SEI WEBINAR SERIES | Keeping you informed of the latest solutions

Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

© 2016 Carnegie Mellon University.

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense 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.

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

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is a registered mark of Carnegie Mellon University.

DM-0003498

Security Requirements Engineering

Christopher Alberts

CERT® Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

© 2016 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Topics

Background

Security Engineering Risk Analysis (SERA) Method

Summary

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Security Requirements Engineering

Background

© 2016 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Software Assurance (SwA)

Definition

- "The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner." [1]

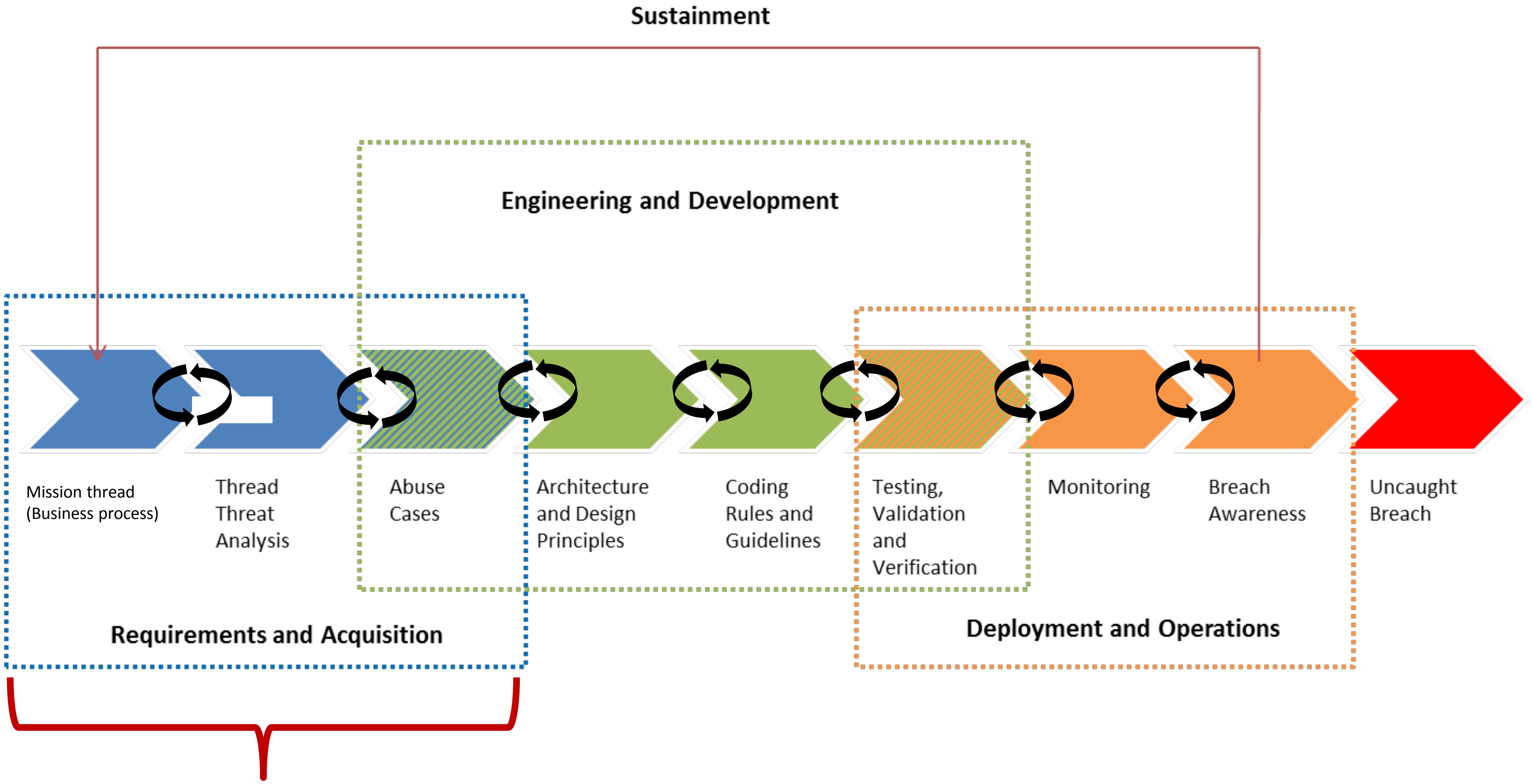
Key Aspects of SwA

- Trustworthiness – No exploitable weaknesses exist, either maliciously or unintentionally inserted.
- Predictable Execution – When executed, software functions as intended.

1. National Information Assurance Glossary CNSS Instruction No. 4009; DoDi 5200.44 p.12

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

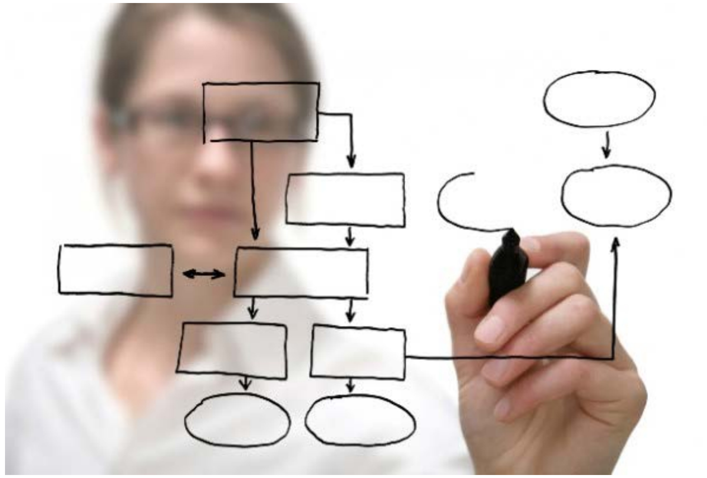
Software Assurance: *Lifecycle Focus*


Sustainment
Engineering and Development
Mission thread (Business process)
Thread Threat Analysis
Abuse Cases
Architecture and Design Principles
Coding Rules and Guidelines
Testing, Validation and Verification
Monitoring
Breach Awareness
Uncaught Breach
Requirements and Acquisition
Deployment and Operations

Focus of this module

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Software Security Requirements



Features (e.g., controls or constraints) that specify how to preserve the confidentiality, integrity, and availability of critical system data[1]

1. Khan, M. U. A. & Zulkernine, M. “On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software,” 353-358. *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International* (Volume:2). Seattle, WA: IEEE Press, 2009.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

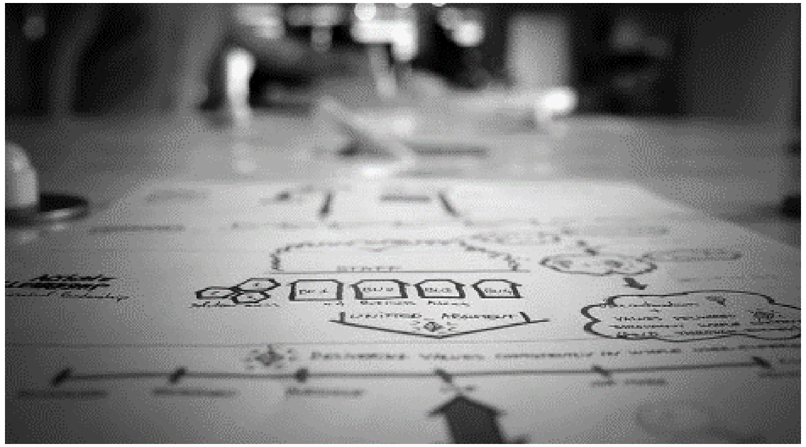
Polling Question

Are you experienced in developing security requirements?

Answers:

- Yes
- No

Security Requirements Engineering: *Key Activities*[1]



1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).

[1] Derived from the Security Quality Requirements Engineering (SQUARE) Method as defined in Allen, Julia H.; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; & Mead, Nancy R. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Focus of this Module

1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).

This module examines the role of risk analysis during security requirements engineering

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Security Requirements Engineering

Security Engineering Risk Analysis (SERA)

© 2016 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Polling Question

Are you experienced in assessing security risk?

Answers:

- Yes
- No

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks across the lifecycle

Why

- Build security into software-reliant systems
- Address design weaknesses as early as possible (e.g., requirements, architecture, design)

Benefits

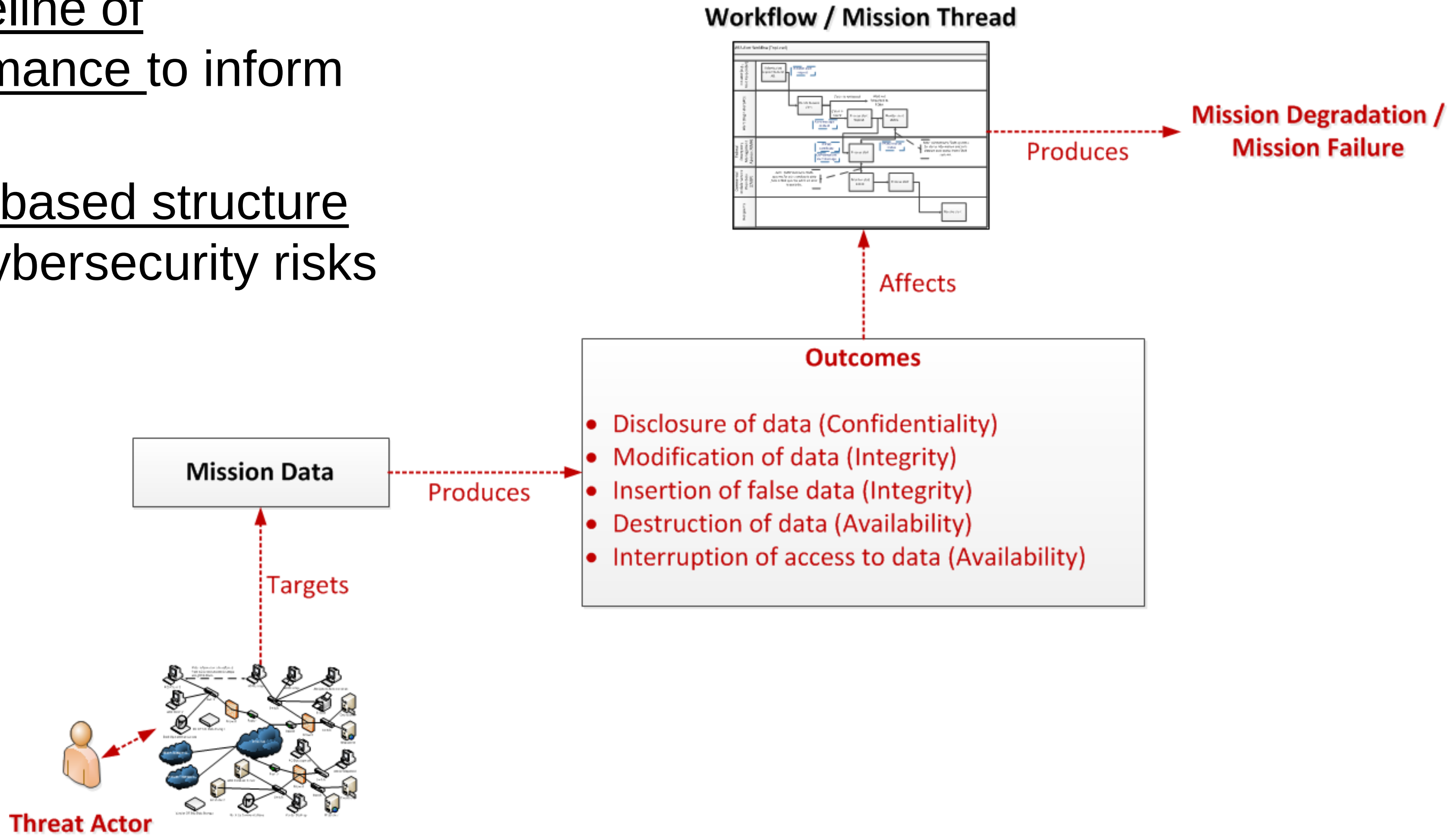
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with risk management standards

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Approach: *Focus on Mission Impact*

SERA analyzes the mission impact of data security breaches.

- Establishes a baseline of operational performance to inform risk identification
- Employs scenario-based structure for documenting cybersecurity risks



Workflow / Mission Thread

Produces

Mission Degradation / Mission Failure

Affects

Outcomes

- Disclosure of data (Confidentiality)
- Modification of data (Integrity)
- Insertion of false data (Integrity)
- Destruction of data (Availability)
- Interruption of access to data (Availability)

Mission Data

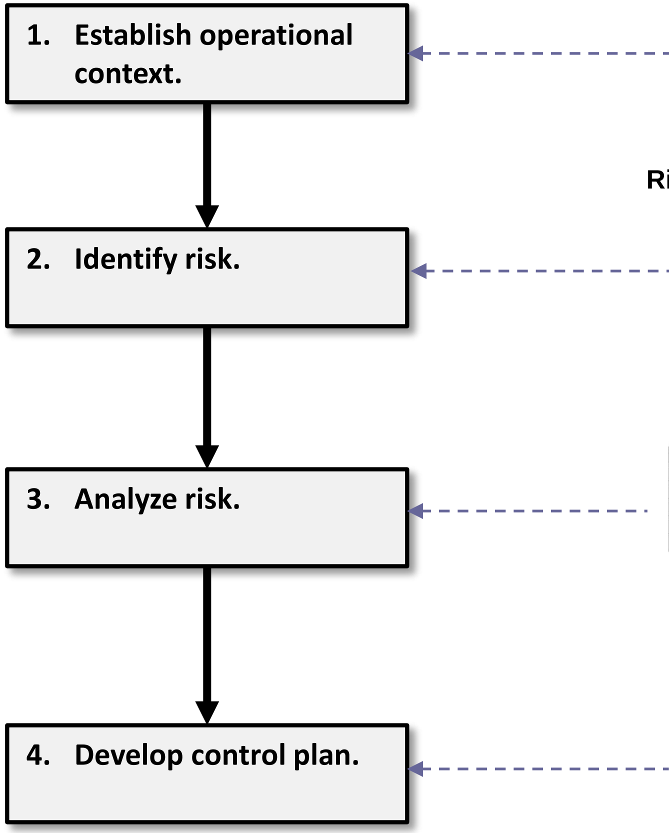
Produces

Targets

Threat Actor

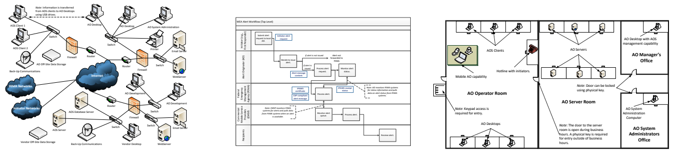
[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Method: *Four Tasks*



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

Modeling Techniques

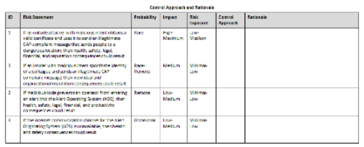


Risk Identification Worksheet

Risk Evaluation Criteria

Risk Analysis Worksheet

Control Approach Worksheet



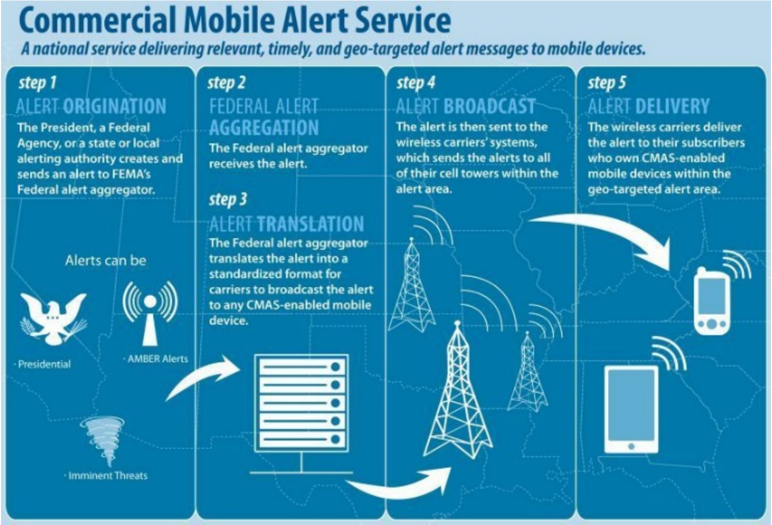
Control Plan Worksheet

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Pilot Example: *Wireless Emergency Alerts (WEA)*[1]

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

- **Initiator** – decides to issue an alert (e.g., weather alert, AMBER alert)
- **Alert originator (AO)** – sends alerts to mobile devices in the targeted area
- **FEMA** – receives and processes alerts
- **Commercial mobile service provider (CMSP)** – receives and processes alerts
- **Recipients** – receive alerts automatically



Commercial Mobile Alert Service

A national service delivering relevant, timely, and geo-targeted alert messages to mobile devices.

step 1
ALERT **ORIGINATION**
The President, a Federal Agency, or a state or local alerting authority creates and sends an alert to FEMA's Federal alert aggregator.

step 2
FEDERAL ALERT **AGGREGATION**
The Federal alert aggregator receives the alert.

step 3
ALERT **TRANSLATION**
The Federal alert aggregator translates the alert into a standardized format for carriers to broadcast the alert to any CMAS-enabled mobile device.

step 4
ALERT **BROADCAST**
The alert is then sent to the wireless carriers' systems, which sends the alerts to all of their cell towers within the alert area.

step 5
ALERT **DELIVERY**
The wireless carriers deliver the alert to their subscribers who own CMAS-enabled mobile devices within the geo-targeted alert area.

[1] Alberts, C.; Woody, C.; & Dorofee, A. *Wireless Emergency Alerts CMSP Cybersecurity Guidelines* (CMU/SEI-2015-SR-020). Software Engineering Institute, Carnegie Mellon University, 2015. http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20CMSP%20Cybersecurity%20Guidelines.pdf

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Establish Operational Context (Task 1)

The operational environment for the system of interest is characterized to establish a baseline of operational performance.

Steps	
1.1	Determine system of interest.
1.2	Select workflow/mission thread.
1.3	Establish operational views.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 1: *Operational Views*

Mission thread / workflow

Technology (e.g., system, system of systems, architecture, network)

Use case

Data

Physical

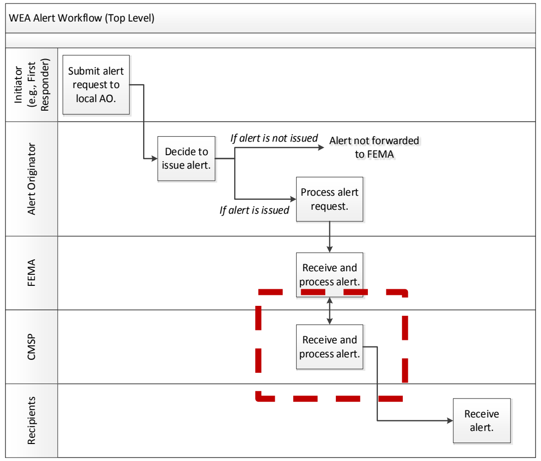
Stakeholder

Others as needed

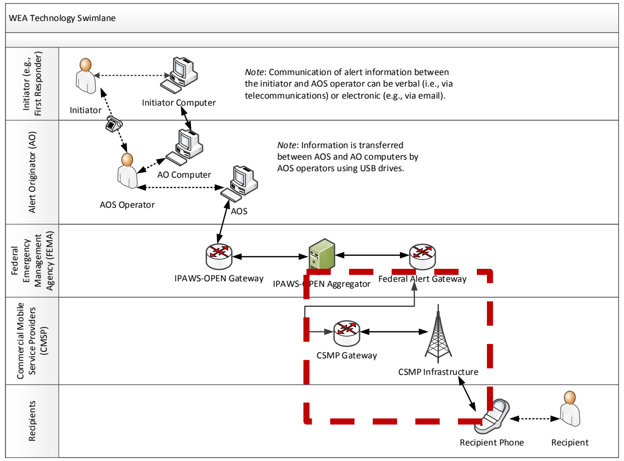
[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 1: *WEA Operational Models*

WEA Workflow/Mission Thread


WEA Alert Workflow (Top Level)
Initiator (e.g., First Responder)
Alert Originator
FEMA
CMSP
Recipients
Submit alert request to local AO.
Decide to issue alert.
If alert is not issued
Alert not forwarded to FEMA
If alert is issued
Process alert request.
Receive and process alert.
Receive and process alert.
Receive alert.

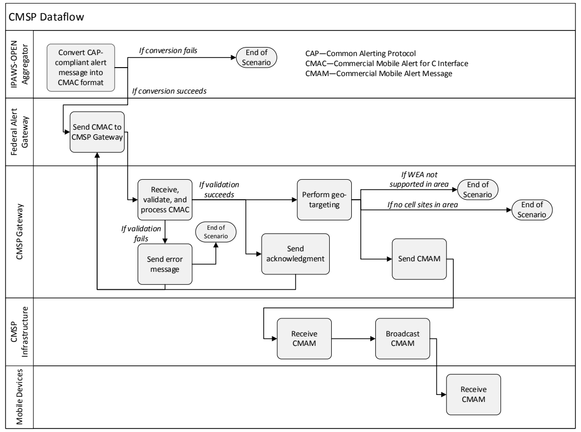
WEA System of Systems



Note: Communication of alert information between the initiator and AOS operator can be verbal (i.e., via telecommunications) or electronic (e.g., via email).

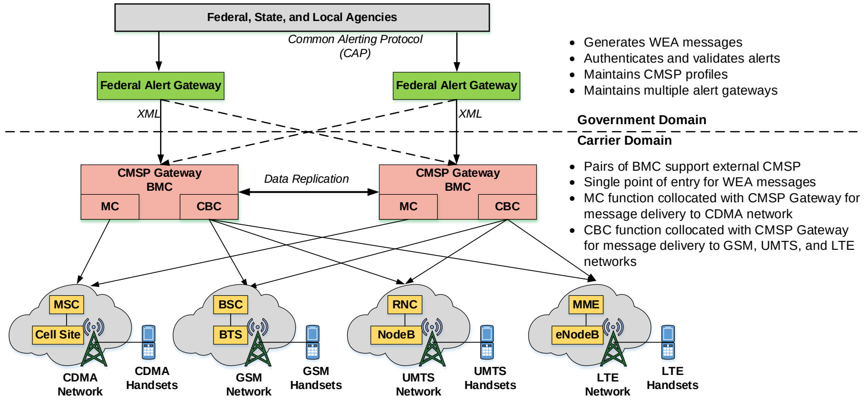
Note: Information is transferred between AOS and AO computers by AOS operators using USB drives.

CMSP Workflow/Mission Thread



CAP—Common Alerting Protocol
CMAC—Commercial Mobile Alert for C Interface
CMAM—Commercial Mobile Alert Message

CMSP Architecture



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

Government Domain

Carrier Domain

- 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

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 1: *Data Security Goals (Excerpt)*

Data Asset	Form	Confidentiality	Integrity	Availability
Alert message	Electronic	There are no restrictions on who can view this data asset (public data)	The data asset must be correct and complete (high integrity).	This data asset must be available when needed (high availability).
Geo-targeting data	Electronic	There are no restrictions on who can view this data asset (public data)	The data asset must be correct and complete (high integrity).	This data asset must be available when needed (high availability).

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Identify Risk (SERA Task 2)

Security concerns are transformed into distinct, tangible risk scenarios that can be described and measured.

Steps	
2.1	Identify threat.
2.2	Establish consequence.
2.3	Identify enablers and amplifiers.
2.4	Develop security risk scenario.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 2: *Threats Selected for Analysis*

R1. Insider Sends False Alerts

R2. Inherited Replay Attack

R3. Malicious Code in the Supply Chain

R4. Denial of Service

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 2: *R1 Threat Sequence*

T1. The insider is upset upon learning that he is not receiving 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 alert message repeatedly.

T4. The insider uses a colleague's workstation to check-in the modified code with the logic bomb.

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 WEA service to send a nonsense WEA alert repeatedly to people across the country.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 2: *Enablers*

Threat Step	Enabler
T7. The malicious code causes the carrier’s WEA service to send a nonsense WEA alert repeatedly to people across the country.	Insufficient capability to check message content can allow illegitimate alert messages to be broadcast automatically to designated mobile devices.

An *enabler* is a condition or circumstance (e.g., weakness, vulnerability) that facilitates a threat’s occurrence.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 2: *R1 Stakeholder Consequences*

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)

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 2: *Amplifiers*

Consequence
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.

Amplifier
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.

An *amplifier* is a condition or circumstance that increases the consequence triggered by the occurrence of a threat.

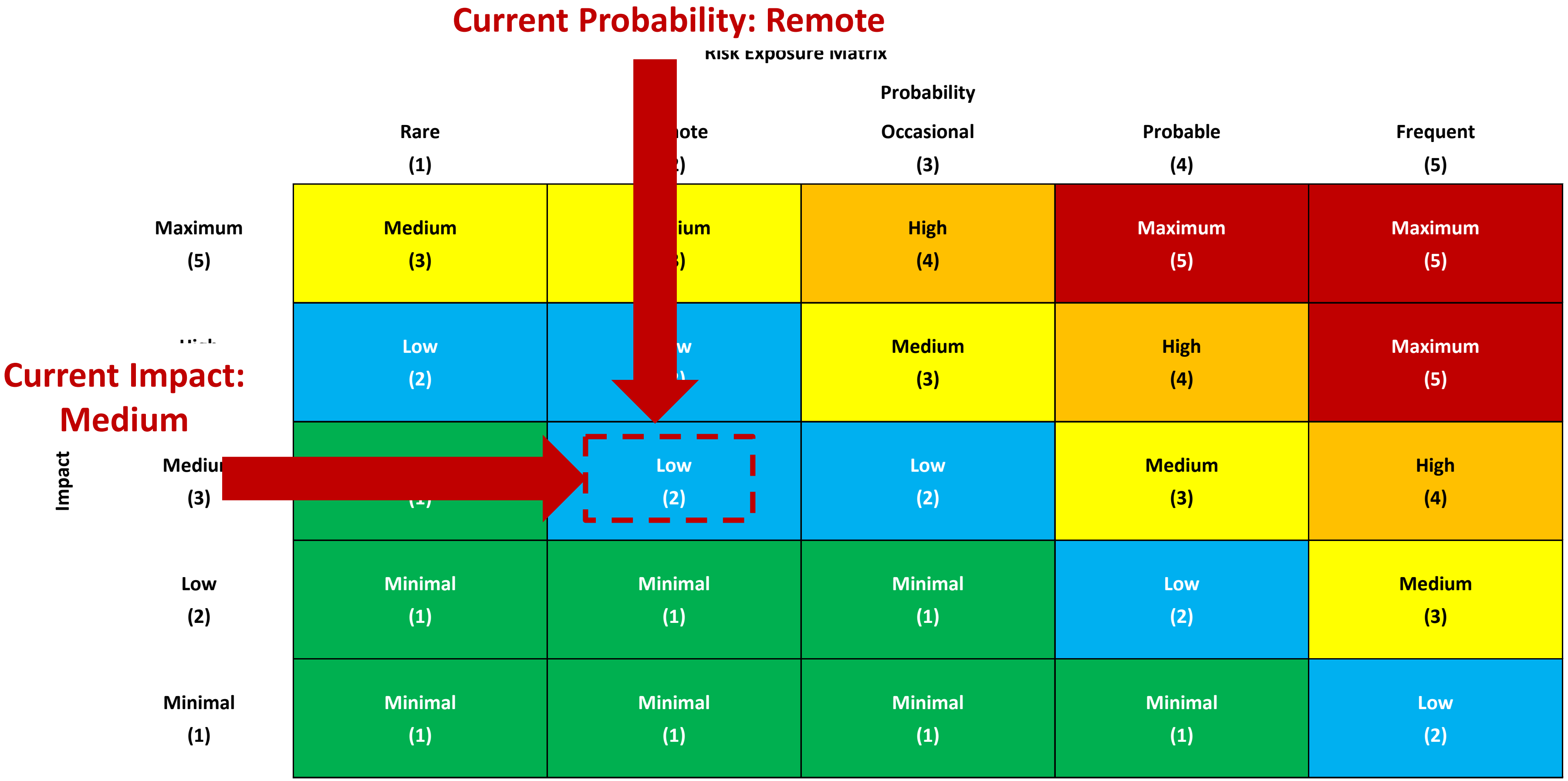
Analyze Risk (SERA Task 3)

Each risk is analyzed in relation to predefined criteria.

Steps	
3.1	Establish probability.
3.2	Establish impact.
3.3	Determine risk exposure.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 3: *R1 Risk Analysis*



Current Probability: Remote

Current Impact: Medium

Risk Exposure Matrix

		Probability				
		Rare (1)	ote)	Occasional (3)	Probable (4)	Frequent (5)
Impact	Maximum (5)	Medium (3)	ium)	High (4)	Maximum (5)	Maximum (5)
		Low (2)	w	Medium (3)	High (4)	Maximum (5)
	Mediu (3)		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)

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Develop Control Plan (SERA Task 4)

Control plans are developed and documented for all security risks that are not accepted.

Steps	
4.1	Prioritize risks.
4.2	Select control approach.
4.3	Establish control actions.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 4: *Prioritized Risk Spreadsheet*

ID	Risk Statement	Imp	Prob	RE
R4	Denial of Service	Max	Rare	Med
R1	Insider Sends False Alerts	Med	Remote	Low
R2	Inherited Replay Attack	Med	Remote	Low
R3	Malicious Code in the Supply Chain	Med	Rare	Min

Note: A control plan will be developed for all security risk scenarios with an impact of medium or greater.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 4: *Controls*

Threat Step

T7. The malicious code causes the carrier’s WEA service to send a nonsense WEA alert repeatedly to people across the country.

Enabler

Insufficient capability to check message content can allow illegitimate CMAM messages to be broadcast automatically to designated mobile devices.

Control

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

A *control* is a safeguard or countermeasure to

- Recognize, resist, and recover from security risks
- Counteract identified enablers and amplifiers

SERA Task 4: *CMSP Cybersecurity Guidelines*

The CMSP Cybersecurity Guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study

Controls were identified in the following areas:

- 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

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Task 4: *Controls with Requirements Implications*

Access Control

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

System Architecture

- The carrier's WEA alerting system has a backup capability that uses a separate communication channel.

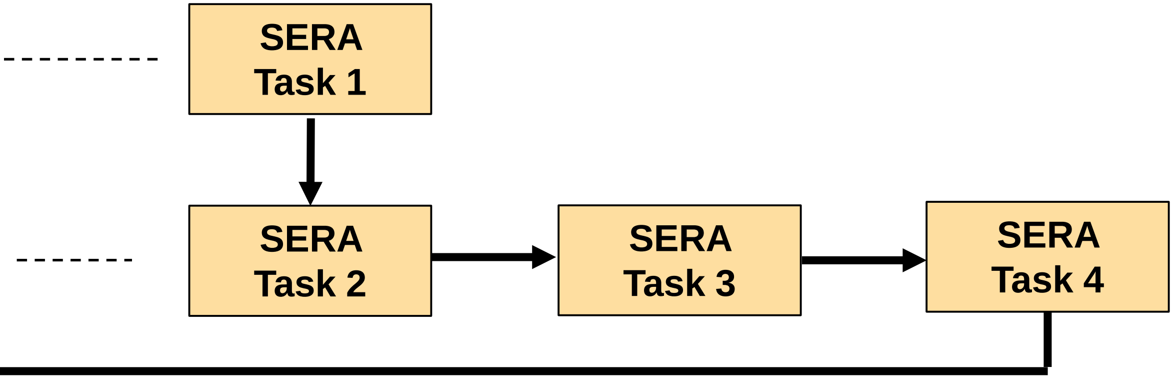
Technical Monitoring

- The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
- The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Security Requirements Engineering and SERA

1. Agree on definitions.
2. Identify system assets and security goals.
3. Perform security risk analysis.
4. Elicit security requirements.
5. Categorize security requirements.
6. Prioritize security requirements.
7. Inspect security requirements using a well-defined method (e.g., Fagan inspections).



[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Polling Question

Are your organization’s security requirements designed to reduce security risk in deployed software or systems?

Answers:

- Yes
- No
- Don’t know

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Security Requirements Engineering

Summary

© 2016 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Key Points

Software assurance:

- The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

Software security requirements:

- Features (e.g., controls or constraints) that specify how to preserve the confidentiality, integrity, and availability of critical system data

Security Engineering Risk Analysis (SERA) Method:

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle
- Can be integrated with security requirements engineering

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

SERA Publications

Alberts, C.; Woody, C.; & Dorofee, A. Introduction to the Security Engineering Risk Analysis (SERA) Framework (CMU/SEI-2014-TN-025). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=427321

Woody, C.; & Alberts, C. “Evaluating Security Risks using Mission Threads.” CrossTalk 10, 2 (September/October 2014): 14-19. http://www.crosstalkonline.org/storage/issue-archives/2014/201409/201409-Woody.pdf

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

Alberts, C.; Woody, C.; & Dorofee, A. Wireless Emergency Alerts CMSP Cybersecurity Guidelines (CMU/SEI-2015-SR-020). Software Engineering Institute, Carnegie Mellon University, 2015. http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20CMSP%20Cybersecurity%20Guidelines.pdf

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

For Additional Information

Christopher Alberts
Principal Engineer
Cyber Security Engineering
CERT® Division, Software Engineering Institute

Email	cja@cert.org
Phone	412-268-3045
WWW	http://www.cert.org/cybersecurity-engineering/
U.S. mail	Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

© 2016 Carnegie Mellon University
[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Software Engineering Institute | Carnegie Mellon