US Army Corps of Engineers
Infrastructure Systems Conference

Electronic Security Systems Process Overview

Electronic Security Center

4 August 2005

Outline

- *About the Electronic Security Center*
- Physical Security System Model
- Project Initiation
    - Identify Need
    - Threat Assessment
    - Vulnerability Assessment
    - Risk Analysis
    - Define Countermeasures
- Designer Responsibilities
- Quality Control
- Criteria

**US Army Corps
of Engineers**

Engineering and Support
Center, Huntsville

*The
Electronic Security Center*

- Intrusion Detection Systems
  - *Mandatory Center of Expertise*

- *Corps of Engineers*

- *Huntsville, AL*

Electronic Security Center Charter

- AR 190-13 Requirement:

    - Maintain Nucleus of ESS Specialists

    - Respond Expediently to Army ESS Needs

    - Chartered as USACE Mandatory Center of Expertise by ER-1110-1-8158 (Program Management Plan)

- HQUSACE Proponent:

    - CEMP-ET, Mr. Robert A. Fite (202) 761-7169

Electronic Security Center Mission

- Surveys

- Criteria and Design

- Design Reviews

- Technical Proposal Reviews

- Review Contractor Submittals

- Procure, Install, Test, Start-up Systems

- Teaching

- Special Studies and Investigations
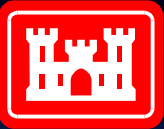
Physical Security Model

- ESS enhances the probability of <u>detecting</u> an aggressor before he compromises a protected asset.

- <u>Delay</u> and <u>response</u> elements are required to defeat the aggressor after he is detected.

Deter

Detect
(& assess)

Delay

Defeat the Aggressor!

Deter

Deter

Respond
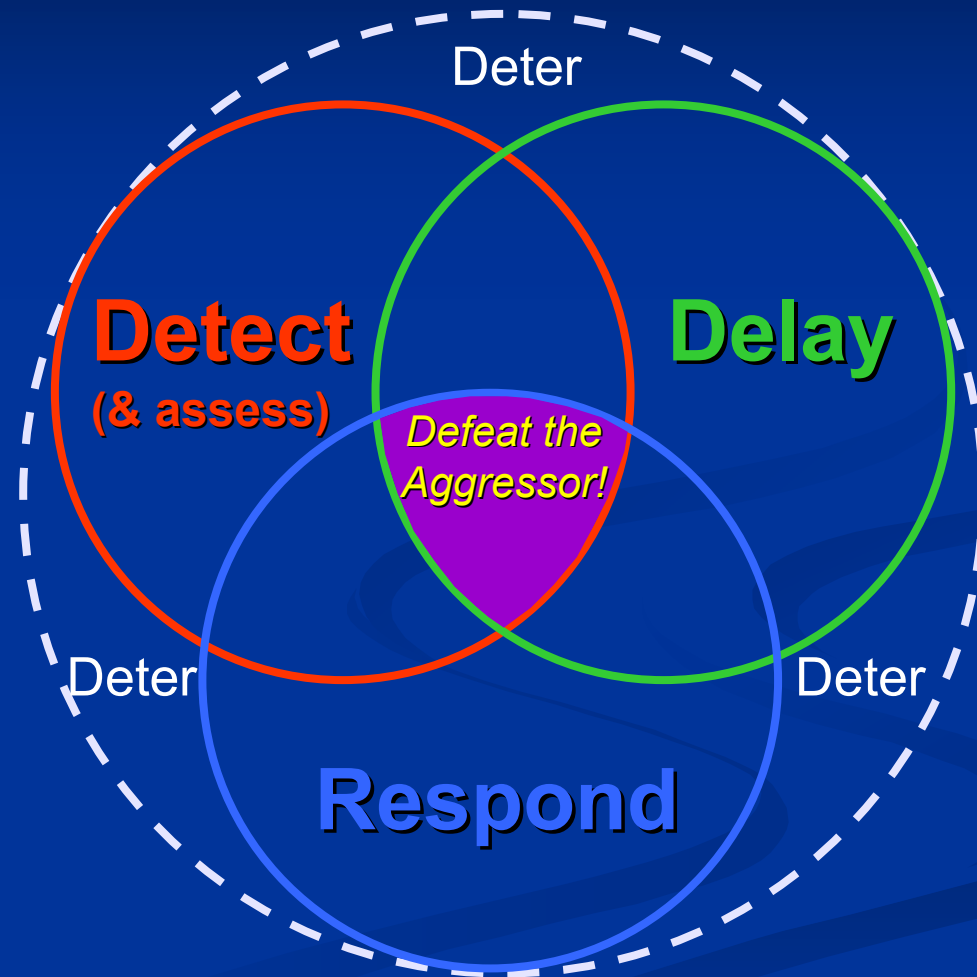
ESS is only one component of physical security…

Functional Elements of an Effective Security System
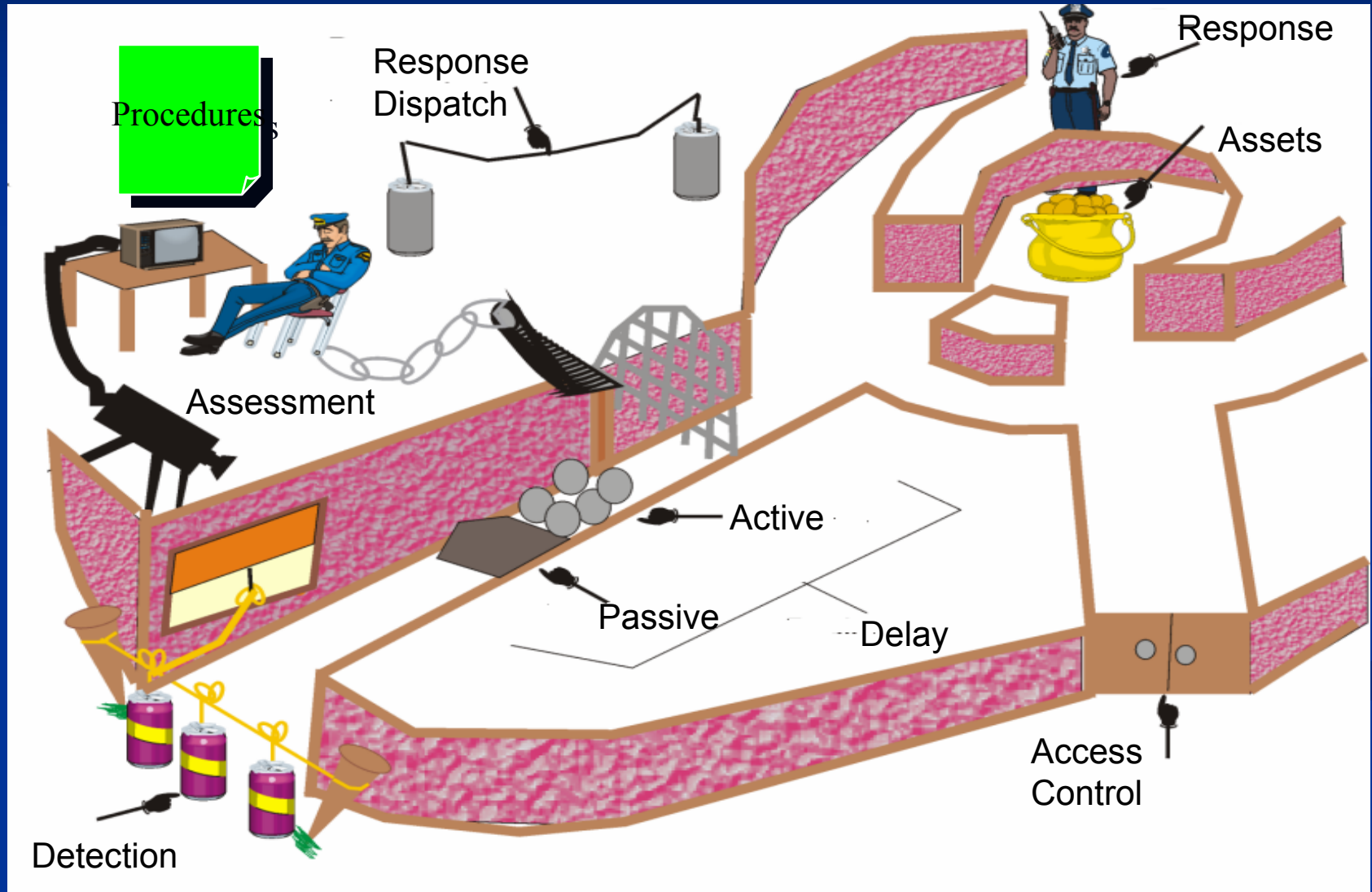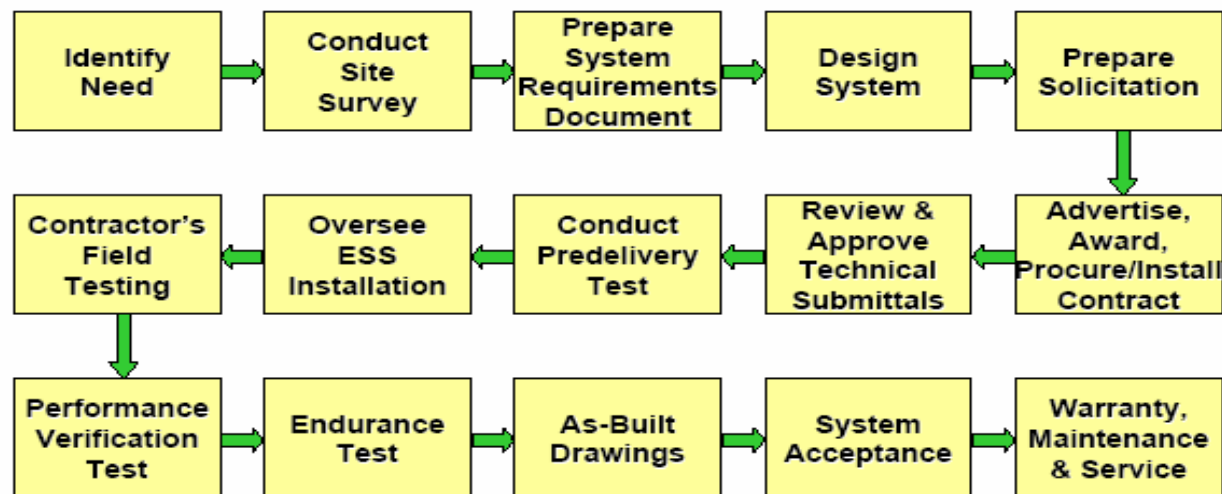
US Army Corps
of Engineers

Engineering and Support
Center, Huntsville

ESS Implementation

ESS implementation, whether a brand new system or an upgrade of an existing system, will generally progress as follows...

Identify Need → Conduct Site Survey → Prepare System Requirements Document → Design System → Prepare Solicitation

Prepare Solicitation → Advertise, Award, Procure/Install Contract → Review & Approve Technical Submittals → Conduct Predelivery Test → Oversee ESS Installation → Contractor's Field Testing

Contractor's Field Testing → Performance Verification Test → Endurance Test → As-Built Drawings → System Acceptance → Warranty, Maintenance & Service

Measure twice, cut once...an engineered solution!

Don't forget training!

Identify Need

- **Basis of Need**
- **Assess Threats**
- **Assess Vulnerability**
- **Analyze Risk**
- **Define Countermeasures**

Team Effort – Cannot be done by one person

Basis of Need

- **Regulatory Compliance**

  (thou shall…)

- **Risk Management**

  (smart, cost effective)

Army Regulatory Requirements

US Army Corps of Engineers

Engineering and Support Center, Huntsville

	AR 190-13	AR 190-11	AR 190-16	AR 190-51	DA PAM 190-51	AR 380-19	AR 37-103	DCID 1/21	AR 50-5-1	AR 190-59
ARMS, AMMUNITION, & EXPLOSIVES (AA&E)	X	X								
MEDICAL FACILITIES	X			X	X					
ADP FACILITIES	X					X				
SENSITIVE COMPARTMENTED INFO FACIL (SCIF)	X							X		
COMMO FACILITIES	X		X		X					
FINANCE & ACCOUNTING OFFICES (F&AO)	X			X	X					
ARMY MUSEUMS	X			X						
COMMISSARIES/WAREHOUSES	X			X	X					
CENTRAL ISSUE FACILITY (CIF)	X			X	X					
TRAINING AIDS SUPPORT CENTER (TASC)	X			X	X					
POL STORAGE	X			X	X					
COMMO/ELECTRONICS STORAGE	X			X	X					
REPAIR PARTS STORAGE	X			X	X					
ENG SUPPLIES/CONST MATERIALS	X			X	X					
MAIL/POSTAL	X									
NUCLEAR STORAGE AREAS	X								X	
CHEMICAL STORAGE AREAS	X									X
MILITARY/CIVILIAN WORKS	X									

Risk Management

$$R = P_A * C * (1 - P_E)$$

where

R = Risk associated with specific threat/asset scenario

P_A = Likelihood of adversary attack

C = Consequences of successful attack

P_E = Security system effectiveness in mitigating the attack
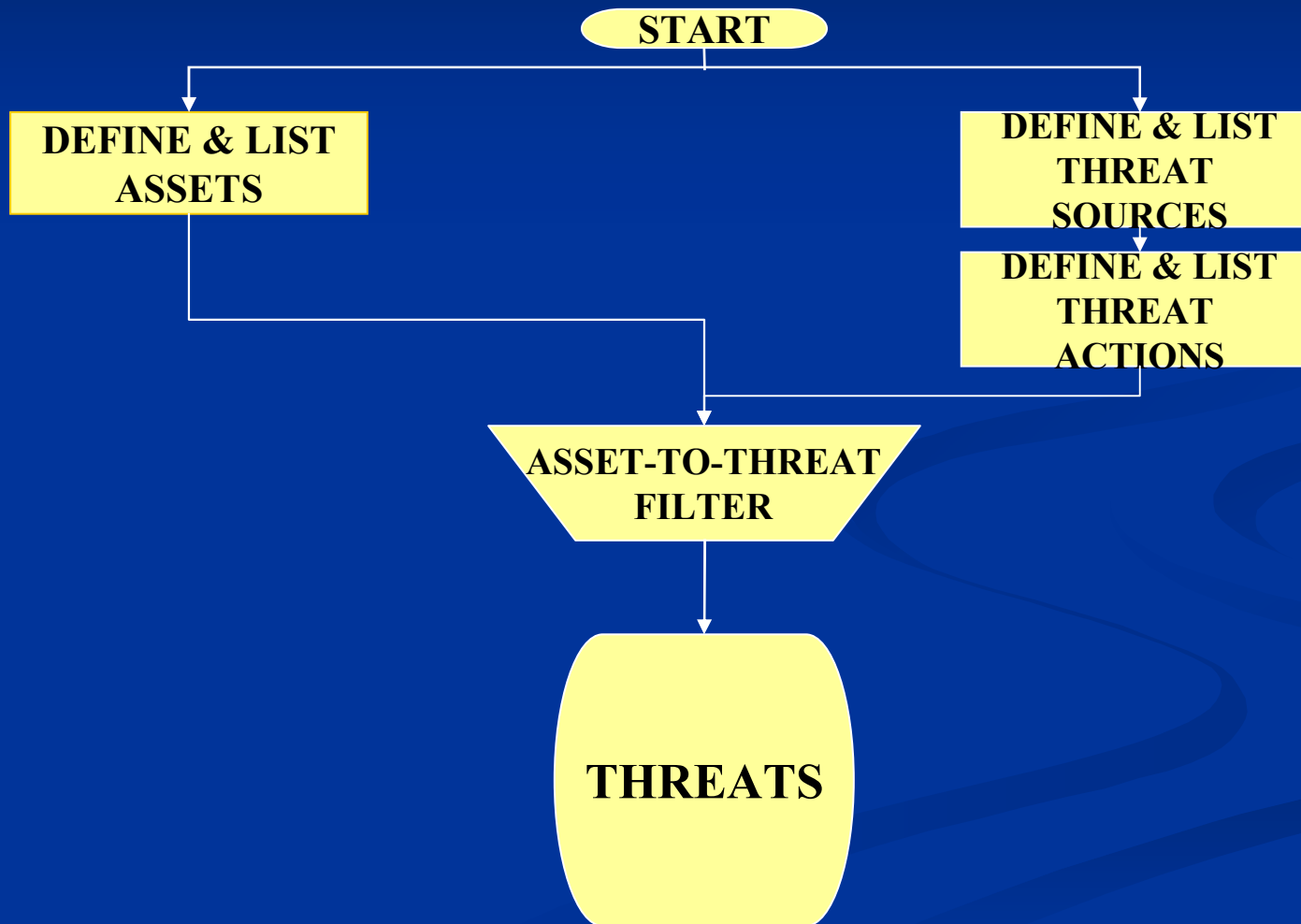
Threat Assessment

- Normally Already Done for Military Facilities
  - Requirements Implemented by Regulation
- Requires Identification of:
  - Assets Requiring Protection
  - Threat Sources
  - Threat Actions
  - Threat Characteristics
  - Threat Tools
  - Severity of Success on the Asset
- Evolving Threats Must be Considered

Assets

- **PEOPLE**: Includes all persons who may venture on the property.
  - Some distinct groups may require unique protective measures.
  - These groups include High-Ranking Executives, Employees, Occasional Visitors to private spaces, and the public.
- **EQUIPMENT**: Those things of value that are not built into a building and are not consumable.
- **BUILDINGS**: Real property of the asset.

- **FUNDS**: Funds as assets refer to negotiable documents or cash that are required for normal operation of the agency.
- **MATERIAL**: Materials include consumable supplies or merchandise needed in the conduct of normal business.
- **REPUTATION**: The reputation of the agency and its public perception.
- **PERSONAL PROPERTY**: The property owned by employees or visitors while on the protected property.
- **INFORMATION**: Information in any form — paper copies, digital, electronic print, electronic images, audio recordings, etc.

Building an Assets List

- Group Assets That Require Similar Protection

- Locate Assets That Require Similar Protection

- Determine Level of Protection Required for Each Category of Asset

Threat Sources

US Army Corps
of Engineers

Engineering and Support
Center, Huntsville

- Terrorists

- Extremists

- Organized Crime

- Saboteurs

- Sophisticated Criminals

- Unsophisticated Criminals

- Insiders

- Spies

Threat Actions

US Army Corps of Engineers

Engineering and Support Center, Huntsville

- **ROBBERY**: Stealing by threat to persons in occupied premises.

- **BURGLARY**: Breaking & entering unoccupied premises to steal.

- **SABOTAGE**: Intentional destruction of material, equipment, or systems to disrupt services or processes.

- **VANDALISM**: Intentional destruction or damaging property for vengeance or marking turf.

- **THEFT OF KNOWLEDGE**: Theft of information that may or may not be known to be lost.

- **KIDNAPPING & HOSTAGE TAKING**: Kidnapping is forceful abduction of some individual with the holding location generally unknown. With hostage taking, the holding location is generally known

- **INJURY OR DEATH** (Battery): The inflicting of injury or death by an adversary against another person.

- **ASSAULT**: The attempt or perceived threat of injury or death.

- **DISRUPTION OF SERVICES**: Those actions taken by adversaries that go beyond destruction of material, equipment, or systems.

- **DEVASTATING ATTACK**: An attack with the purposes of mass destruction of property and multiple deaths and injuries.

Vulnerability Assessment

- Most Data Collected During a Site Survey

  - Observational Data Collection

  - Interviews

- Identify Weaknesses and Examine Effectiveness of Countermeasures Against Threats

  - Vulnerabilities = Difference Between Existing Protection and Needed Protection

- Use Results of Threat Assessment to Determine Vulnerabilities

  - Compare Existing Security Measures Against Threat

Site Survey

- **Survey Team -- (Typically 2 to 4 people)**

    - **Facility User/Operations**
    - **DPW/Logistics**
    - **DOIM/Communications**
    - **Safety**
    - **Security**
        - **Local**
        - **IDS-MCX or MACOM**

Performing the Survey

- **Know who your customer is**
- **In-Brief**
- **Drawing Packages**
    - **As-builts for existing ESS**
    - **Infrastructure**
    - **Electronic copies if available**
- **Threat Assessment**
- **Visit facilities or assets to be protected**
- **Environmental considerations**
- **Formulate existing conditions and recommended actions**
- **Exit Briefing**
- **Report Generation**

US Army Corps of Engineers

Engineering and Support Center, Huntsville

Risk Analysis

- Determine Adverse Consequences (Impact) of Threat Event
  - Loss of Life
  - Loss of Capability
  - Cost
- Determine Probability of Threat Occurrence
  - Use Weighted Factors
  - Knowledgeable Professionals Reduce Subjectivity (Educated Guessing)

Ways of Dealing with Risk

- Apply Preventive Measures that Prevent an Adverse Occurrence

- Apply Contingent Measures that Reduce the Adverse Impact of an Adverse Occurrence

- Accept the Risk
  - Usually Selected If:
    - The Impact Is Low
    - The Probability of Occurrence Is Low
    - No Solution Offered by Technology

Define Countermeasures

- Develop Alternatives For Reducing Vulnerabilities
- Key Considerations:
  - Cost
  - Effectiveness
  - Interoperability
  - Regulatory Requirements
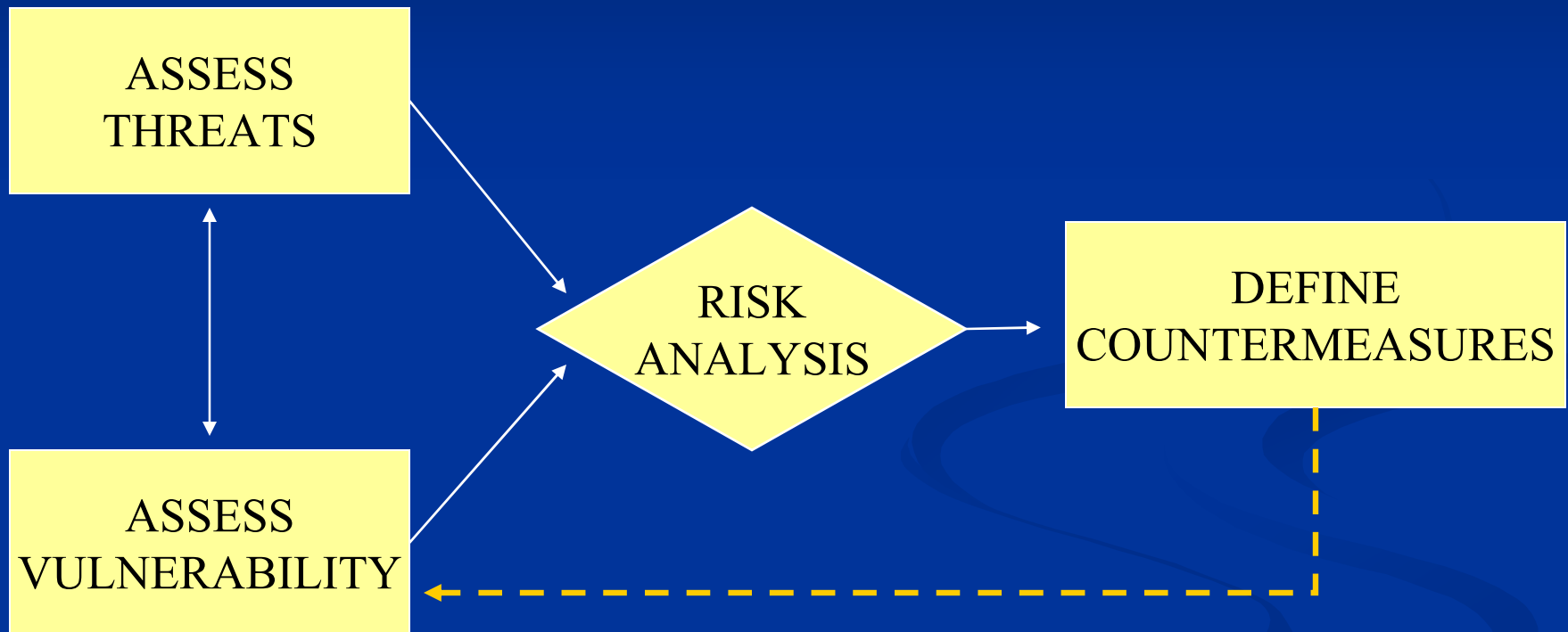
Designer Responsibilities

- Work With the End User to Define Basic Factors
  - Threat Conditions at a Facility/Asset
  - Identify Security Vulnerabilities
  - Specify the Security System Requirements
  - Determine Site Operational/Environmental Conditions
  - Resolve Cost Considerations/Constraints
- Resolution of the Basic Factors is a Critical First Step and Must be Completed Before:
  - Initiating Engineering Design
  - Hardware/Software Acquisition
  - Integration and Installation Activities

Criteria

- **Unified Facilities Criteria**

    - UFC 4-020-01FA : Security Engineering Project Development

    - UFC 4-020-02FA : Security Engineering Concept Design

    - UFC 4-020-03FA : Security Engineering Final Design

    - UFC 4-020-04FA : Security Engineering Electronic Security Systems

ESS Implementation

ESS implementation, whether a brand new system or an upgrade of an existing system, will generally progress as follows…

Identify Need → Conduct Site Survey → Prepare System Requirements Document → Design System → Prepare Solicitation

Contractor's Field Testing ← Oversee ESS Installation ← Conduct Predelivery Test ← Review & Approve Technical Submittals ← Advertise, Award, Procure/Install Contract

Performance Verification Test → Endurance Test → As-Built Drawings → System Acceptance → Warranty, Maintenance & Service
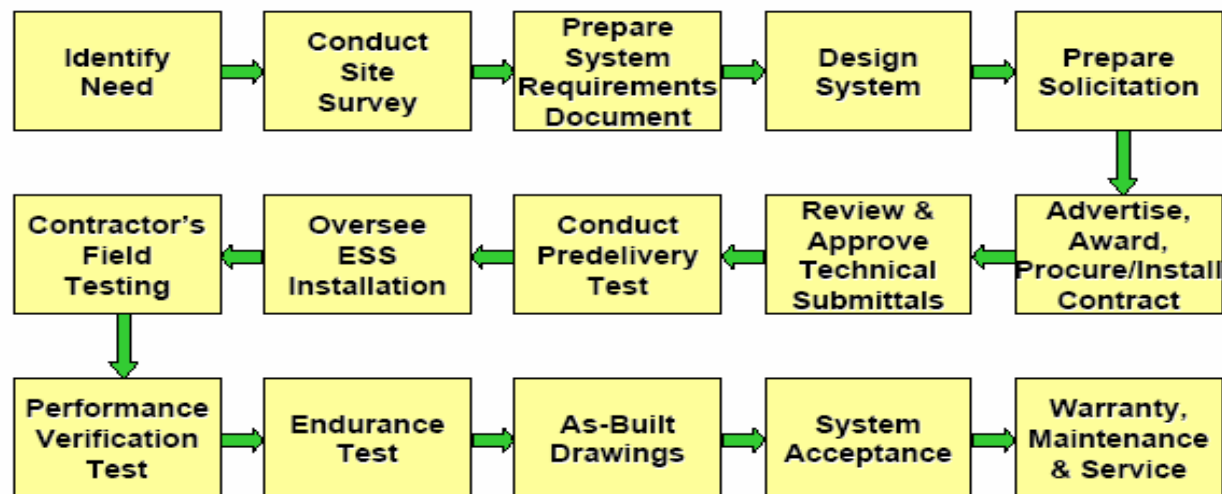
Measure twice, cut once…an engineered solution!

Don't forget training!

Elements of a Security System
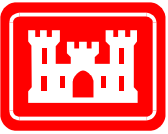
US Army Corps of Engineers
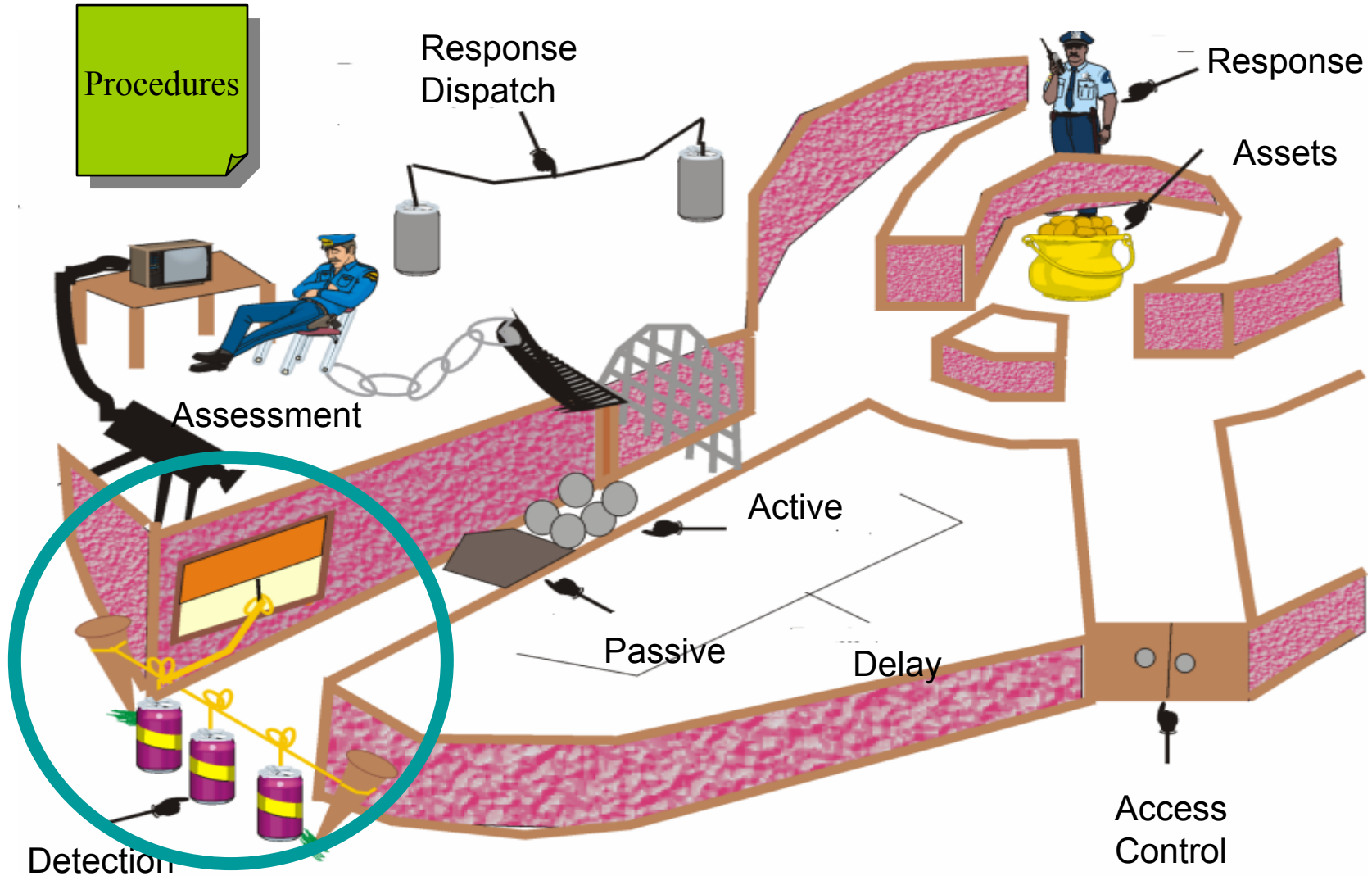
Engineering and Support Center, Huntsville

DETECT

ASSESS

DELAY

RESPOND

Functional Elements of an Effective Security System

US Army Corps of Engineers
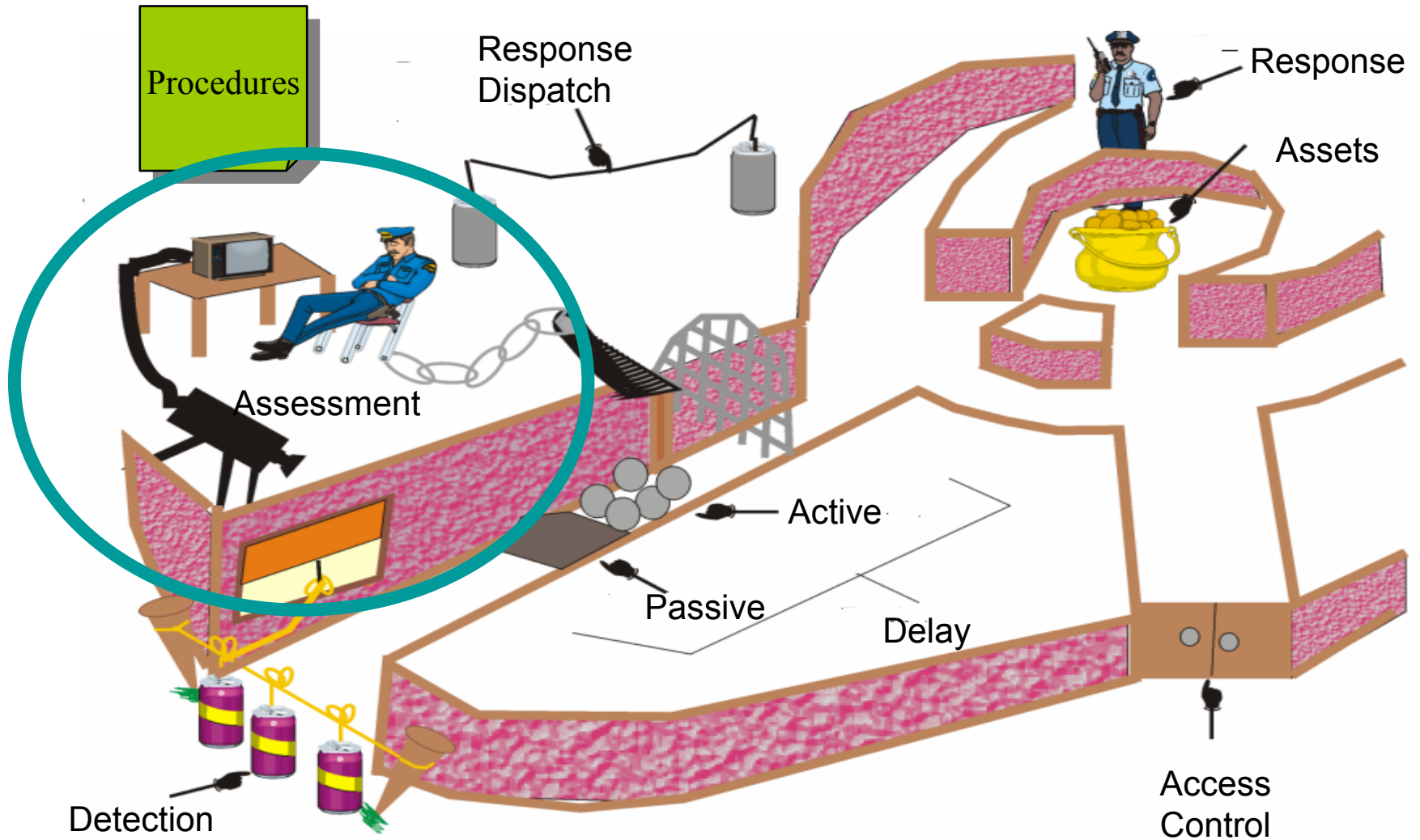
Engineering and Support Center, Huntsville

Procedures

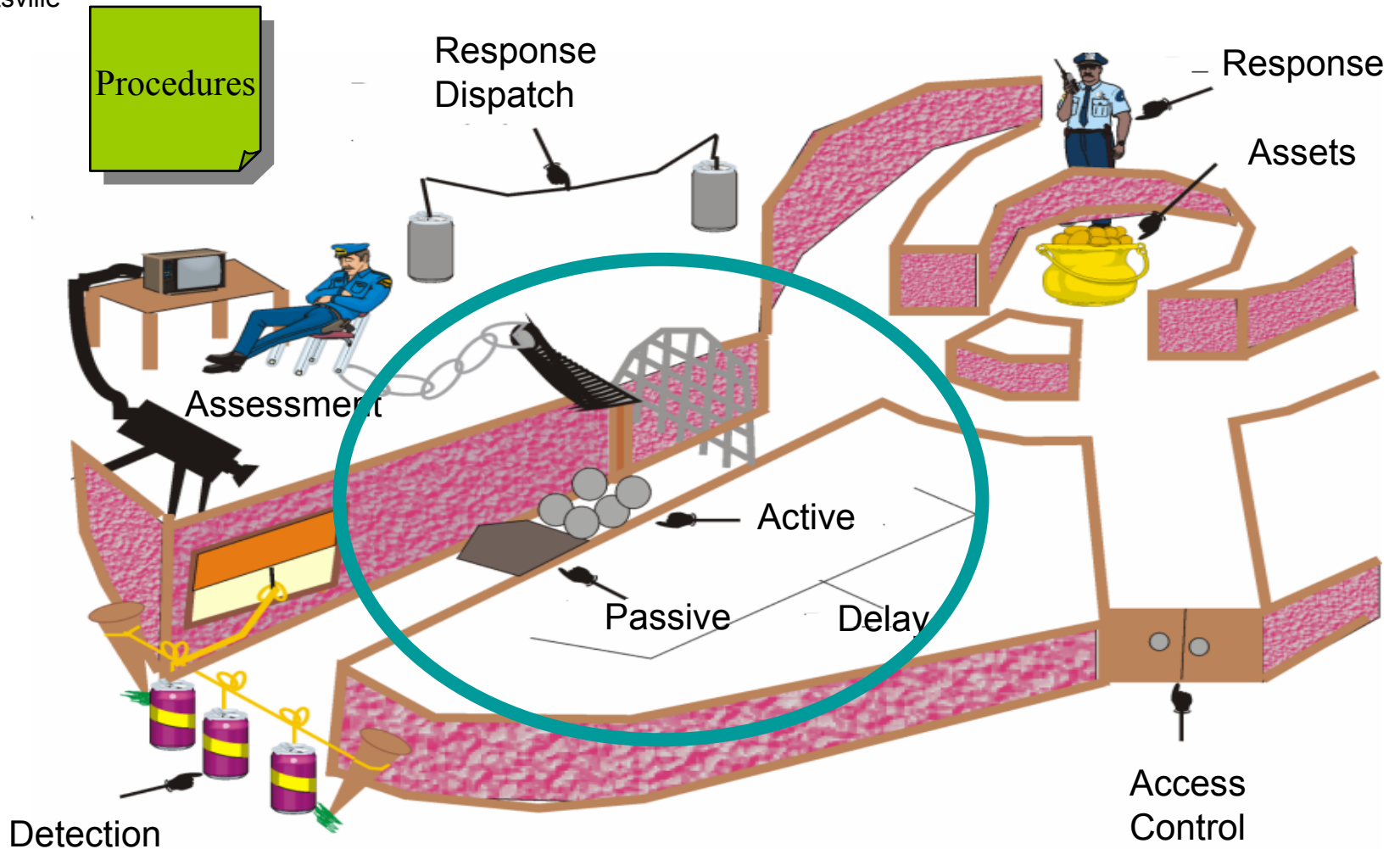Response Dispatch

Response

Assets

Assessment

Active

Passive

Delay

Detection

Access Control

- Sensing a Specified Target Moving Through a Line of Demarcation

  - Interior Sensors Suitable for Expected Target

  - Exterior Sensors Suitable for Expected Target

  - Limited to Areas Free of Likely Nuisance Alarm Sources

  - Continuous Ring or Area Surrounding Assets
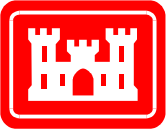
Functional Elements of an Effective Security System

US Army Corps of Engineers
Engineering and Support Center, Huntsville

Procedures

Response Dispatch

Response

Assets

Assessment

Active

Passive

Delay

Detection

Access Control

Assessment

- Visual Evaluation of a Detected Target
  - Validates a Detection As Threat or Non-Threat
  - Offers Additional Information About Target
    - Direction of Movement
    - Speed of Movement
    - Numbers of Targets
    - Tools or Armament of Targets
  - Coordinated With Detection
  - Information Assists Response Forces
- Assessment is Time Sensitive
  - Guard Direct Assessment
  - Guard CCTV Remote Assessment
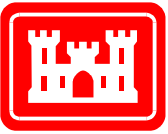
Functional Elements of an Effective Security System

US Army Corps of Engineers
Engineering and Support Center, Huntsville

Procedures

Response Dispatch

Response

Assets

Assessment

Active

Passive

Delay

Detection

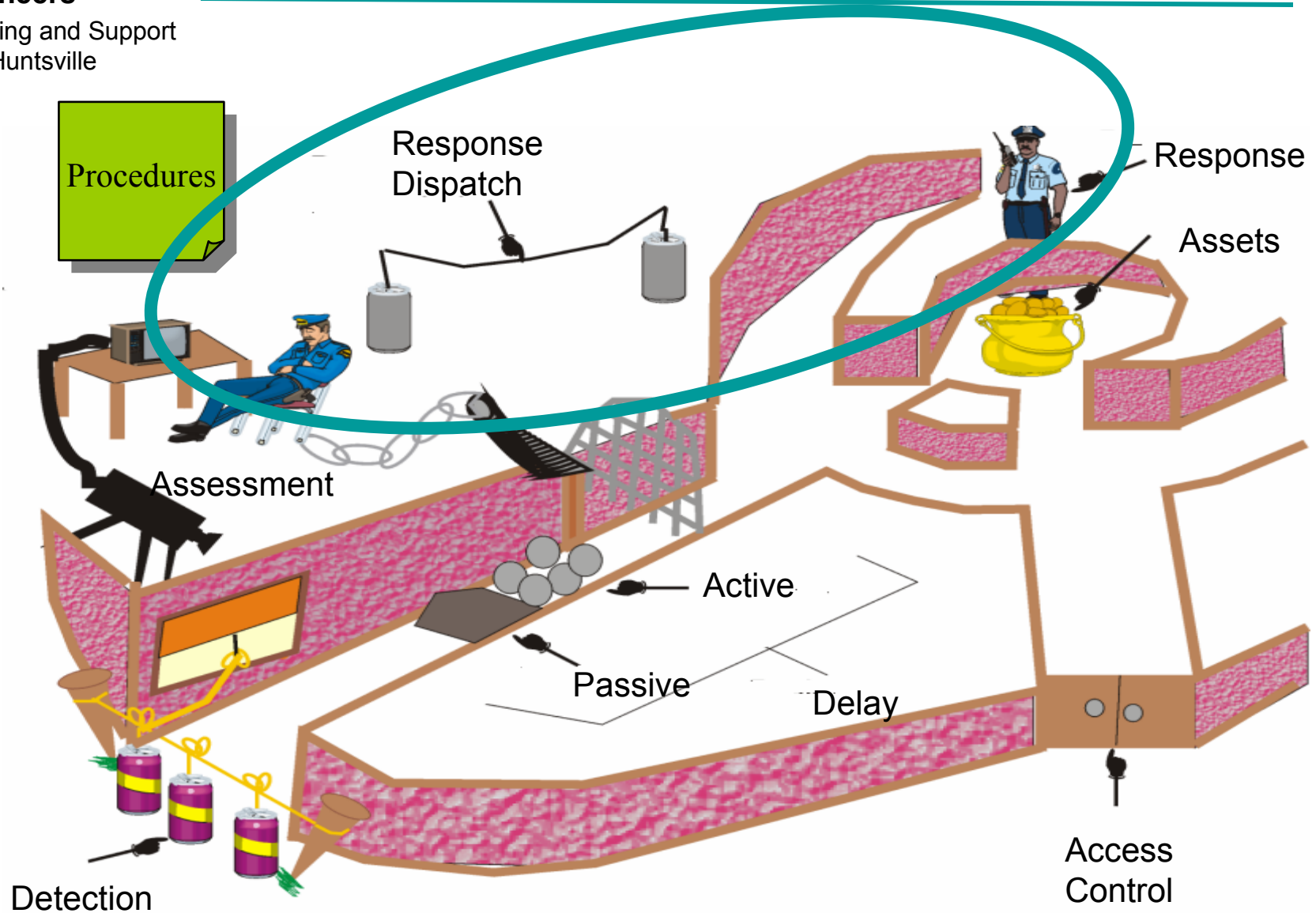Access Control

Delay

- Features That Slow Intruders Until Response Forces Can Intercept

  - Consist of Some Form of Barrier

    - Man-Made or Natural

    - Active or Passive

- Barriers Are Often Tailored for Selected Threat Characteristics
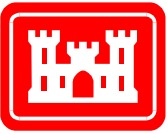
Functional Elements of an Effective Security System

US Army Corps of Engineers
Engineering and Support Center, Huntsville

Procedures

Response Dispatch

Response

Assets

Assessment

Active

Passive

Delay

Access Control

Detection

Response

- Action Taken to Prevent Intruders From Accomplishing Their Objectives Against an Asset
  - Consists of Response Forces, Weapons, Vehicles Communications, and Tactics
  - Deployment Time Influences System Response Time and Delay Time Requirements
  - Must Be Structured to Be Effective for an Entire Range of Intrusions
- Security Strategy
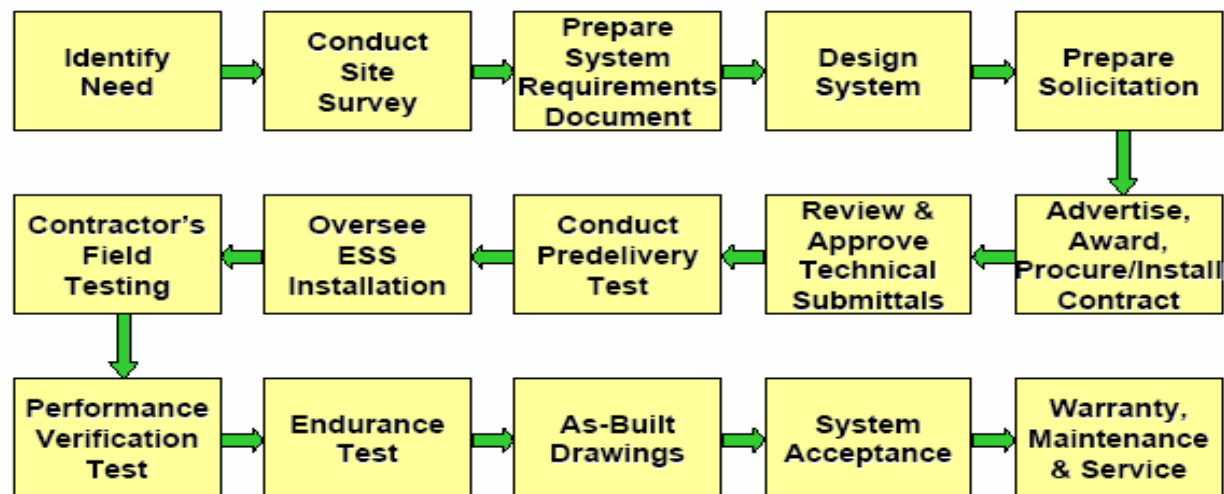 - Denial
  - Containment
  - Forensic

Quality Assurance

- **Review of Data Packages**
    - **System Drawings**
    - **Manufacturer's Data**
    - **Certifications**
    - **Testing**
        - **Pre-delivery Testing**
        - **Contractor's Field Tests**
        - **Performance Verification Testing**
        - **Endurance Testing**

Criteria

- **Unified Facility Guide Specifications**

    - **UFGS 13720A: Electronic Security System (ESS)**

    - **UFGS 13721A: Small Electronic Security System**

    - **UFGS 16751A: Closed Circuit Television System (CCTV)**

    - **UFGS 13702N: Basic Intrusion Detection System (IDS)**

    - **UFGS 13703N: Commercial Intrusion Detection System (IDS)**

Criteria

- **Unified Facility Guide Specifications**

  - UFGS 16792A: Wireline Data Transmission Systems

  - UFGS 16794A: Coaxial Data Transmission Systems

  - UFGS 16768A: Fiber Optic Coaxial Data Transmission Systems

Criteria

US Army Corps of Engineers

Engineering and Support Center, Huntsville

(Under Development)

- **Unified Facilities Criteria**

  - Electronic Security Systems

  - Pre-Delivery Test Procedures

  - Performance Verification Test Procedure

- **Unified Facility Guide Specifications**

  - Update to CCTV Spec (Navy)

Criteria

(Proposed)

- **Unified Facilities Criteria**
  - ESS Equipment Siting Guide
  - Update FT Pistol ESS Typical Design Drawings

- **Unified Facilities Guide Specifications**
  - Wireless Data Transmission System
  - Stand-alone Mass Notification System
  - Video Intercom System
  - Mobile Relocatable Central Monitoring Station
  - Update to 13720 for Wide Area Sensors

Contact Information

- Name: Ken Haynes

- Phone: 256-895-1747

- Cell: 256-656-7557

- E-mail:

  doyce.k.haynes@hnd01.usace.army.mil

- Company:
  - US Army Engineering and Support Center, Huntsville
  - Electronic Security Center