Overview of Physical Security and Protective Measures

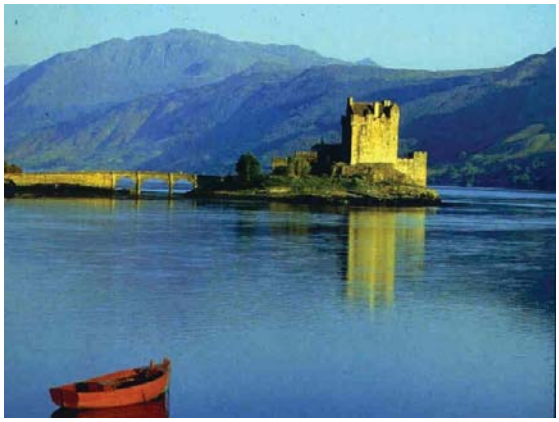
NAVFAC Far East
Presented by: Richard Cofer, P.E.
Naval Facilities Engineering Command Atlantic
Capital Improvements Business Line
Engineering Criteria and Programs

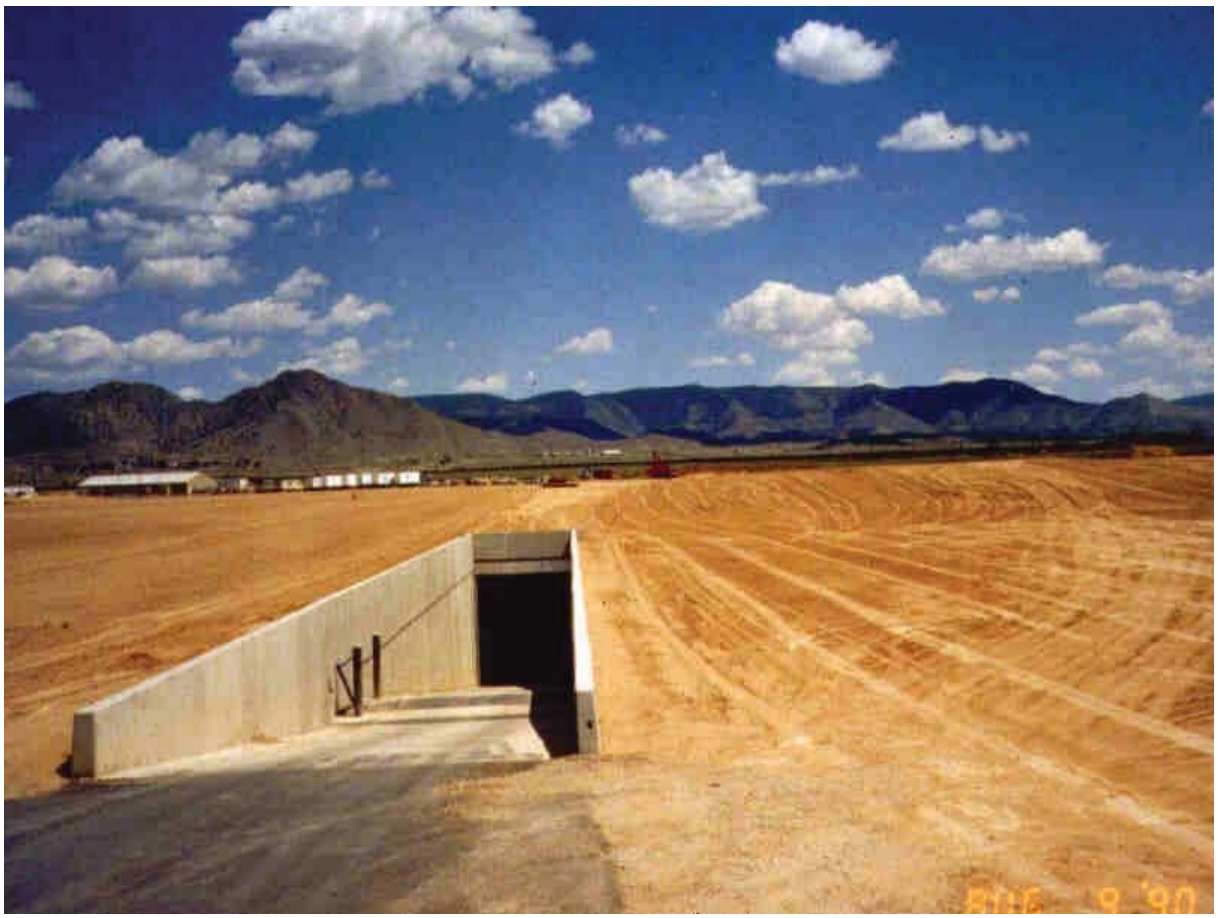
September 2019

HOW DO WE PROTECT OUR ASSETS?

Secure Facilities and Spaces

- **Secure Facilities and Spaces are designed and operated to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.**





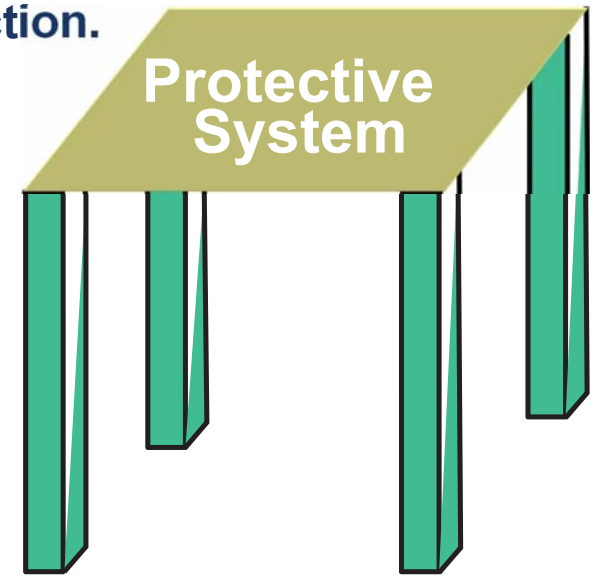
Antiterrorism vs. Physical Security

- **Force Protection:** *Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information.*
- **Protection:** *Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.*
- **Antiterrorism:** *Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.*
- **Physical Security:** *That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.*

Term definitions from Joint Publication 1-02, DoD Dictionary of Military and Associated Terms

Protective Systems

- **An integrated system of countermeasures designed to protect assets against threats to specific level of protection.**
  - **UFC 4-020-01**
- **Sitework Elements**
- **Building Elements**
- **Equipment**
- **Manpower/ Procedures**



Protective System

Security professionals design systems by:

- **Combining protective measures and operational procedures into an integrated system that works within a installation's, facility's, and user's constraints**
  - Components should complement each other and correct for vulnerabilities.
  - Components of the system should be coordinated to minimize gaps in responsibilities and performance.

Protective Systems

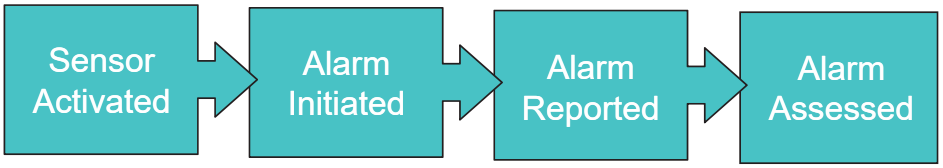
- System must detect potential threats, delay threats, and respond to threats.
  - This concept is referred to as of detect, delay/deny, and defend/defeat.





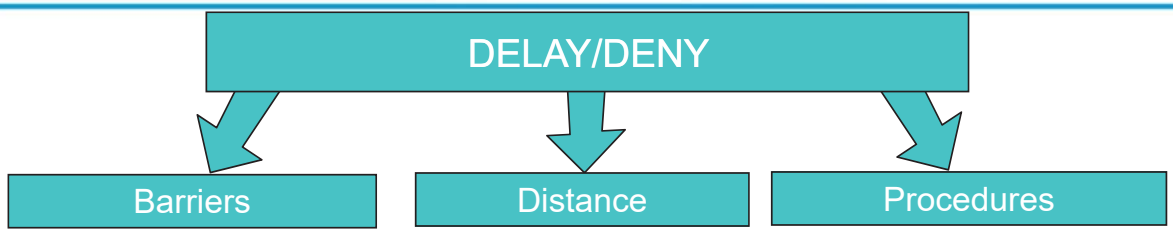

Protective systems must support the concept of detect, delay and respond.

Protective Systems: Detect



- Detect the presence of an aggressor
- Assess the validity of the threat
- Communicate the appropriate information to the response capability.

Protective Systems: Delay



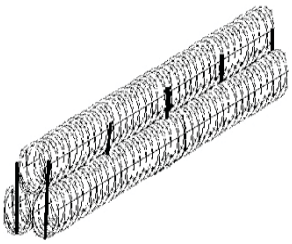
- **Delay is the time it takes for the aggressor to get from the point of detection to the point where the response capability interrupts or neutralizes the aggressor.**
- **Provide protective measures intended to hinder aggressor from reaching asset before response capability can intervene.**
- **Delay must be synchronized with security force response time to ensure assets are protected from compromise.**

Protective Systems: Defend/Defeat

- **Response sometimes referred to as defend/defeat, is the time it takes for the response capability to interrupt or neutralize a threat. This includes**
  - **Communication**
  - **Mobilization**
  - **Travel time**
  - **Tactics**

Protective System Delay

- How long does it take to:
  - Climb a fence with barbwire?
  - Cut through a fence?
  - Get over fence with a ladder?
  - Get over Concertina wire?
  - Break into a door?



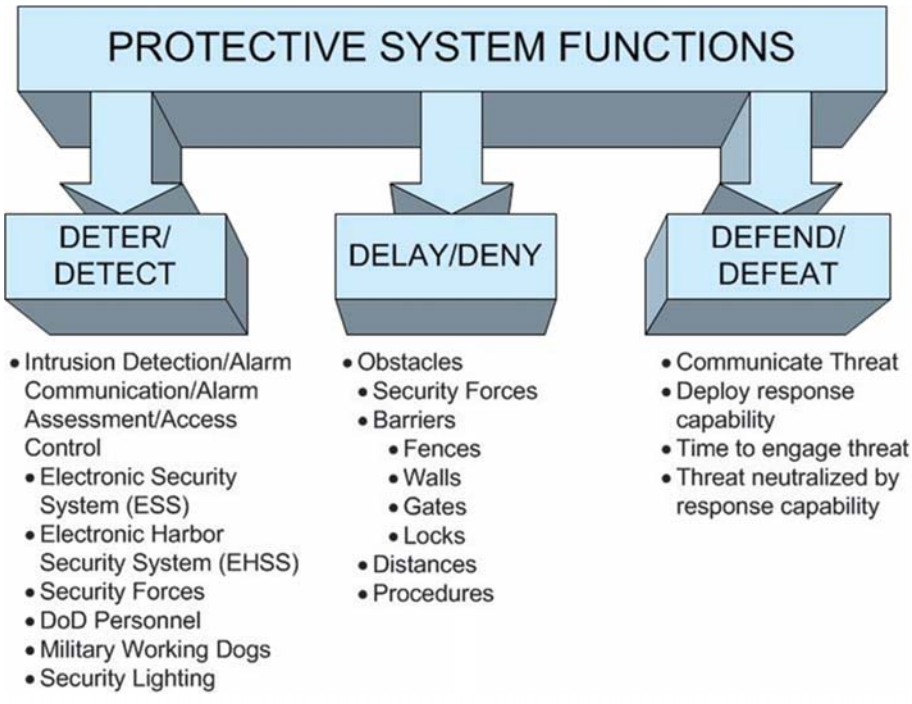
- How does response time and delay factor into the decision making process?

Adding Delay into the System

Response Capability

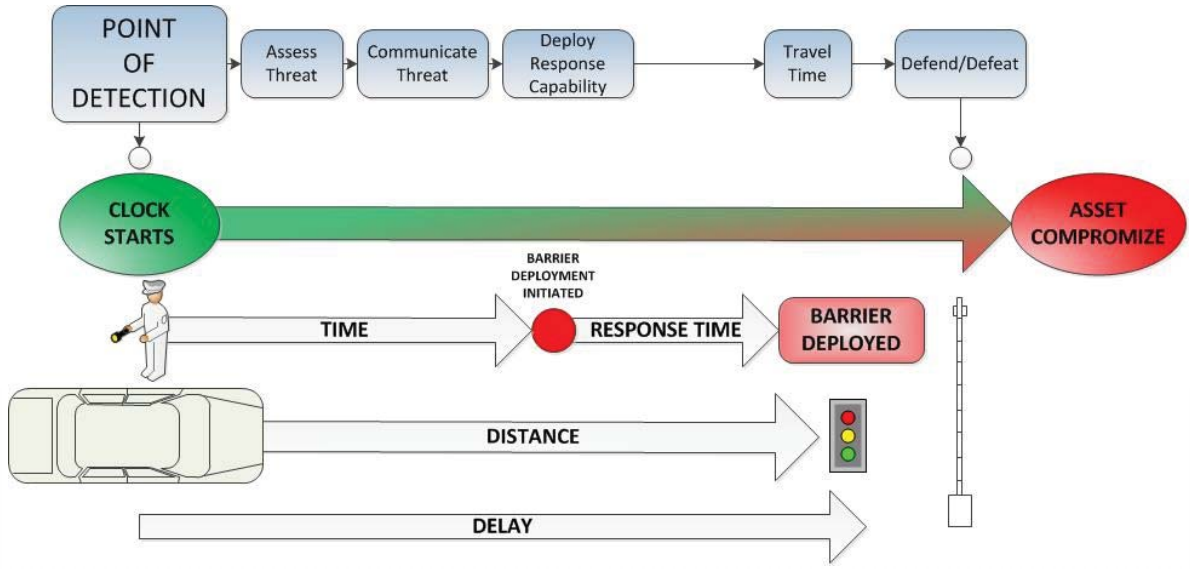
- Security Police
- Military Police
- Military Working Dogs
- Rapid Response Force
- Passive Barriers
- Active Barriers
- Waterfront Barriers

Protective System



Protective System Timeline

To be effective, the system must ensure the time between detection of an intrusion and intervention by response capability is less than the time it takes to compromise the asset.



Response Capability

What dictates a Protective System

- The requirements for Protective System must be established during the project planning stage.
- The decision to provide Protective Systems is based upon the following criteria:
  - DoD/Service policy/regulations
  - Operational procedures
  - Asset value (Relative value of items being protected)
  - Response Capability
  - Availability of security forces to patrol and observe protected areas
  - Availability of fiscal resources (procurement, installation, energy conservation, and maintenance costs)
  - Risk

Policies for Protective Systems

DOD PHYSICAL SECURITY AND ANTITERRORISM	
Title 10 U.S. Code, Sections 2859	Construction Requirements Related To Antiterrorism And Force Protection
Joint Publication 3-07.2	Antiterrorism (FOUO)
DoDI 2000.12	DoD Antiterrorism (AT) Program
DoDI 2000.16	DoD Antiterrorism (AT) Program Implementation and Standards
DoDD 3020.40	DoD Policy and Responsibilities for Critical Infrastructure
DoDM 5100.76	Physical Security of Sensitive Conventional Arms, Ammunitions, and Explosives
DoDM 5105.21	Sensitive Compartmented Information (SCI) Administrative Security Manual (Vols 1-3)
DoDM 5200.01	Information Security Program
DoDI 5200.08	Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
DoD 5200.08R	Physical Security Program
DoDI 0-5210.63	DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials
DoDI 5210.65	Minimum Security Standards for Safeguarding Chemical Agents
DoD Manual 5200.08 Vol 3	Access to DoD Installations
DNI / ICS 705-1	Physical and Technical Security Standards for SCIFs
ICS 705-2	Standards for the Accreditation and Reciprocal Use of SCI
IC Tech Spec	IC Technical Specification for Construction and Management of SCIFs
DoD Manual 5205.07	DoD Special Access Program (SAP) Security Manuals (Vols. 1-3)

Policies for Protective Systems

DON/USMC PHYSICAL SECURITY AND ANTITERRORIS	
SECNAVINST 3300..2C	DoN Antiterrorism Program
SECNAVINST M-5510.36	Department of the Navy Information Security Program
SECNAVINST S8126.1A	Navy Nuclear Weapons Security Policy
OPNAVINST 3300.53C	Navy Antiterrorism Program
OPNAVINST 3400.12	Required Operational Capability Levels for Navy Installations and Activities
OPNAVINST 5210.16	Security of Nuclear Reactors and Special Nuclear Material
OPNAVINST 5530.13C	Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E)
OPNAVINST 5530.14E	Navy Physical Security and Law Enforcement
OPNAVINST 5530.16A	Minimum Security Standards for Safeguarding Biological Select Agents and Toxins
NTTP 3-07.2.3	Navy Tactics, Techniques, And Procedures: Law Enforcement And Physical Security
NTTP 3-07.2.1	Navy Tactics, Techniques, And Procedures: Antiterrorism
MCO 5530.14A	Marine Physical Security Program

Policies for Protective Systems

ARMY / AIR FORCE PHYSICAL SECURITY AND ANTITERRORISI	
AR 190-13	Army Physical Security Program
AR 190-11	Physical Security of Arms, Ammunitions, and Explosives
AR 190-17	Biological Select Agents and Toxins Security Program
AR 190-51	Security of Unclassified Army Property
AR 190-59	Chemical Agent Security Program
AR 380-5	Department of the Army Information Security Program
AR 380-40	Policy for Safeguarding and Controlling Communications Security (COMSEC) Material
AFI 31-101	Integrated Defense
AFI 31-401	Information Security Program Management
AFPD 10-39	Safeguarding Biological Select Agents and Toxins

Policies for Protective Systems

- Geographic Combatant Commander (GCC) Requirements
  - GCC issue requirements for antiterrorism and physical security for installations within their area of responsibility through OPORDS.
  - Ensure GCC requirements are incorporated in addition to the requirements found in DoD and Service Directive/Instructions.
  - Resolve any differences in the requirements by applying the most stringent requirement.
- Installation Specific
  - As required by DODI 2000.16 and service directives, each installation must have an AT Plan and Physical Security Plan.
  - Plans provided procedures and recommendations for reducing risk and vulnerability of DOD personnel, their family members, facilities, and assets. As such, the installation AT Plan and Physical Security Plan reflect the foundation for requirements determination.
  - Installation specific requirements must be factored into all capital improvement initiatives.

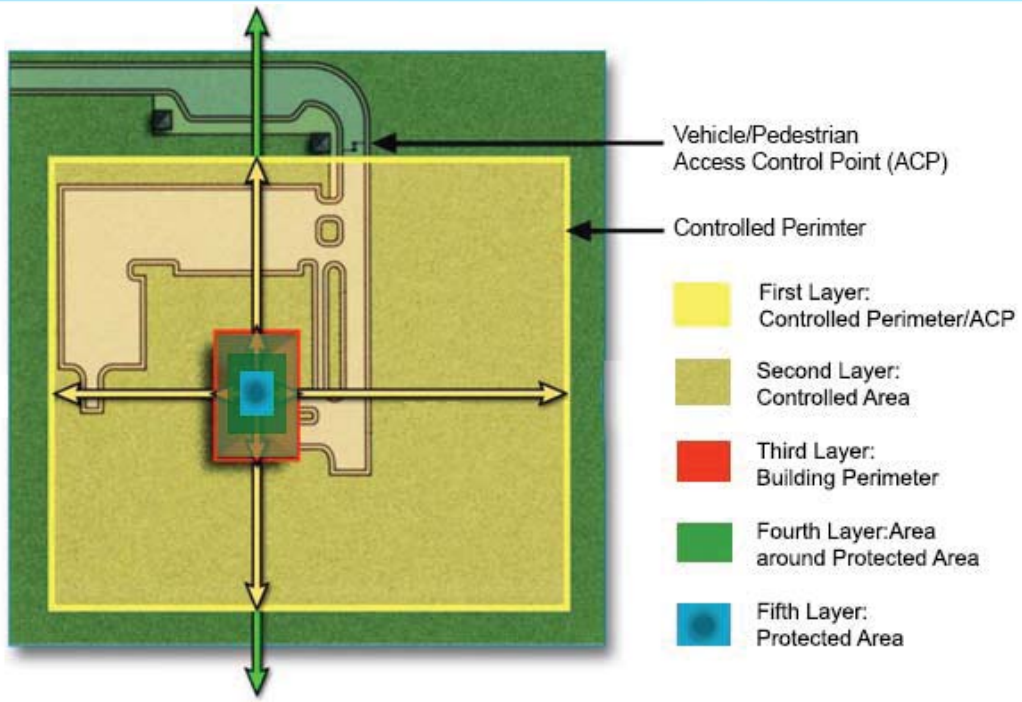
Design of Protective Measures

- The design of protective elements must take a system approach
- Physical Security Equipment (PSE) and protective measures are not independent!
- Design requires integration of PSE and protective measures with facility components and operations
  - Example: IDS “detects”; facility walls, doors, and locks provide “delay/deny”
  - Example: Determining proper detection and delay elements requires knowledge of response time

Security in Depth (SID)

- **Combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force.**
  - **Incorporating SID ensures that no single point of failure will render assets vulnerable to compromise.**
  - **SID strategy should establish a clearly defined sequence of boundaries and zones through which aggressors must pass to reach the protected asset.**
  - **Security measures and access controls should increase as aggressors approach the protected asset and transition from lower to higher security zones.**

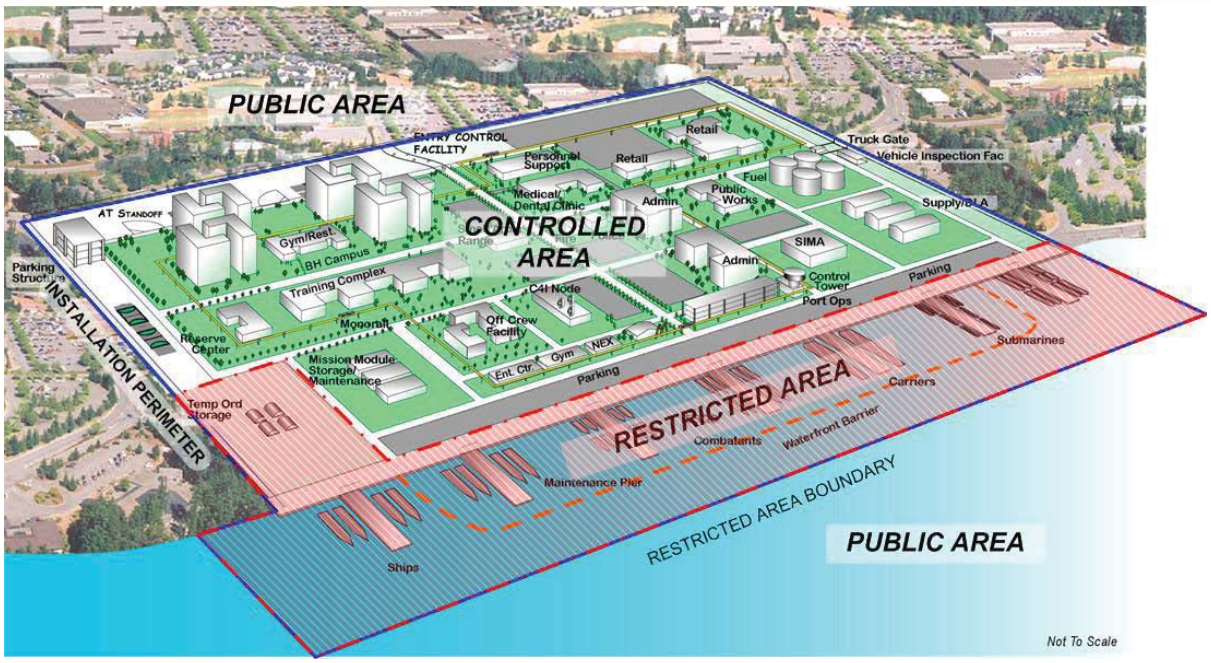
Security or Defense-in-Depth



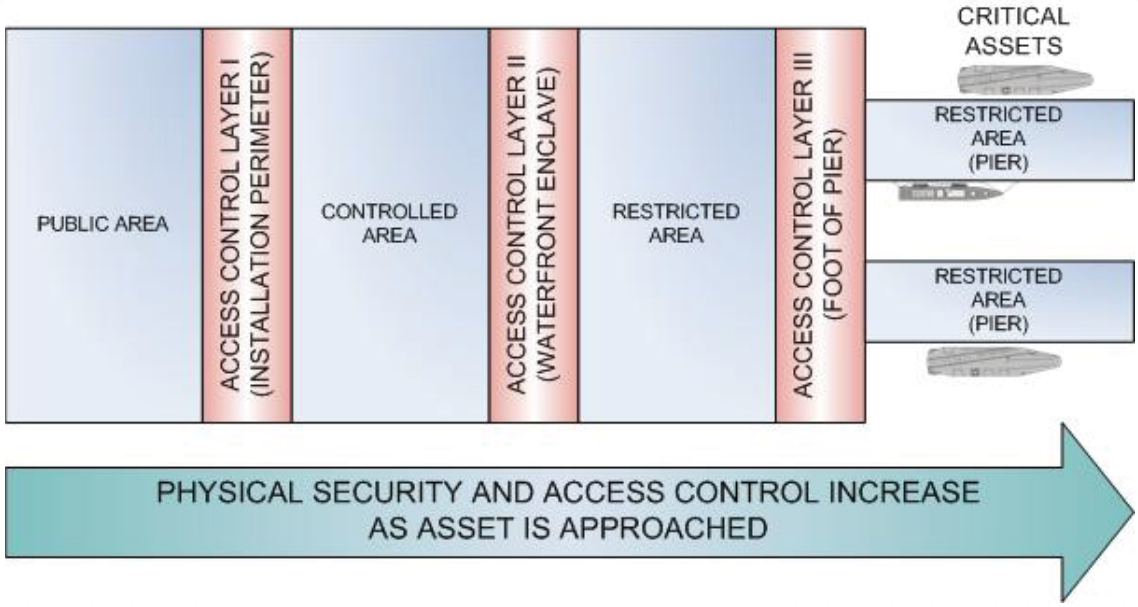
Security in Depth (SID)

- **The primary means of achieving SID include:**
  - **Located on a Military installation or compound with a dedicated response force of U.S. citizens or U.S. persons.**
  - **Located within a controlled or restricted area.**
  - **Located within a building or fenced compound that employs access control.**
  - **Located within the building away from exterior walls.**
  - **Located within a building on an upper floor.**
  - **Space adjacent to or surrounding the protected area is controlled and protected by alarm.**

Zone Concept



Zone Concept



SID and Zoning

Note: Security Lighting is not ideal

Other Design Philosophies

- "All Hazards" approach
  - Trying to find one design procedure to encompass threats like tornadoes, hurricanes, seismic, and blast.
- Protection versus "Resiliency"
  - Some assets too hard to protect
  - Resiliency relies on a work-around or quick replacement of parts to minimize downtime if asset is taken out.
  - Avoid; if possible, single point failures that can shut down an entire system.
  - Can you accept the consequences of asset being unavailable for a period of time?

Remember

Whenever possible, Protective measures should be:

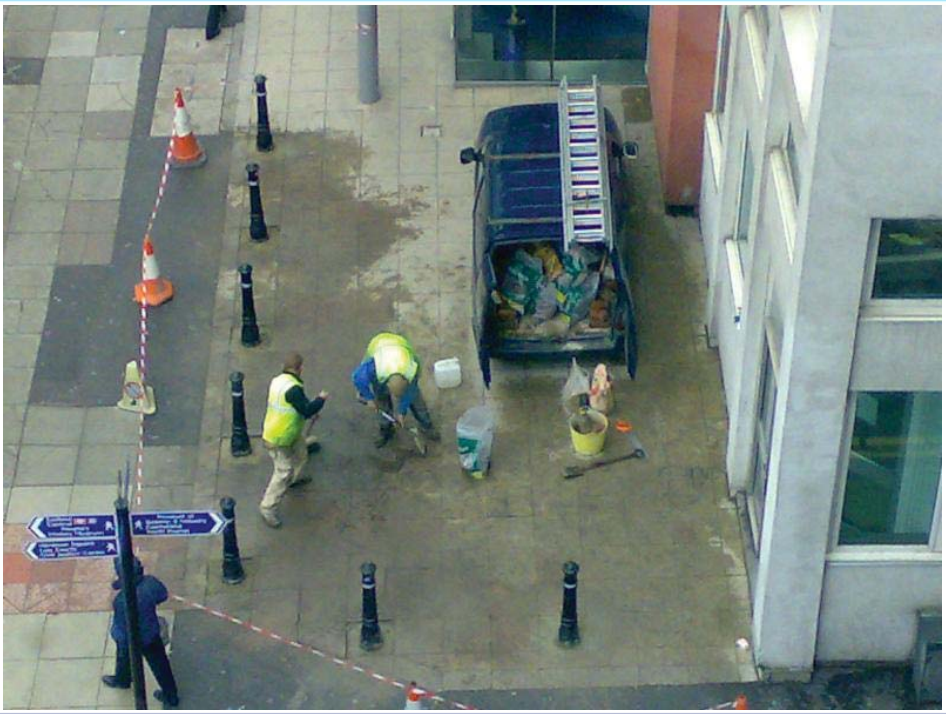
- **Appropriate**
- **Effective**
- **Unobtrusive**
- **Economical**

Effective, Unobtrusive, or Economical?

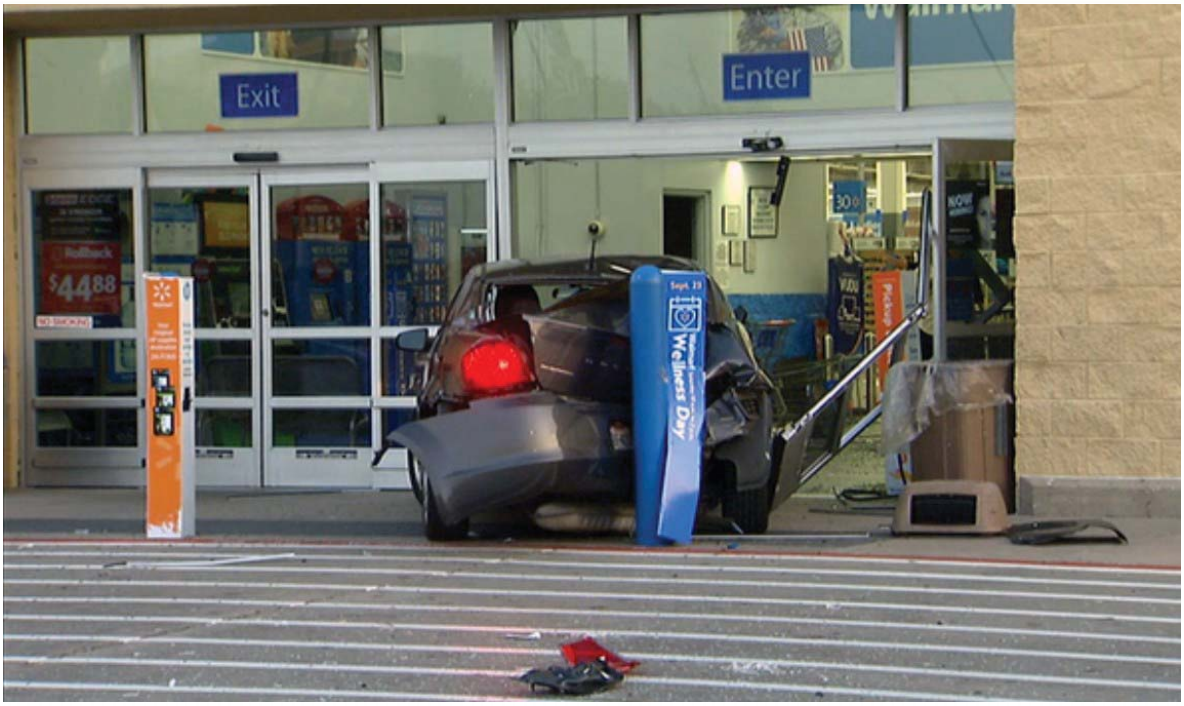
Effective, Unobtrusive, or Economical?

Effective, Unobtrusive, or Economical?

Effective, Unobtrusive, or Economical?

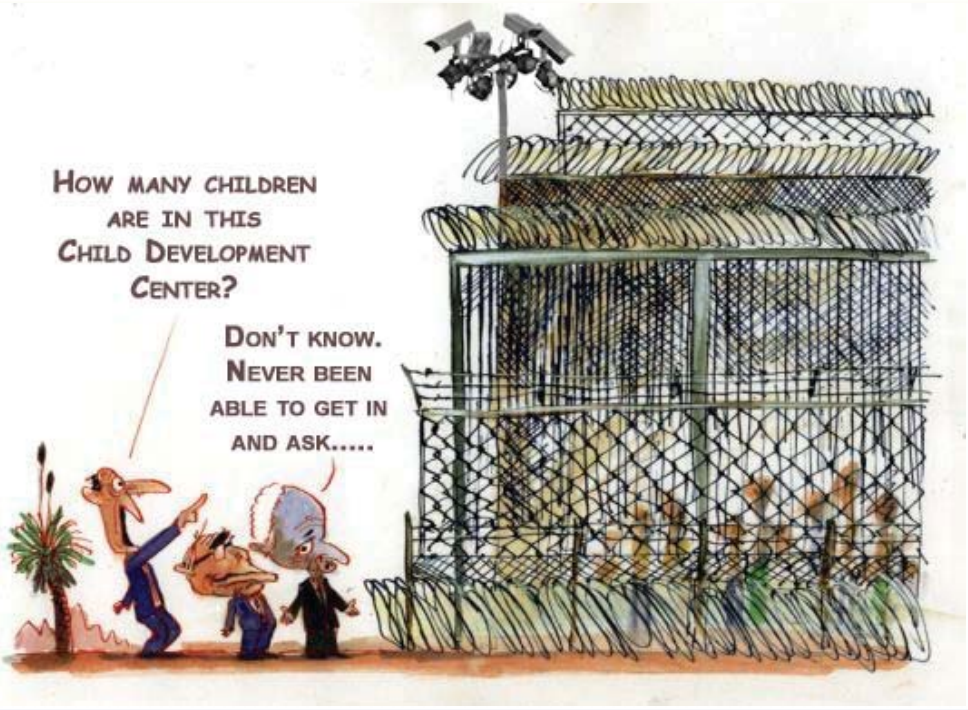


Effective, Unobtrusive, or Economical?



Effective, Unobtrusive, or Economical?

Effective, Unobtrusive, or Economical?



Thanks!