Unit XI

COURSE TITLE	Building Design for Homeland Security **TIME** 45 minutes

UNIT TITLE

Electronic Security Systems

OBJECTIVES

1. Explain the basic concepts of electronic security system components, their capabilities, and their interaction with other systems
2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety
3. Use the assessment process to identify electronic security system requirements that can mitigate vulnerabilities
4. Justify selection of electronic security systems to mitigate vulnerabilities

SCOPE

The following topics will be covered in this unit:

1. Perimeter layout and zoning of sensors
2. Intrusion detection systems and sensor technologies
3. Entry-control systems and electronic entry control technologies
4. Closed circuit television and data-transmission media
5. Control centers and building management systems
6. Definitions of the degree of security and control

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*,
   a. Pages 3-47 to 3-50
   b. Appendix D
   c. Security Systems and Security Master Plan sections of Checklist at the end of Chapter 1, pages 1-81 and 1-92
2. Case Study – Appendix A: Suburban, Hazardville Information Company or Appendix B: Urban, HazardCorp Building as selected
3. Student Manual, Unit XI-A or Unit XI-B as selected (info only – do not list in SM)
4. Unit XI visuals (info only – do not list in SM)

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist*

Attacks Against Buildings, pages 3-47 to 3-50; Appendix D; and Security Systems and Security Master Plan sections of the Checklist at the end of Chapter 1 (pages 1-81 to 1-92)
2. Instructor Guide, Unit XI
3. Student Manual (one per student) for selected Case Study
4. Overhead projector or computer display unit
5. Unit XI visuals
6. Risk Matrix poster and box of dry-erase markers (one per team)
7. Chart paper, easel, and markers

PREPARING TO TEACH THIS UNIT

•   **Tailoring Content to the Local Area:** This instruction unit is generic and need not be applied to the Local Area. However, this unit comes after Units IX and X where Local Area content is most easily inserted and this instruction unit supplements Units IX and X. Then,

as appropriate, locally oriented discussion can be inserted, especially if done in conjunction with the Case Study version selected for the course offering.

- **Optional Activity:** There are no optional activities in this unit, except Student Activity questions that are applicable to the selected Case Study (Suburban or Urban).

- **Activity:** The students will complete their familiarization with the Case Study materials. The Case Study is a complete risk assessment and analysis of mitigation options and strategies for a typical commercial office building located in a mixed urban-suburban environment business park (suburban) or a 50-story high-rise office building located in a downtown urban environment (urban). The assessment will use the DoD Antiterrorism Standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in **FEMA 426** and other FEMA publications related to risk management, emergency planning, and disaster recovery.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- Tell students how long they have to work on the requirements.

- While students are working, <u>all</u> instructors should closely observe the groups' process and progress. If any groups are struggling, immediately assist them by clarifying the assignment and providing as much help as is necessary for the groups to complete the requirement in the allotted time. Also, monitor each group for full participation of all members. For example, ask any student who is not fully engaged a question that requires his/her viewpoint to be presented to the group.

- At the end of the working period, reconvene the class.

- After the students have completed the assignment, "walk through" the activity with the students during the plenary session. Call on different teams to provide the answer(s) for each question. After each response simply ask if anyone disagrees. If the answer is correct and no one disagrees, state that the answer is correct and move on to the next requirement. If there is disagreement, provide the "school solution" and move on.

- If applicable to this activity, explain what information is to be transferred to the Risk Matrix poster. For this activity, the assessment of the building's security systems in greater depth may prompt the groups to adjust the vulnerability ratings in their Threat Matrix, with resultant changes to risk ratings.

- If time is short, simply provide the "school solution" and ask for questions. Do not end the activity without ensuring that students know if their answers are correct or at least on the
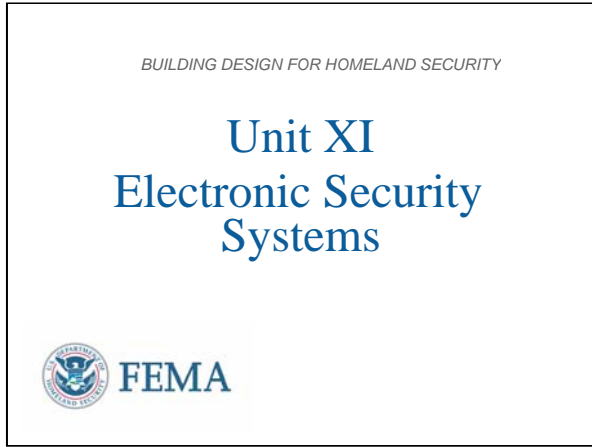
right track. Note, there is no right or wrong answer, but all answers must be justified with rationale.

- Ask for and answer questions.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-1

BUILDING DESIGN FOR HOMELAND SECURITY

Unit XI
Electronic Security
Systems

FEMA

Introduction and Unit Overview

This is Unit XI Electronic Security Systems (ESS). This unit will describe the types of sensors, concepts of operation of electronic security systems, and terminology used in the industry.

VISUAL XI-2

Unit Objectives

Explain the basis concepts of electronic security system components, their capabilities, and their interaction with other systems.

Describe the electronic security system concepts and practices that warrant special attention to enhance public safety.

Use the Building Vulnerability Assessment Checklist to identify electronic security system requirements that can mitigate vulnerabilities.

Justify selection of electronic security systems to mitigate vulnerabilities.

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-2

Unit Objectives

At the end of this unit, the students should be able to:

1. Explain the basis concepts of electronic security system components, their capabilities, and their interaction with other systems.
2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety.
3. Use the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** to identify electronic security system requirements that are needed to mitigate vulnerabilities.
4. Justify selection of electronic security systems to mitigate vulnerabilities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-3

Electronic Security System (ESS) Concepts

• Basic concepts of site security systems

• Use of ESS

• General ESS Description

• ESS Design Considerations

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-3

Electronic Security Systems Concepts

The **Building Vulnerability Assessment Checklist**, **Section 12 (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** can be used for the assessment of security systems. Security systems historically have been designed, installed, serviced, and monitored by physical security companies, typically after the completion of the building. New Internet and wireless technologies have significantly changed the way in which security systems are designed and now incorporation of security system design and processes should begin at the earliest stages of design or renovation. An electronic security system is the physical implementation of the elements of the Layers of Defense:
- Deter
- Detect
- Deny
- Devalue

In this unit, the student should have an appreciation for:
- Basic concepts of ESS
- Use of ESS
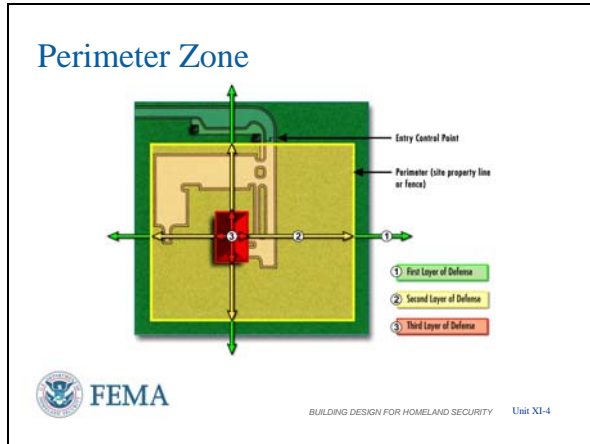- General ESS Description
- ESS Design Considerations

Fundamental objective:
  Provide appropriate, effective, and economical protective design for assets.

Approach:
  Coordinated effort between security, law enforcement, and engineering communities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-4

Perimeter Zone

The protection of a facility is designed with layers of defense, detection, and response. Before we discuss security systems, we need to review several basic concepts:

- A protected area's perimeter is usually defined by an enclosing wall or fence, or a natural barrier, such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined.

Perimeter Zone and Layers of Defense

- First layer of defense is from the perimeter outward (either fenceline or owned property).
- Second layer of defense is between the perimeter and the building.
- Third layer of defense is the building envelope.
- A fourth layer of defense may be a room inside the building.

VISUAL XI-5
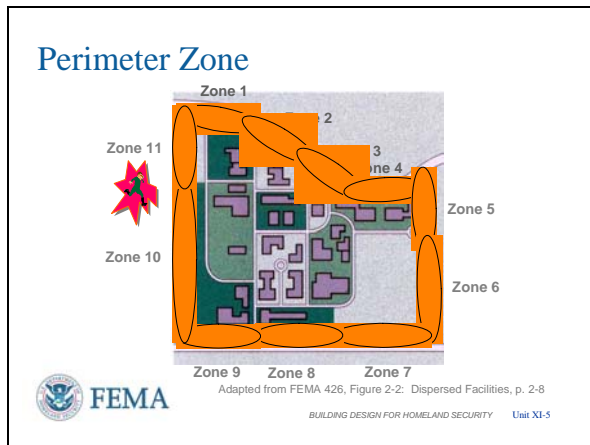
Perimeter Layout and Zoning Sensors

- After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter.
- The exterior and interior Intrusion and Detection Systems should be configured as layers of unbroken rings concentrically surrounding the asset. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on

INSTRUCTOR NOTES	CONTENT/ACTIVITY

a defensive layer, in the area between two defensive layers, or on the asset itself, depending on the delay required.

- If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter.

VISUAL XI-6

This slide shows old generation and new generation CCTV cameras and motion detectors.

Intrusion Detection Systems

There are a number of different sensor technologies:

- Boundary Penetration Sensors
- Volumetric Motion Sensors
- Exterior Intrusion Detection Sensors
- Fence Sensors
- Buried Line Sensors
- Microwave Sensors
- Infrared Sensors
- Video Motion Sensors

VISUAL XI-7

Boundary Penetration Sensors

- Structural Vibration Sensors
- Glass Breaking Sensors
- Balanced Magnetic Switches
- Passive Ultrasonic Sensors
- Grid Wire Sensors

Structural vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, (subterranean digging) or employing other forcible methods of entry.

Glass breaking sensors detect the breaking

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. (This type of sensor should not be used without another sensor type). **Balanced magnetic switches** (BMSs) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry. **Passive ultrasonic sensors** detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors), and windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds. **Grid wire sensors** consist of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers. (This type sensor can be used well with structural vibration sensors).

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-8

Volumetric Motion Sensors

Designed to detect intruder motion within the interior of the protected volume
- Microwave Motion Sensors
- Passive Infrared (PIR) Motion Sensors
- Dual Technology Sensors
- Video Motion Sensors
- Point Sensors
- Capacitance Sensors
- Pressure Mats
- Pressure Switches

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-8

Volumetric Motion Sensors

Designed to detect intruder motion within the interior of the protected volume:
- Microwave Motion Sensors
- Passive Infrared (PIR) Motion Sensors
- Dual Technology Sensors
- Video Motion Sensors
- Point Sensors
- Capacitance Sensors
- Pressure Mats
- Pressure Switches

Microwave motion sensors use high-frequency electromagnetic energy to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.

Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver).

Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.

Passive infrared (PIR) motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.

Dual technology sensors combine two different technologies in one unit to minimize the generation of alarms caused by sources

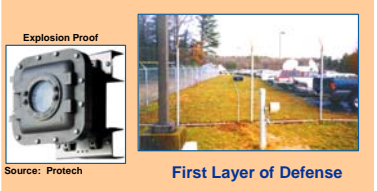| INSTRUCTOR NOTES	CONTENT/ACTIVITY
	other than intruders. • Stereo Doppler is a dual channel microwave design. The combination of a Microwave (MW) Sensor and a Passive Infrared Sensor (PIR) must activate simultaneously to create an alarm. **Video motion sensors** generate an alarm when an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors, analog and digital. Analog detectors generate an alarm in response to changes in a picture's contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. **Point sensors** are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches. **Capacitance sensors** detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground. Think of some types of car alarms. **Pressure mats** generate an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Pressure switches are mechanically activated contact switches or single ribbon switches.

VISUAL XI-9

Exterior Intrusion Detection Sensors

- Strain Sensitive Cable - fences and gates
- Fiber Optic Cable - fences, gates, and gravel pathways
- Bistatic/Monostatic Microwave - line of sight, clear zones
- Active Infrared - portals, short perimeter gap filters
- Ported Coax - exterior clear zones
- Dual Technology (PIR/MW) - portals and gap fillers
- Video Motion - volumetric traffic, open areas

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the POD (Probability of Detection) for buildings and other facilities.

Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (e.g., heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, blowing debris, and animals are major sources of unwanted alarms.

The combination of MW (**M**icro**w**ave) and PIR (**P**assive **I**nfra**r**ed) works well to eliminate weather, birds/animals, vegetation, blowing debris, hail etc from causing false

INSTRUCTOR NOTES	CONTENT/ACTIVITY

alarms.

VISUAL XI-10
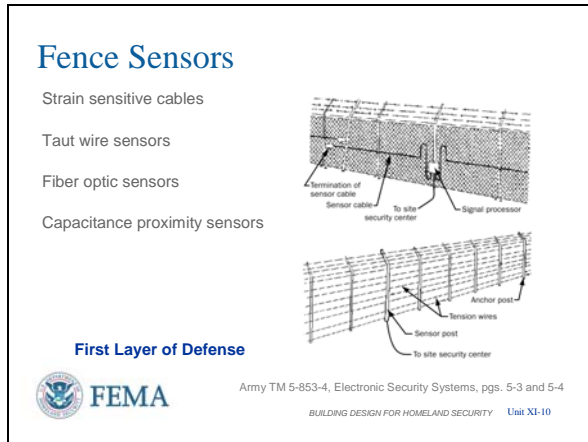
Fence Sensors

- Strain sensitive cables
- Taut wire sensors
- Fiber optic sensors
- Capacitance proximity sensors

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain.

Strain sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion.

Taut wire sensors combine a physically taut-wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end.

Fiber optic sensors are functionally equivalent to the strain-sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to determine whether an alarm should be initiated.

Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm.

| INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-11
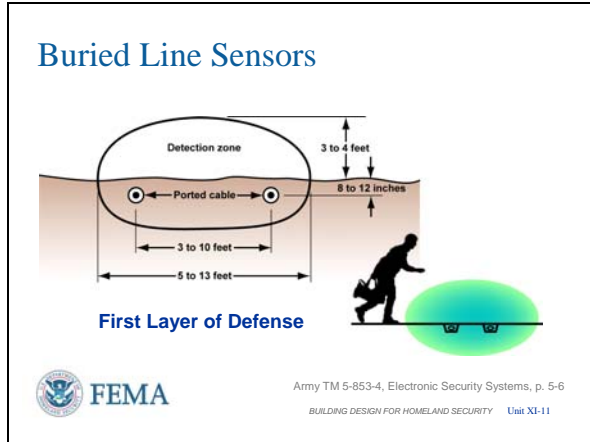
Buried Line Sensors

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field.

Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles.

VISUAL XI-12
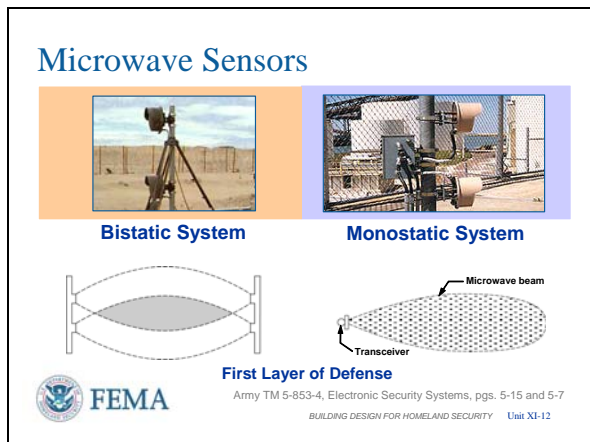
Microwave (MW) Sensors

- Bistatic system
- Monostatic

Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.

A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct line of sight of each other.

Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays

INSTRUCTOR NOTES	CONTENT/ACTIVITY

for the transmitter and receiver, which are usually combined into a single package.

VISUAL XI-13

Infrared (IR) Sensors

The IR sensors are available in both active and passive models. An <u>active sensor</u> generates one or more near-IR beams that generate an alarm when interrupted. A <u>passive sensor</u> detects changes in thermal IR radiation from objects located within its field of view.

<u>Active sensors</u> consist of transmitter/receiver pairs. The transmitter contains an IR light source (such as a gallium arsenide light-emitting diode [LED]) that generates an IR beam. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

VISUAL XI-14

This slide shows old generation and new generation video motion sensors.
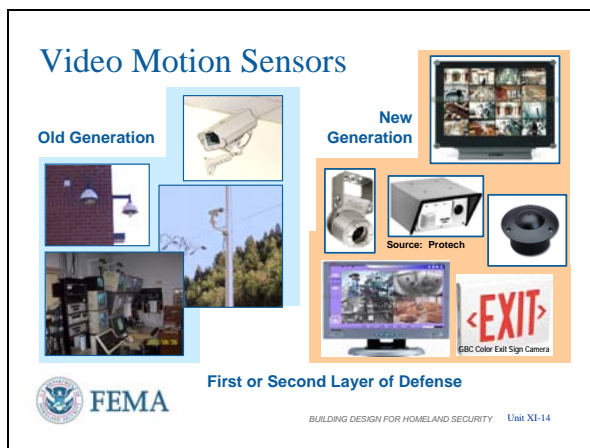
Video Motion Sensors

Video motion sensors are available on most digital video recorders used in security applications.
- They can be programmed to activate alarms, initiate recording, or any other designated action when motion is detected by a security camera.
- Some digital video recorders can be programmed to monitor very specific fields of view for specific rates of motion in order to increase effectiveness and minimize extraneous detections.
- Video motion sensors can also greatly <u>improve the efficiency of security personnel</u> monitoring security cameras by alerting them when motion is detected.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-15

Electronic Entry Control

Coded Devices

Credential Devices

Biometric Devices

FEMA

First or Second Layer of Defense

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-15

Entry Control Systems and Technology

- Coded Devices
- Credential Devices
- Biometric Devices

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals. These means of entry control can be applied manually by guards or automatically by using entry control devices.

- In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry.
- In an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

All entry control systems control passage by using one or more of three basic techniques (e.g., something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these techniques are grouped into three categories: coded, credential, and biometric devices.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-16

Coded Devices

- Electronic Keypad Devices
- Computer Controlled Keypad Devices

Coded devices operate on the principle that a person has been issued a code to enter into an entry control device. This code will match the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Electronically coded devices include electronic and computer controlled keypads.

Electronic keypad devices are similar to telephone keypads (12 keys). This type of keypad consists of simple push-button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

Computer controlled keypad devices are devices similar to electronic keypad devices, except they are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the keys are depressed and may provide additional functions, such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

PRECAUTIONS:
- Care should be taken so other persons cannot observe individuals entering

INSTRUCTOR NOTES	CONTENT/ACTIVITY
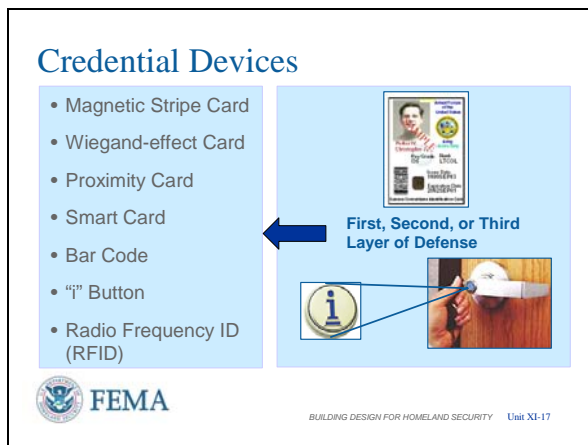
their assigned code. Installation of an opaque shield around the device aids in control of unauthorized observations. This helps to eliminate the use of another's code to gain entry into an unauthorized area.

- Also, care should be taken to replace coded pads that show wear from repeated code entries. Code compromise may be accomplished by attempting use of the worn keys (which results in less permutations of the combination to gain access).

- Individual codes are best for access control and accountability.

VISUAL XI-17

Credential Devices

Credential Devices

- Magnetic Stripe Card
- Wiegand-effect Card
- Proximity Card
- Smart Card
- Bar Code
- "i" Button
- Radio Frequency ID (RFID)

First, Second, or Third Layer of Defense

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-17

Credential Devices

- Magnetic Stripe Card
- Wiegand-effect Card
- Proximity Card
- Smart Card
- Bar Code
- Button
- Radio Frequency Identification Device

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (e.g., plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read.

A **magnetic stripe card** is a strip of magnetic material located along one edge of the card that is encoded with data (sometimes encrypted). The data are read by moving the card past a magnetic read head.

A **Wiegand-effect card** contains a series of small-diameter, parallel wires approximately

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	½-inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power. A **proximity card** is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an integrated circuit embedded in the card to generate a code that can be magnetically or electrostatically coupled to the reader. A **smart card** is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information and other data may be stored in the microprocessor's memory. A **bar code** consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be easily duplicated.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	The **"i" button** is a computer chip enclosed inside a 16mm stainless steel can. The "i" button can grant its owner access to a building, a PC, a piece of equipment, or a vehicle. Some "i" buttons can be used to store cash for small transactions, such as transit systems, parking meters, and vending machines. Also used as an electronic asset tag to store information needed to keep track of valuable capital equipment.
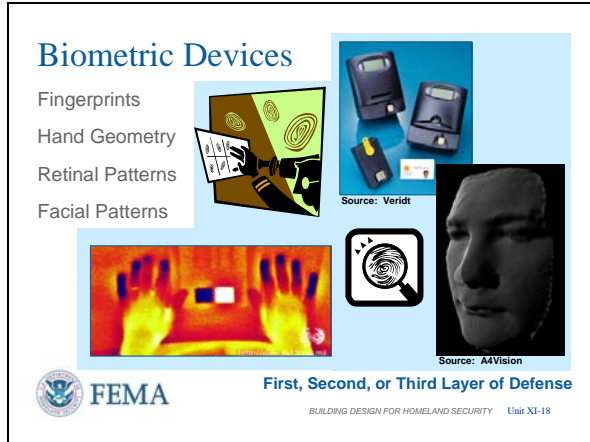|
	The Radio Frequency Identification Device (RFID) Systems rely on a radio frequency identification chip implanted in an access card, i.e., Proximity, Smart, or similar which transmits card owner information wirelessly.
	Although this is leading edge technology, significant security and privacy issues exist to a level that government agencies eager to use this technology have abandoned their acceptance and use until the security and privacy issues are resolved. The ability for the remote operation of this technology gives it great interest for now and the future.
	Without a biometric device necessary to be used with a credential device the only thing to be verified from an after incident entry point log review is "the device" was used to enter the area. Without some other means of identification (biometrics or Personal Identification Number), a person other than the owner can use a lost or stolen card, and cannot be tied to the card.
	In the absence of biometric devices, anti-pass back devices, and procedures should be in place to eliminate unauthorized usage. Assign responsibility of the person issued the device for ensuring two people cannot use the same credential device. This is commonly occurs when one tells another they "forgot" their device.

Course Title: Building Design for Homeland Security

Unit XI: Electronic Security Systems

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-18

Biometric Devices

- Fingerprints
- Hand Geometry
- Retinal Patterns
- Facial Recognition

The third basic technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted.

Fingerprint verification devices use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

Hand geometry devices use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width,

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	webbing between fingers, and light transmissivity through the skin to verify identity. Both two- and three-dimensional units are available. **Retinal pattern** is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity IR light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood-vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature. **Facial Recognition** is a facial identification/verification reader system with touch screen PIN (Personal Identification Number) and 3D facial biometric access. An audio request for a PIN entry references the 3D face template stored in the database with the corresponding PIN. Verification is made from the correct PIN entry matching the reader image. Night, changing light conditions, and motion will not change the high rate of accuracy according to the manufacturer.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-19

Closed Circuit Television Systems

- Interior CCTV - alarm assessment, card reader door assessment, emergency exit door assessment, and surveillance of lobbies, corridors, and open areas
- Exterior CCTV - alarm assessment, individual zones and portal assessment, specific paths and areas, exclusion areas, and surveillance of waterside activities
- Transmission media includes twisted pair telephone cable, coaxial TV cable, LAN (Local Area Network) cable, fiber optics, and wireless. Each has cost, line length, resolution, reliability, and quality considerations. Security, encryption, and redundancy are also concerns throughout the length of run from sensor to monitor/alarm.
- Only color should be installed. There is very little use of black and white television when attempting to assemble a description of an individual who is wearing clothing in the shades of gray to white. Were they wearing blue jeans, or black or green trousers?

VISUAL XI-20

Security Operations Center

The operator monitoring the alarms and displays of a Security Operations Center is probably the most ineffective sensor in the system.

- The workspace should be conducive to maintaining attention, not like the two smaller photos where the monitors are outside the normal line of sight and in glare.
- The workspace should have some hardening as it is a single point of vulnerability in the system where response is initiated.
- Visual and/or audio alerts need to draw the

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	operators attention to alarms and focus the operator on the specific monitor with the detection information requiring real-time assessment for action.
	• <u>CCTV</u> can assist in these alerts using image-based motion detection or SMART CCTV where attention is drawn to the camera that pan/tilts/zooms to the location from which the alarm is coming, such as the door where a balanced magnetic switch loses continuity or a motion detector senses motion where none is expected.
	• Forwarding of alarms to cell phones, pagers, personal digital assistants, or radios keeps the staff on notice that a problem exists. It also allows the operator to take a bathroom break without having to have another person stand-in at the monitors.
	• Digital Video Recorders (DVR) store more information with better quality resolution for not only detection, but also assessment and future potential criminal proceedings.
	• Like fire alarm systems, all physical lines carrying alarm information should be supervised to identify any tampering with a line and to ensure functionality. Backup feeds or alternate feeds following different routes also increase reliability, especially in computer-based IP (Internet Protocol) systems.
	• Since electric power is needed for system operation throughout the system, backup power with redundant lines should also be considered.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-21

Summary

Use the Building Vulnerability Assessment Checklist to identify electronic security system requirements.

Public safety is enhanced by electronic security systems (deter, detect, deny, devalue).

Electronic security systems components and capabilities interact with other systems (LAN, doors, windows, lighting, etc.).

Electronic security systems can be used to mitigate vulnerabilities.

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-21

Summary

Remember all the different components of the system must support each others' function. For example, the best barriers are those tied to a detection system, like a strain sensitive cable alarm sensor on a chain link fence, with a steel cable woven into the fence, delay function, and overseen by an assessment method, such as a CCTV system.

The best practice is to evaluate products against operational and desired results criteria. This has proven to be a problem during attempted evaluations conducted by agencies trying to compare two different systems. System operating protocols were different from each other and, as a result, could not produce compatible/comparable results.

NOTE: All system control boxes should be equipped with an intrusion detection alarm which annunciates at the box and at the system control console, and is tied electronically to the events report log to be acknowledged, investigated (response) and cleared on the log. A link to CCTV recorded events is also advisable for immediate visual response/review.

- Use the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** to identify electronic security system requirements.
- Public safety is enhanced by electronic security systems (deter, detect, deny, devalue).
- Electronic security systems components and capabilities interact with other systems (LAN, doors, windows, lighting, etc.).
- Electronic security systems can be used to mitigate vulnerabilities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-22

Unit XI Case Study Activity

Electronic Security Systems

Background

Emphasis: Various components and technology available for use in electronic security systems

FEMA 426, Building Vulnerability Assessment Checklist

Assess Electronic Security Systems in Case Study for vulnerabilities and recommended mitigation measures

Risk Management Series:
Reference Manual
to Mitigate Potential Terrorist Attacks Against Buildings
December 2003

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY   Unit XI-22

Refer participants to **FEMA 426**, Vulnerability Checklist Section 12 and Tab XI-A or XI-B in the Student Manual for the selected Case Study activity.

At the end of 10 minutes, reconvene the class and facilitate group reporting. The plenary session should take 5 minutes.

Student Activity

In this unit, the emphasis was upon the various components and technology available for use in electronic security systems.

The **Building Vulnerability Assessment Checklist in FEMA 426 (Table 1-22, pages 1-81 to 1-89)** can be used as a screening tool for preliminary building design vulnerability assessment and assessment of existing buildings.

Activity Requirements

- Working in small groups, refer to the selected Case Study to determine answers to the worksheet questions.
- Then review results to identify vulnerabilities and possible mitigation measures.

Take 10 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

In the next unit, you will finalize and present the Case Study Results determined by your team. This will include preparation and presentation of the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk, although other vulnerabilities and recommended mitigation measures may also be presented. Prioritize the top three risks and the top three recommended mitigation measures with rationale and justification. Include any consideration for changes to security systems per this instruction unit.

UNIT XI-A CASE STUDY ACTIVITY:
ELECTRONIC SECURITY SYSTEMS
(Suburban Version)

In this unit, the emphasis will be upon the various components and technology available for use in electronic security systems. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment or for assessment of an existing building and site.

Requirements

Refer to the Appendix A Case Study to determine answers to the following questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** that address security systems.

2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit V-A Student Activity and, based on this detailed analysis, decide if any rating needs adjustment.

3. Select mitigation measures among security system design and operation features to reduce vulnerability and associated risk.

4. Estimate the new risk ratings for high risk asset-threat pairs of interest based on the recommended mitigation measures and complete the table.

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
	Perimeter Systems		
12.1	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What is the number of fixed, wireless and pan-tilt-zoom cameras used?	Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective	*The parking lot behind the HIC building is well lit and monitored by older generation analog CCTV cameras using telephone wires that are connected to video displays in the HIC Security Officer's office and recorded on standard VHS tape.* *The CCTV cameras are commercial*

Section	Vulnerability Question	Guidance	Observations
	Who are the manufacturers of the CCTV cameras?

What is the age of the CCTV cameras in use? | and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design.

Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras.

Reference: *GSA PBS P-100* | *grade black and white with a 180-degree field of view that the security officer can control via the display panel.*

The front parking lot is lit, but not monitored. |
| 12.2 | Are the cameras programmed to respond automatically to perimeter building alarm events?

Do they have built-in video motion capabilities? | The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals.

Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities* | Unknown without a more detailed assessment. |
12.5	Are intercom call boxes used in parking areas or along the building perimeter?	See Item 12.4.	No.
12.6	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Telephone wire.
12.7	Who monitors the CCTV system?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	The HIC security officer.

Security System Mitigation Measures
(Suburban Version)

Asset-Threat/Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
1. Site / Vehicle Bomb	High	Upgrade CCTVs to digital and use DVRs. Install CCTVs to monitor front parking and expand back parking coverage.	Medium
2. Architectural / Vehicle Bomb	High	Upgrade CCTVs to digital and use DVRs. Install CCTVs to monitor interior lobby and loading dock.	Medium
3. Mechanical Systems / Chemical (CBR Attack)	High	Evaluate installation of basic chemical sensors on outside air intake of HVAC system or acquisition of portable sensors for use by Building Security. (Intrusion Detection equivalent)	Medium
4. Mechanical Systems / Biological (CBR Attack)	High	Evaluate acquisition of portable or basic level biological sensors for use by Building Security. (Intrusion Detection equivalent)	High to Medium
5. Mechanical Systems / Radiological (CBR Attack	High	Evaluate acquisition of portable or basic level radiological sensors for use by Building Security. (Intrusion Detection equivalent)	High to Medium

UNIT XI-B CASE STUDY ACTIVITY:
ELECTRONIC SECURITY SYSTEMS
(Urban Version)

In this unit, the emphasis will be upon the various components and technology available for use in electronic security systems. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment or for assessment of an existing building and site.

Requirements

Refer to the Appendix B Case Study to determine answers to the following questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-81 to 1-89 of FEMA 426)** which address security systems.

2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit V-B Student Activity and, based on this detailed analysis, decide if any ratings need adjustment.

3. Select mitigation measures among security system design and operation features to reduce vulnerability and associated risk.

4. Estimate the new risk ratings for high risk asset-threat pairs of interest based on the recommended mitigation measures and complete the table.

Section	Vulnerability Question	Guidance	Observations
12	**Security Systems**		
	Perimeter Systems		
12.1	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What is the number of fixed, wireless and pan-tilt-zoom cameras used?	Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective	*There is a mixture of black/white and color CCTV used. All entries to the building, especially the Loading Dock, are covered by color CCTV systems. The cameras are color, pan, tilt, and zoom. Elevator lobbies on underground parking levels both under the building and under the plaza are also on color cameras with pan, tilt, and zoom.*

Section	Vulnerability Question	Guidance	Observations
	Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design. Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Reference: *GSA PBS P-100*	*Underground parking has fixed black and white CCTV cameras except at the vehicle entrances and exits where the cameras are color, pan, tilt, and zoom to aid in identifying people who do not pay or cause damage to the drop arms or automated equipment. There are black and white cameras covering stairwell doors on underground parking levels.* *One person in Building Security Office monitors cameras and alarms on a 24/7 basis. DVR (Digital Video Recording) is used to record all perimeter color cameras.* *Requires further investigation to determine analog or digital design of cameras, only know that DVR for recording is digital.* *There are 14 fixed B/W cameras, no wireless cameras were identified during assessment, and 24 color cameras with pan-tilt-zoom.* *The manufacturers and age of the CCTV cameras require further investigation.*

Section	Vulnerability Question	Guidance	Observations
12.2	Are the cameras programmed to respond automatically to perimeter building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	No perimeter cameras are programmed to respond to perimeter building alarms. However, the access keypads on the two building elevators and the two building stairwells serving the UG parking levels have Duress PINs. These alarms can be easily set to draw attention to the specific camera covering the area. See Question 12.13 for capability configured on Interior Systems. There is no video motion capability installed.
12.4	Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other high risk locations by assessment. Reference: *GSA PBS P-100*	There are no panic/duress alarms or call buttons available to the general public in the parking areas. However, there are Duress PINs that work on perimeter access keypads in the building UG parking – elevators and stairwells. These are only available to tenants and staff.
12.5	Are intercom call boxes used in parking areas or along the building perimeter?	See Item 12.4.	No intercom call boxes were identified during the assessment, either in parking areas or along the building perimeter. See Question 12.4

Section	Vulnerability Question	Guidance	Observations
12.7	Who monitors the CCTV system?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	One Building Security person per shift monitors cameras and alarms in Building Security Office (Security Operations Center / Fire Control Center) located in the Administration area on the first floor and providing 24/7 coverage.
12.8	What is the quality of video images both during the day and hours of darkness? Are infrared camera illuminators used?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Lighting is coordinated with CCTV requirements to ensure good quality pictures, both on the monitors and on recordings, especially where color cameras are installed. There are no infrared camera illuminators installed.
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	The access control systems, CCTV systems, and physical security alarms are on building emergency power.
	Interior Systems		
12.12	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What is the number of fixed, wireless and pan-tilt-zoom	Security technology is frequently considered to compliment or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed are an integral component of the overall security program. Their design, engineering, installation, operation, and management must	There is a mixture of black/white and color CCTV used. The Lobby on the first floor and the elevator lobbies on all floors are on color CCTV systems and cameras are color, pan, tilt, and zoom. Administration, electrical, and utilities, along with the utility risers have fixed Black and

Section	Vulnerability Question	Guidance	Observations
	cameras used? Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	be able to meet daily security challenges from a cost effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design. Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Reference: *GSA PBS P-100* See Item 12.1. --Reference: *Physical Security Assessment for Department of Veterans Affairs Facilities*	White CCTV (Closed Circuit Television) coverage. One person in Building Security Office monitors cameras and alarms on a 24/7 basis. The Lobby on the first floor and the elevator lobbies on all floors are on color CCTV systems and these are also on recorded using DVR (Digital Video Recording. Requires further investigation to determine analog or digital design of cameras, only know that DVR for recording is digital. There are about 250 fixed B/W cameras, no wireless cameras were identified during assessment, and about 200 color cameras with pan-tilt-zoom. The manufacturers and age of the CCTV cameras would have to be further investigated.
12.13	Are the cameras programmed to respond automatically to perimeter building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Reference: *Physical Security Assessment for Department of*	When an Administration, electrical, and utilities, or utility riser door is opened, the CCTV monitor that includes coverage of that door alerts Building Security in conjunction with the door alarms to assist

Section	Vulnerability Question	Guidance	Observations
		Veterans Affairs Facilities	in identifying the activity. This is also used proactively in that anyone opening a controlled space contacts the Building Security Office prior to opening the controlled space and the person monitoring the CCTVs verifies the person before the space is opened. No video motion capability in installed.
12.24	Are panic/duress alarm buttons or sensors used? Where are they located? Are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other areas high risk locations by assessment. Reference: *GSA PBS P-100*	Designated elevators, including one service elevator, have card readers and PIN (Personal Identification Number) keypads for movement to and from access controlled floors. To get the elevator to move to a specific floor you have to press the floor key, read your card, and enter your PIN. In addition, there is a Duress PIN that alerts building and floor security that an authorized person is moving to a controlled floor with a security problem. The building stairwells extending into the underground parking have card readers and PIN keypads at each level of underground parking to gain entrance to the

Section	Vulnerability Question	Guidance	Observations
			stairwells. A Duress PIN also works at these stairwells.

Security System Mitigation Measures
(Urban Version)

Asset-Threat/Hazard Pair	Current Risk Rating	Suggested Mitigation Measures	Revised Risk Rating
1. Site / Vehicle Bomb		Improve CCTV throughout UG parking – convert B/W to color, expand coverage beyond elevators and stair access. Add coverage of complete perimeter.	
2. Architectural / Vehicle Bomb		Add CCTV (color digital, pan-tilt-zoon) to both building stairwells and both plaza UG parking stairwells.	
3. Architectural / Armed Attack		Access Control – Redesign Lobby to channel pedestrians for screening, add manned armed guards (GSA requirement) to man screening equipment.

Convert retail space on first floor to outside access only, but alarm secondary emergency exits (3 existing) into Lobby. May be overcome by Lobby Redesign. | |

Asset-Threat/Hazard Pair	Current Risk Rating	Suggested Mitigation Measures	Revised Risk Rating
4. Mechanical Systems / Chemical (CBR Attack)		Evaluate installation of basic chemical sensors on outside air intake of HVAC system or acquisition of portable sensors for use by Building Security. (Intrusion Detection equivalent)	
5. Mechanical Systems / Biological (CBR Attack)		Evaluate acquisition of portable or basic level biological sensors for use by Building Security. (Intrusion Detection equivalent)	
6. Mechanical Systems / Radiological (CBR Attack)		Evaluate acquisition of portable or basic level radiological sensors for use by Building Security. (Intrusion Detection equivalent)	