component of SEI's CSE strategy.

The CERT SA Team performs the following CSE assessments:

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

Security Engineering Risk Analysis (SERA) Method

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

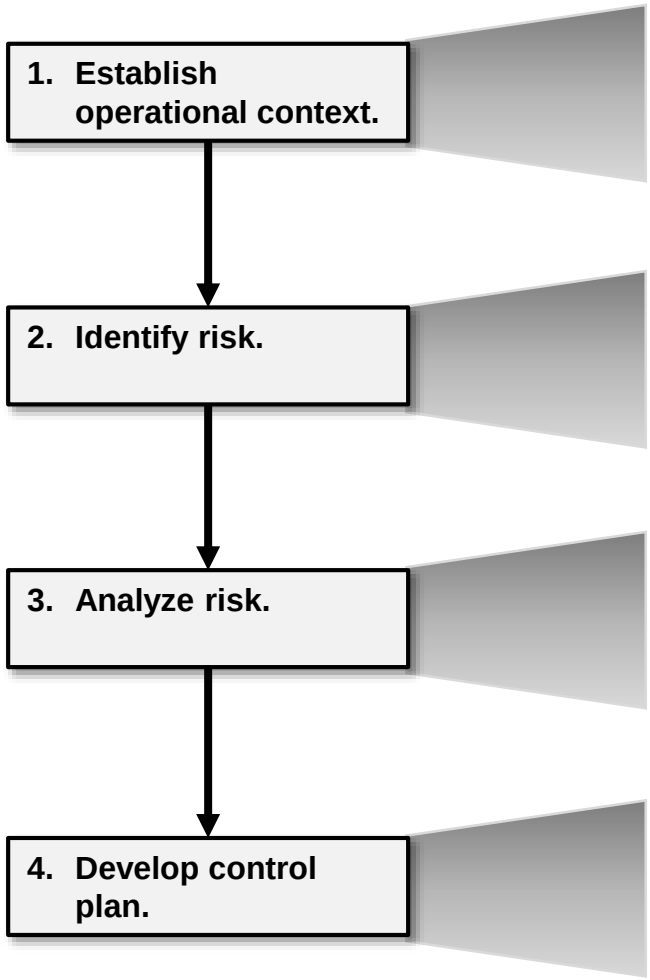
Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST standards and guidelines

SERA Method: *Four Tasks*



Key Output
Compiled data:
- Mission thread
- System architecture
- Software architecture
- Interface diagrams
- Dataflow diagrams
- Use cases
- Network topology

Key Output
- Cyber-risk scenarios

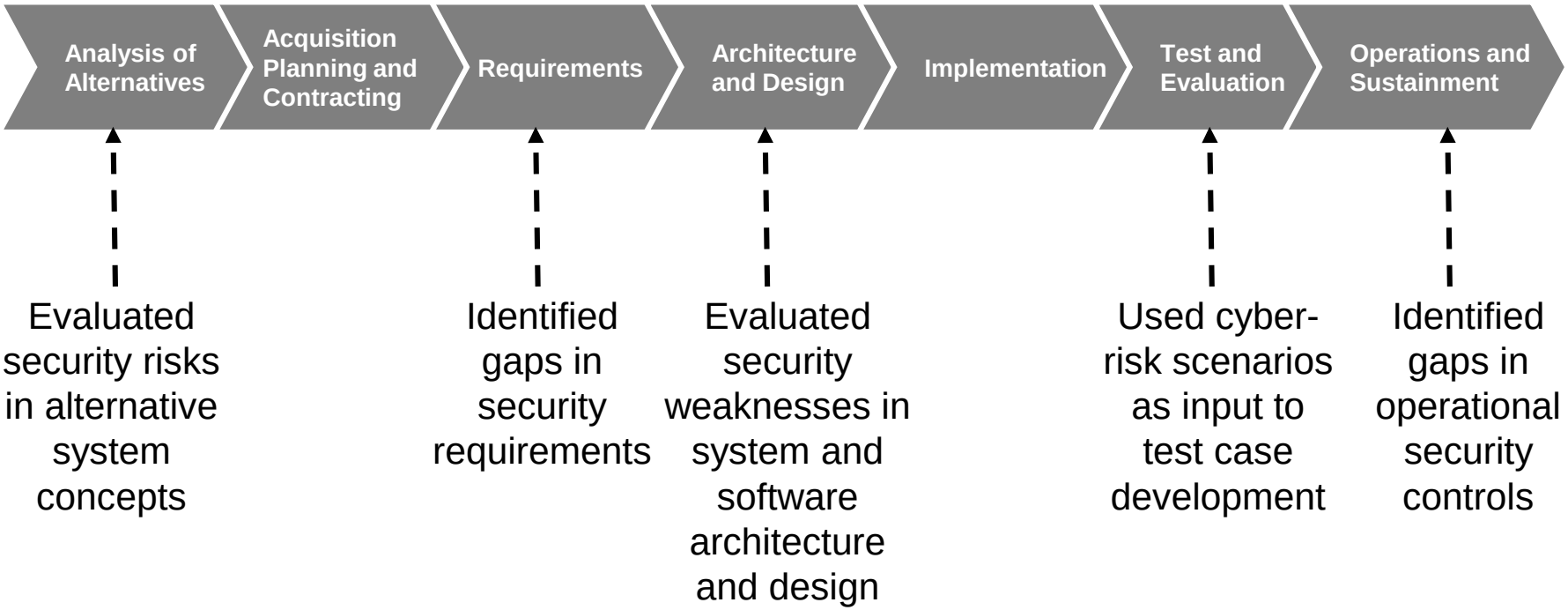
Key Input
- Threat archetypes

Key Output
- Prioritized cyber-risk scenarios

Key Output
- Control plans for high-priority cyber-risk scenarios

SERA Method: *Security Analysis Across the Lifecyle*

The SERA Method has been piloted across the acquisition and engineering lifecycle.

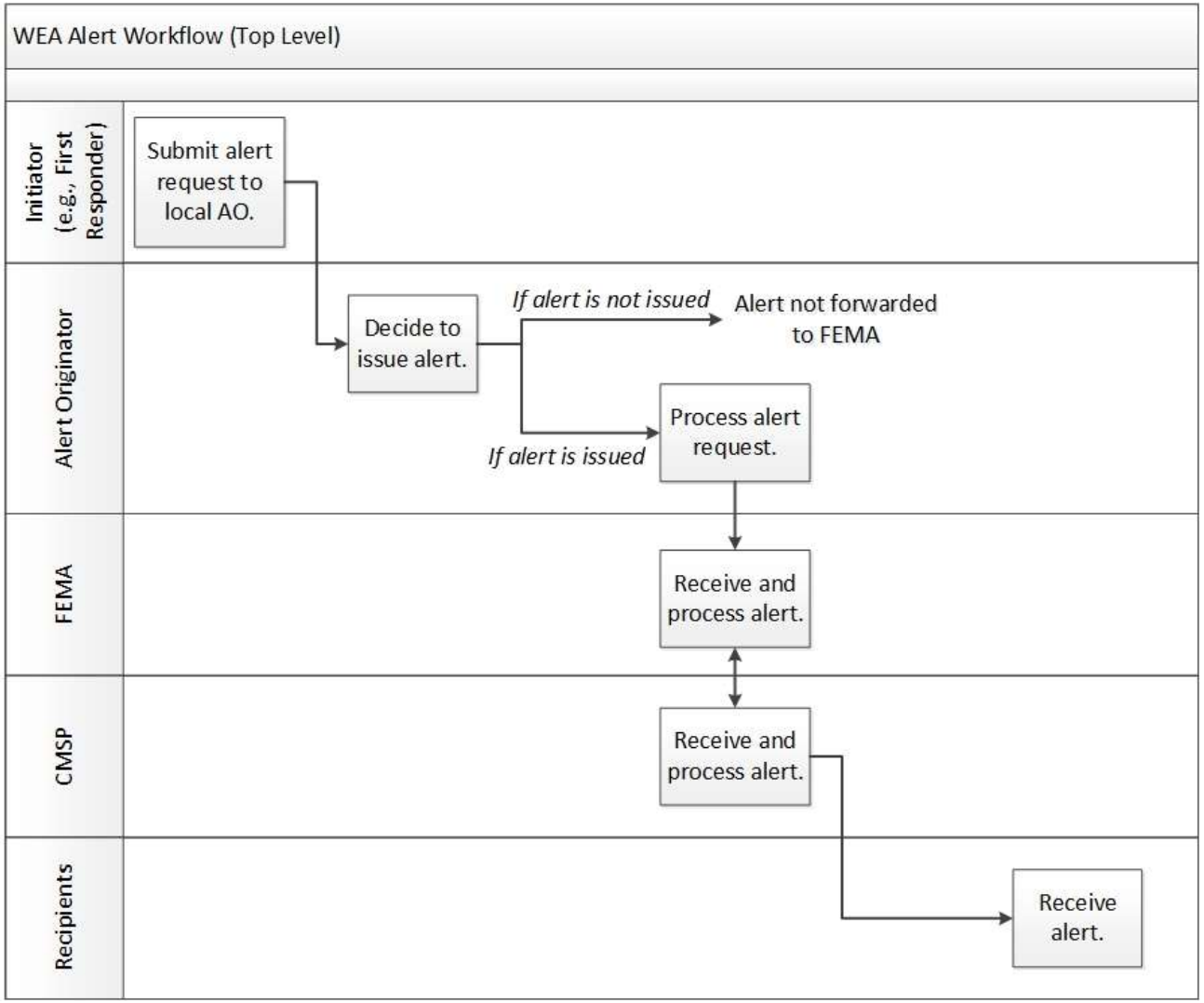


Example: *Wireless Emergency Alerts (WEA) Service*

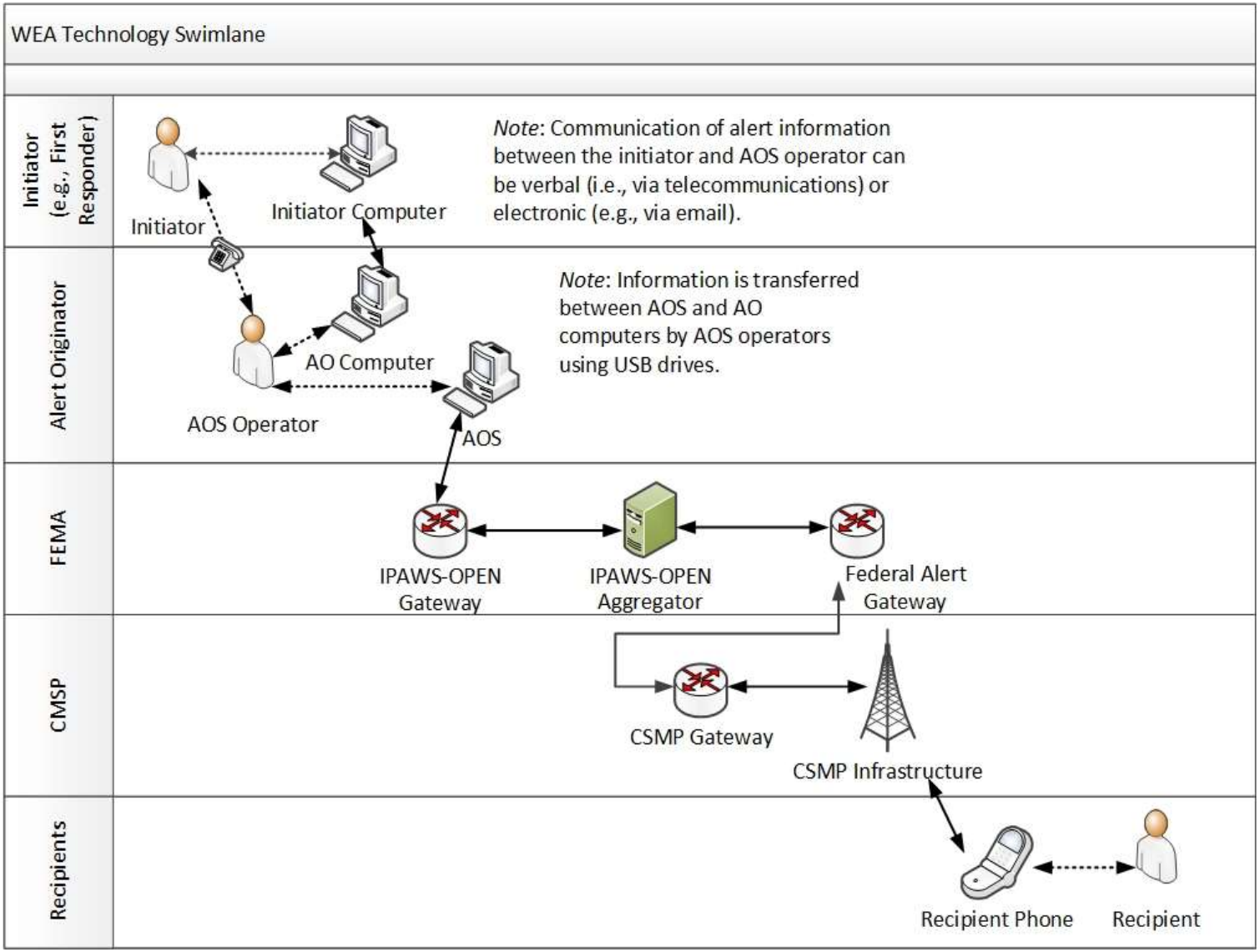
WEA is a major component of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS).

- Enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via **Commercial Mobile Service Providers (CMSPs)**.
- Customers of participating wireless carriers with WEA-capable mobile devices will automatically receive alerts in the event of an emergency if they are located in or travel to the affected geographic area.

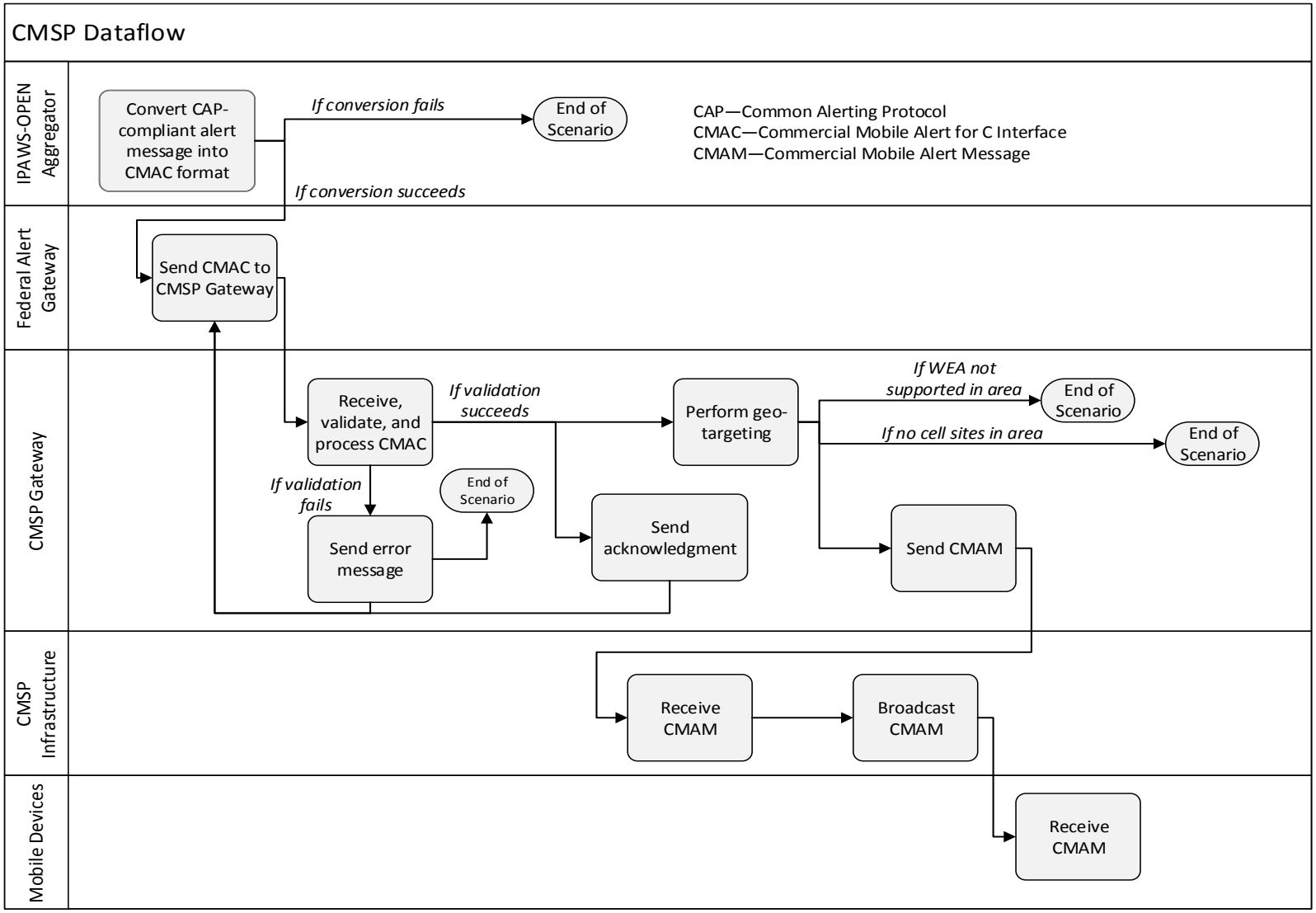
Example: *WEA Workflow*



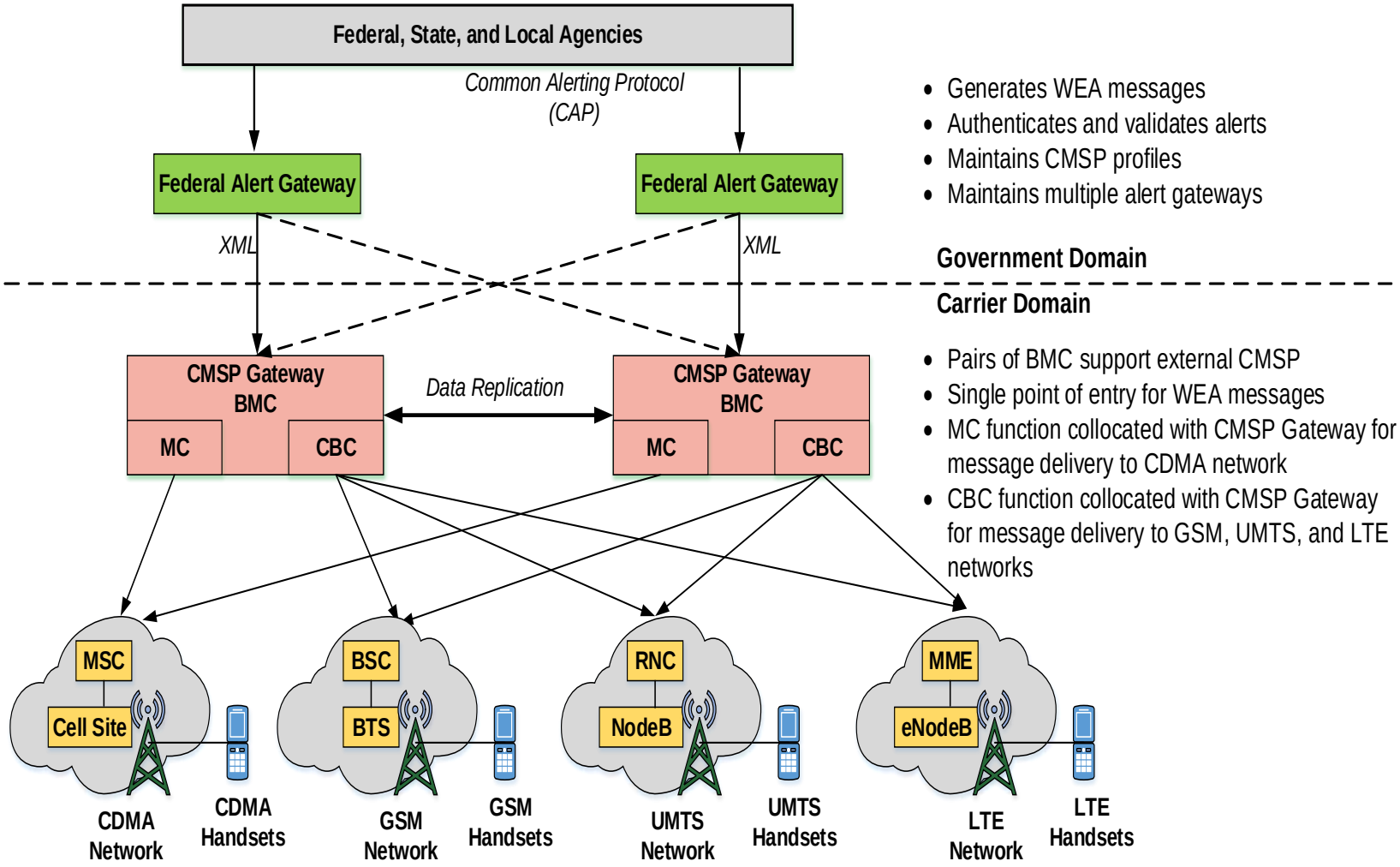
Example: *WEA Systems of Systems*



Example: *CMSP Workflow*



Example: *CMSP Architecture*

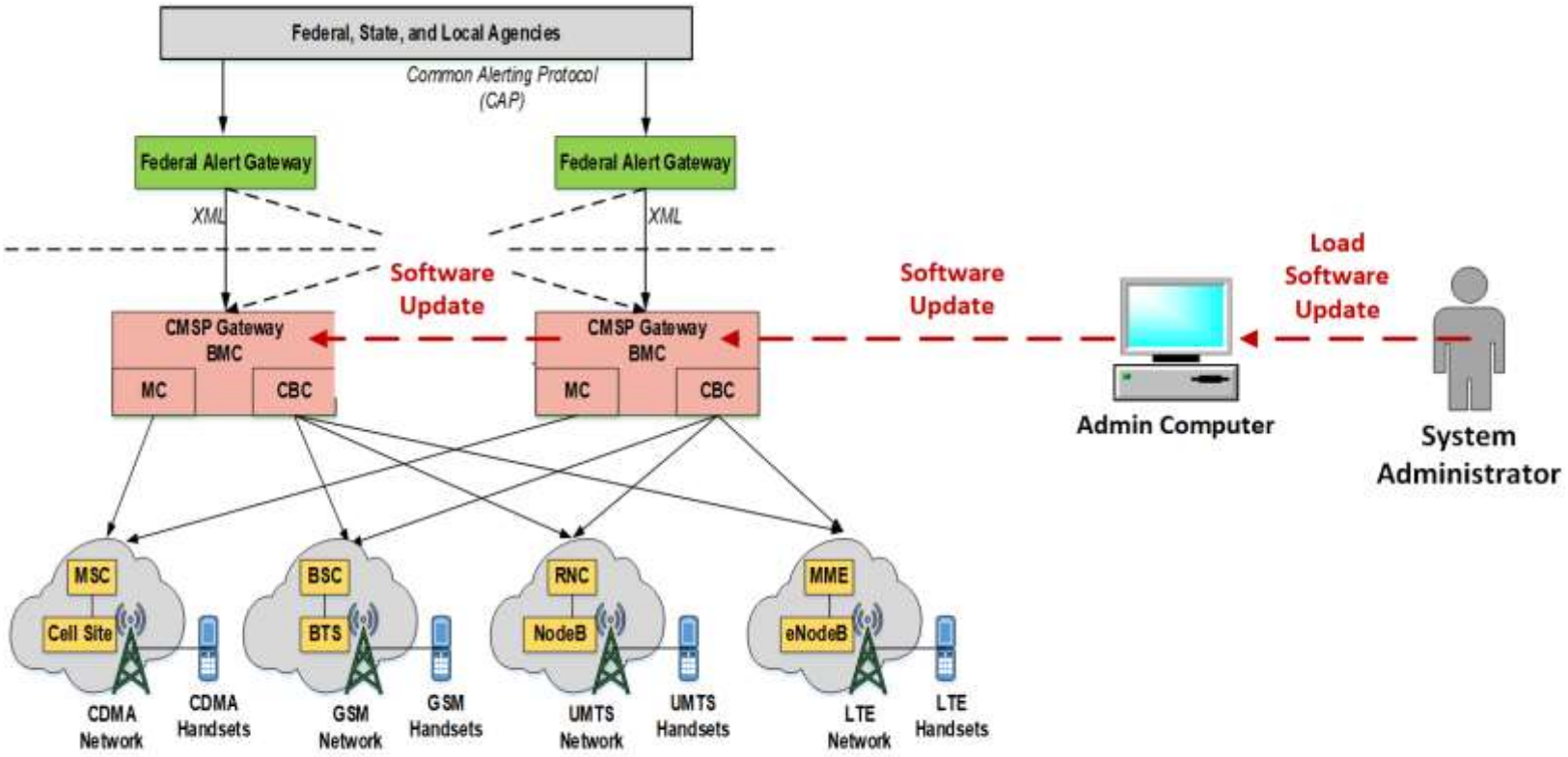


- Generates WEA messages
- Authenticates and validates alerts
- Maintains CMSP profiles
- Maintains multiple alert gateways

- Pairs of BMC support external CMSP
- Single point of entry for WEA messages
- MC function collocated with CMSP Gateway for message delivery to CDMA network
- CBC function collocated with CMSP Gateway for message delivery to GSM, UMTS, and LTE networks

Note: Acronyms in this figure are defined in the main body of the report.

Example: *CMSP Upgrade Process*



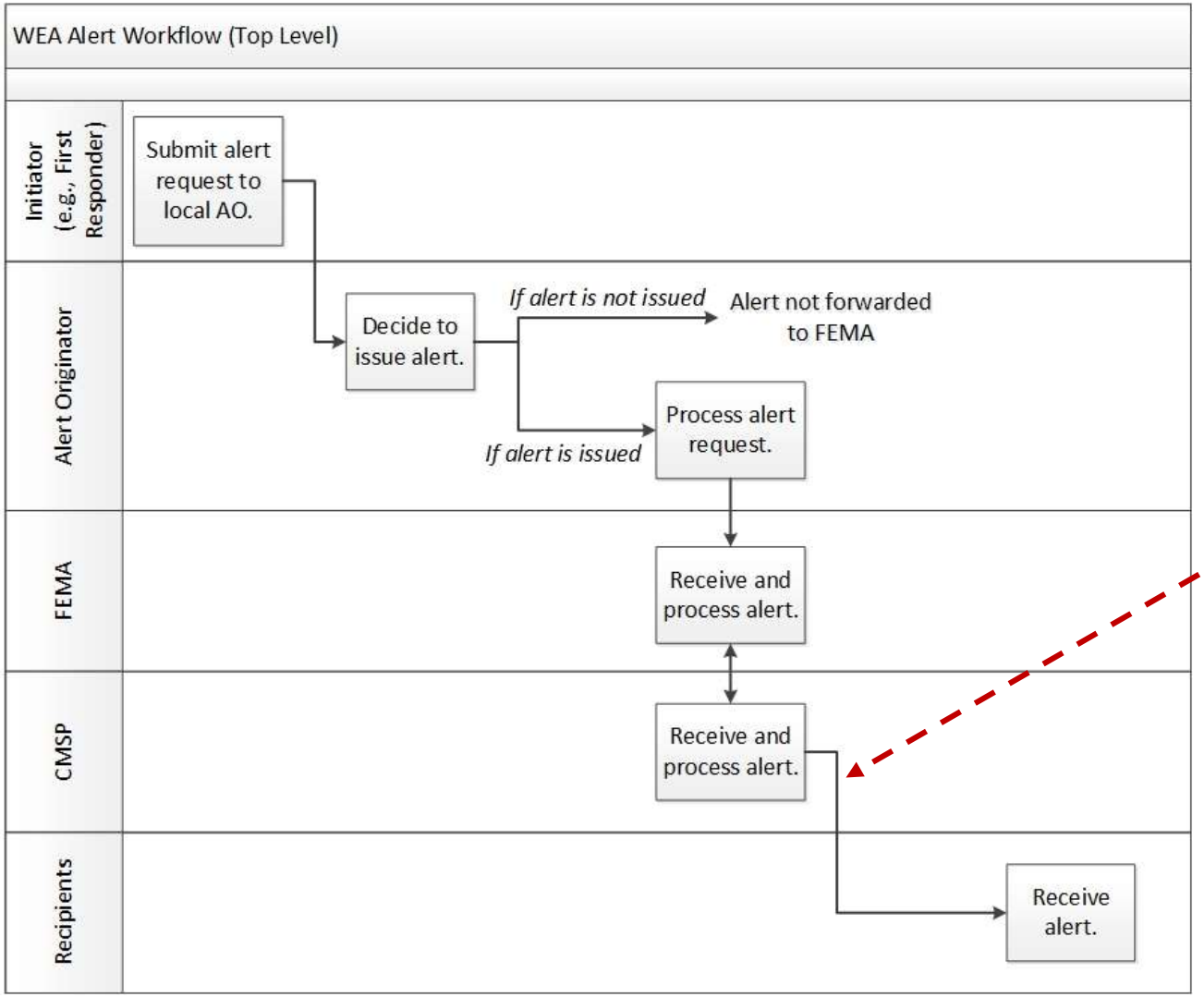
Note: Acronyms in this figure are defined in the main body of the report.

Example: *Selected Threat Archetype*

Element	Attribute
Actor	Insider
Threat Type	Targeted
Access Type	Physical and network
Access Point	Entity of interest
Attack Pattern	Local Execution of Code (CAPEC-549) Traffic Injection (CAPEC-594)
Direct Consequence	Insertion of false data (integrity)

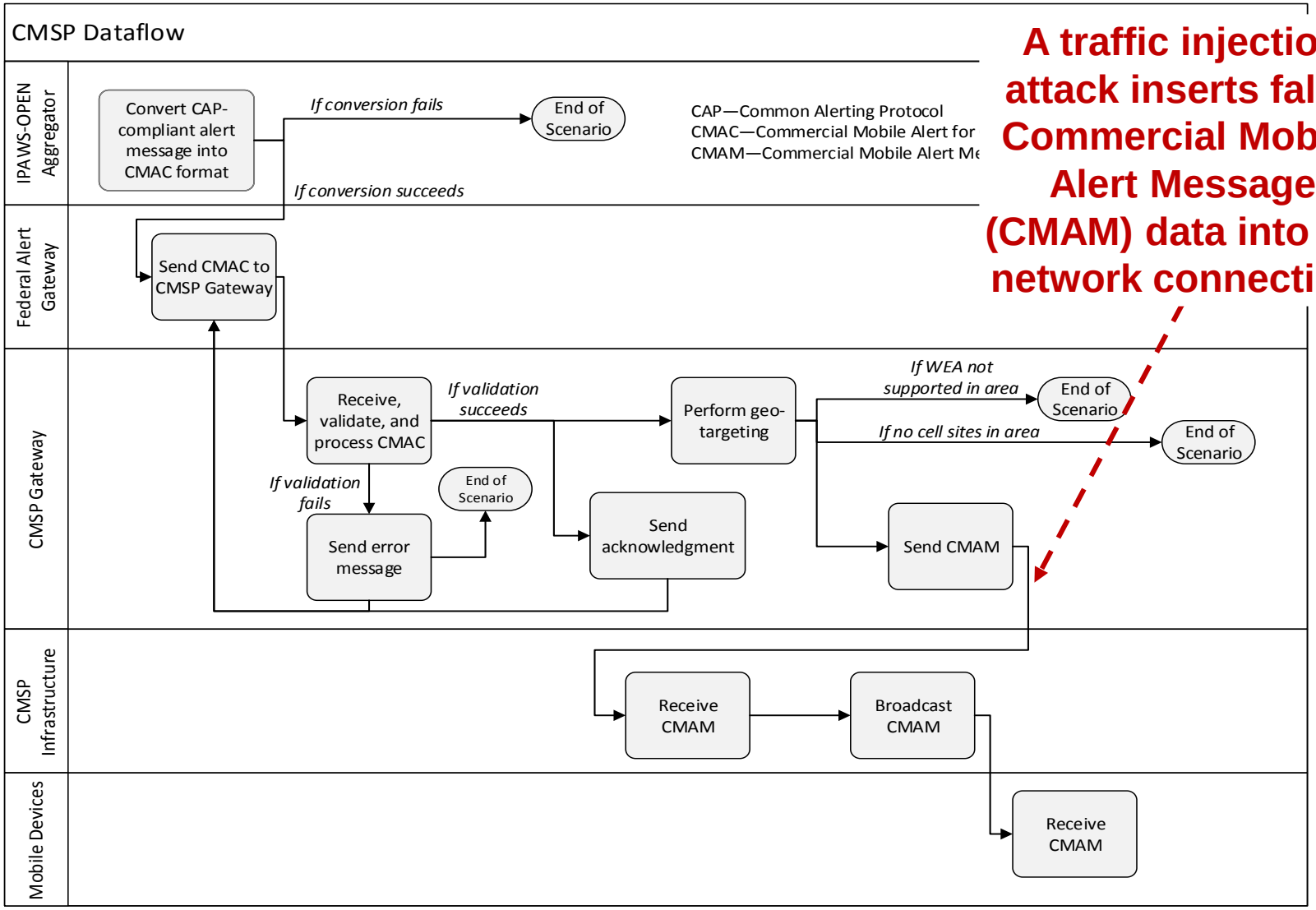
A *threat archetype* is a pattern or model that describes a cyber-based act, occurrence, or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Example: *Mission Impact*



CMSP sends a nonsense WEA message repeatedly to customers.

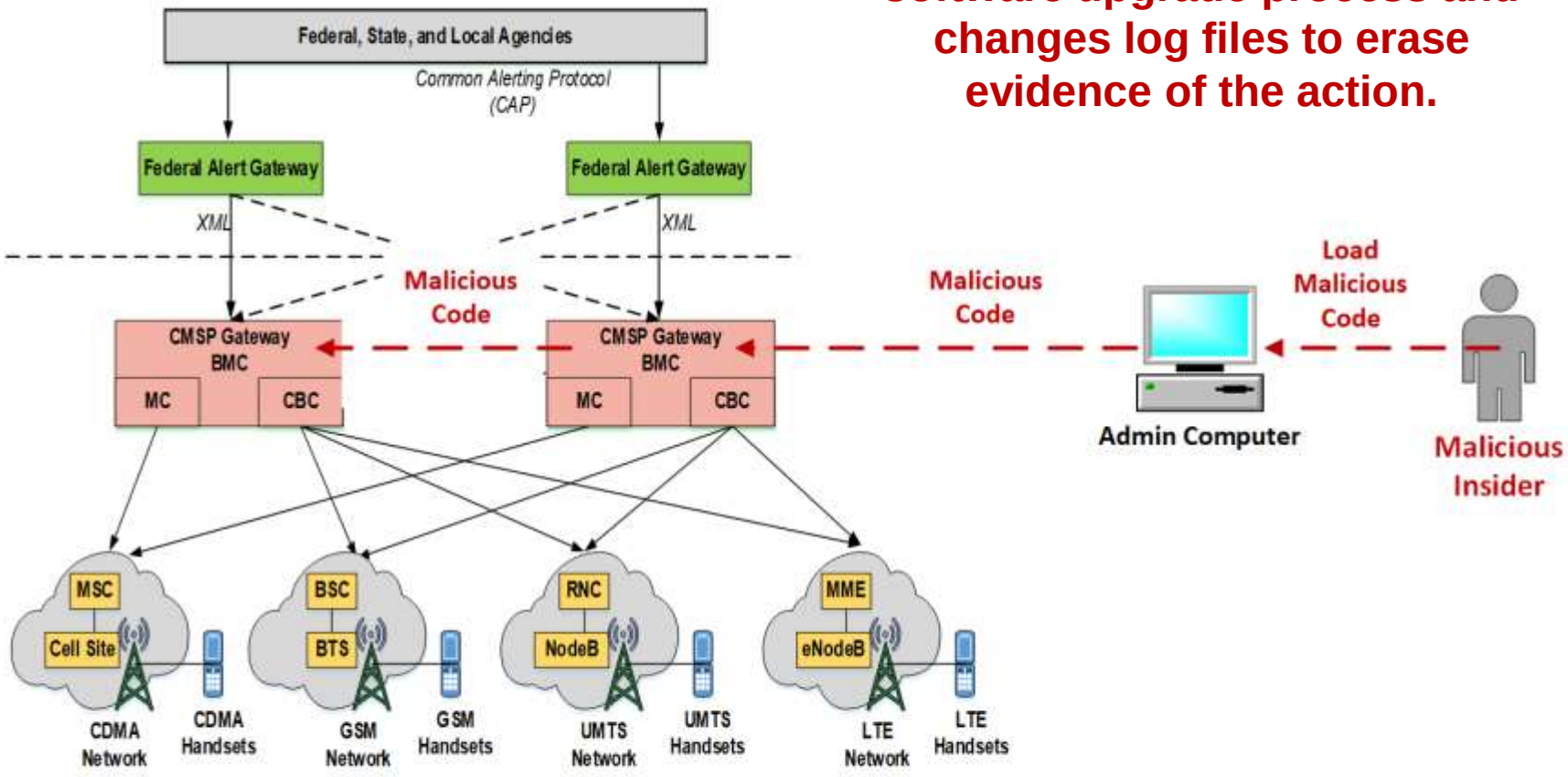
Example: *Cyber Attack*



A traffic injection attack inserts false Commercial Mobile Alert Message (CMAM) data into the network connection.

Example: *SoS Attack Vector*

The insider uploads the malicious code to the CMSP Gateway via the software upgrade process and changes log files to erase evidence of the action.



Note: Acronyms in this figure are defined in the main body of the report.

Example: *Threat Sequence*

1. An insider with technical skills and administrative access to the Commercial Mobile Service Provider (CMSP) Gateway becomes disgruntled after being passed over for a promotion.
2. The insider begins to behave aggressively and abusively toward coworkers.
3. After a while, the insider decides to execute a cyber attack on the CMSP. The insider's goal is to repeatedly send nonsense alerts to customers.
4. The insider uses physical and cyber access to Wireless Emergency Alerts (WEA) information and resources to perform reconnaissance.
5. The insider develops a plan for the cyber attack based on the available information.
6. The insider uses the organization's resources to develop malicious code designed to forward false alerts from the CMSP Gateway.
7. The insider uploads the malicious code to the CMSP Gateway via the software upgrade process and changes log files to erase evidence of the action.
8. When the insider triggers the malicious code, a traffic injection attack inserts false Commercial Mobile Alert Message (CMAM) data into the network connection to the CMSP infrastructure. A nonsense WEA message is sent repeatedly to customers.

Example: *Controls Areas for Cyber-Risk Scenario*

Access Control

Change Management

Code Analysis

Disaster Recovery

Human Resources

Incident Response

Monitoring

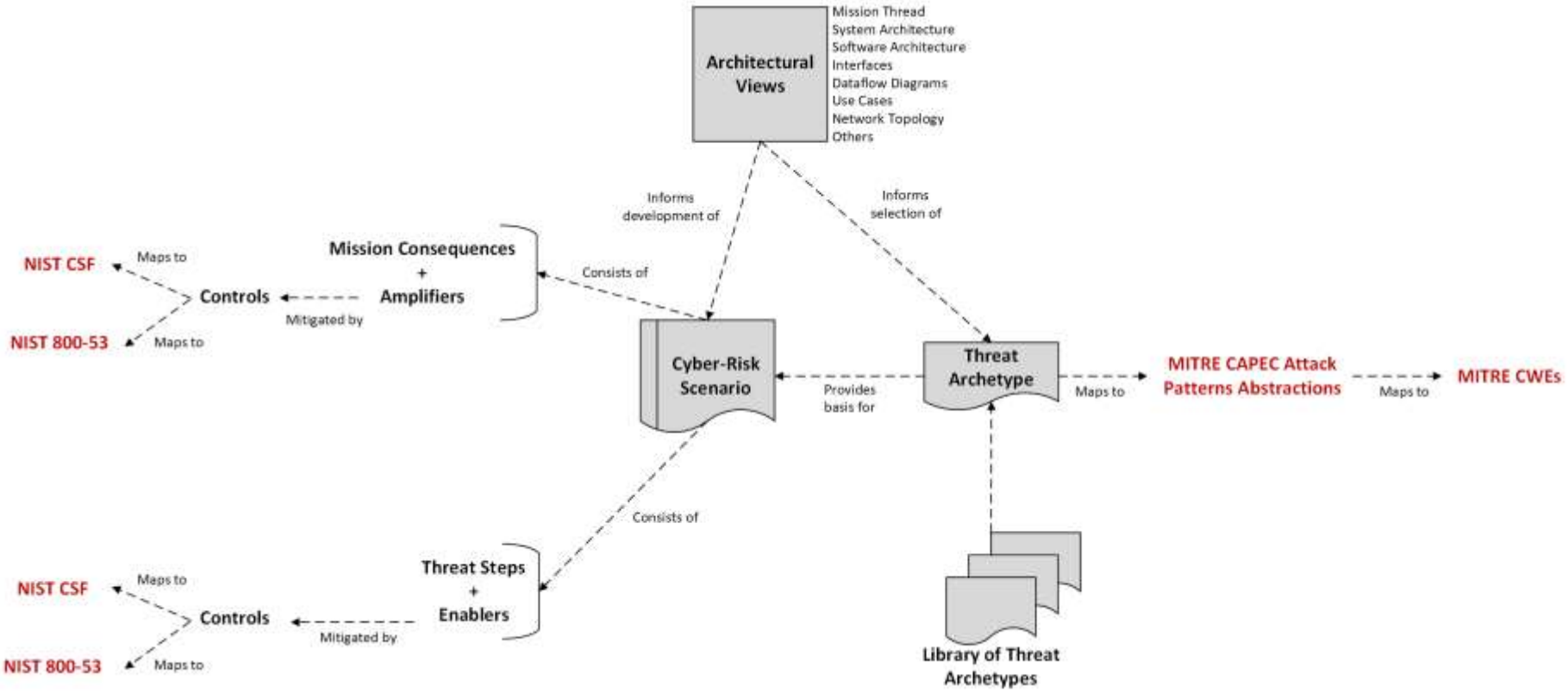
System Architecture

Training

Example: *SERA Threat Sequence Table (Excerpt)*

Step		Enabler	Candidate Control	NIST Mapping
1.	An insider with technical skills and administrative access to the Commercial Mobile Service Provider (CMSP) Gateway becomes disgruntled after being passed over for a promotion.	Insufficient feedback about employee performance	The organization's managers are trained to provide constructive feedback on performance issues.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
2.	The insider begins to behave aggressively and abusively toward coworkers.	Tolerance for inappropriate employee behavior	The organization's managers recognize inappropriate behavior when it occurs and respond appropriately.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
3.	After a while, the insider decides to execute a cyber attack on the CMSP. The insider's goal is to repeatedly send nonsense alerts to customers.	No resolution to underlying employee issue	The organization's managers recognize an employee's escalating frustration and proactively work to diffuse the situation.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
4.	The insider uses physical and cyber access to Wireless Emergency Alerts (WEA) information and resources to perform reconnaissance.	Insufficient access control for information and resources (physical and cyber)	Physical access to information and resources is managed and protected.	NIST CSF: PR.AC-2 NIST 800-53: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
			Access permissions and authorizations for computing resources are managed.	NIST CSF: PR-AC-4 NIST 800-53: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		Insufficient monitoring of the organizational environment for abnormal activity (physical and cyber)	The organization monitors the physical environment for abnormal activity.	NIST CSF: DE.CM-2 NIST 800-53: CA-7, PE-3, PE-6, PE-20
			The organization monitors systems and networks for abnormal activity.	NIST CSF: DE.CM-1 NIST 800-53: AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
			The organization performs targeted monitoring of individuals with suspected behavioral issues.	NIST CSF: DE.CM-3 NIST 800-53: AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
			The organization responds appropriately when abnormal activity is detected.	NIST CSF: RS.MI-1, RS-MI-2 NIST 800-53: IR-4

SERA Data Mapping



SERA cyber-risk data can be mapped to security standards, such as

- NIST Cybersecurity Framework (CSF) and NIST 800-53
- MITRE CAPEC attack patterns and MITRE CWEs

SERA Method: *Summary*

Customer Types:

- DoD weapon system acquisition (5 pilots)
- Foreign Military Sales (FMS) (2 pilots)
- Civil agency system acquisition (2 pilots)

Lifecycle Phases

- Analysis of alternatives (AoA)
- Requirements specification
- Architecture analysis
- Operational test and evaluation (OT&E)
- Operations and Sustainment (O&S)

Time to conduct:

- 1-6 months (depending on scope)

Security Engineering Risk Analysis (SERA)

Summary

Key Points -1

SEI CSE research is defining an approach for integrating software security engineering with SSE across the acquisition lifecycle.

Assessments are a key component of the SEI CSE strategy.

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

Key Points -2

The SERA Method

- Defines a systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the
  - Lifecycle
  - Supply chain
- Builds security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assembles a shared organizational view (business and technical) of cybersecurity risk