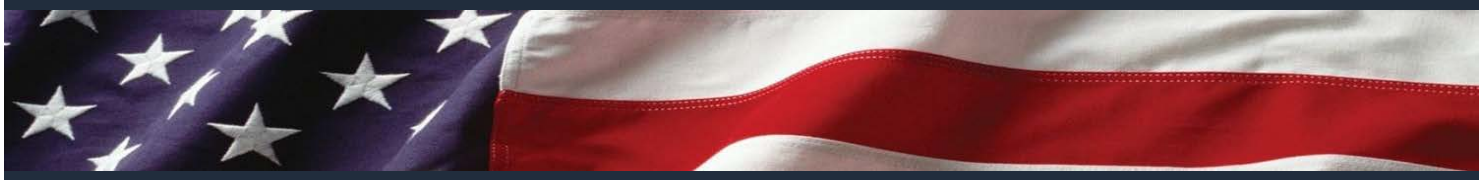


Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Participant Workbook

This page is intentionally left blank.

Table of Contents

Syllabus S-1

Module 1: Course Introduction and Overview 1-1

Module 2: Overview of Hostile Operations 2-1

Module 3: Vulnerability Assessment 3-1

Experiential Learning Activity 1: Vulnerability Assessment Activity ELA1-1

Module 4: Hostile Surveillance Requirements 4-1

Module 5: Surveillance Detection Requirements and Fundamentals 5-1

Experiential Learning Activity 2: Detection Fundamentals Activity ELA2-1

Module 6: Reporting and Response 6-1

Module 7: Compromise and Deployment 7-1

Experiential Learning Activity 3: Capstone Activity ELA3-1

This page is intentionally left blank.

Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Syllabus

This page is intentionally left blank.

SECTION I
COURSE DESCRIPTION

Course Number: PER-346

Course Title: Surveillance Detection for Bombing Prevention

Version Control Number: 2.0

Effective Date: January 2018

Course Purpose. The purpose of this course is to provide public safety and security professionals fundamental knowledge and skills to recognize hostile surveillance at facilities and planned and unplanned events and respond appropriately.

Course Goal. The goal of this course is to provide fundamental knowledge and skills necessary to establish a detection capability to identify and mitigate a threat from hostile surveillance activity for bombing prevention.

Course Scope. This course provides public safety and security professionals with the knowledge and skills to employ the fundamentals of surveillance detection for bombing prevention related to a facility/system or a planned or unplanned event and to recognize hostile surveillance activity. The course includes an overview of surveillance, the terrorist attack cycle, and each of the five elements of the surveillance detection plan. It concludes with a capstone activity.

Terminal Learning Objectives

a. Given a written examination, participants will describe the role of surveillance in the terrorist attack cycle. (TAC-0130)

b. Given a written examination, participants will describe the key considerations included in the vulnerability assessment as it applies to surveillance detection according to the criteria discussed in class. (RMP-0110)

c. Given an assigned facility, participants will identify the vulnerabilities of that facility in accordance with the key considerations provided in class. (SD-0210)

d. Given a written examination, participants will describe the three major requirements for hostile surveillance of a facility according to the guidelines provided in class. (SD-0110)

e. Given a written examination, participants will describe the fundamentals of surveillance detection for bombing prevention according to the guidelines provided in class. (SD-0120)

f. Given an assigned facility, participants will identify the locations of hostile surveillance positions and surveillance detection points based on the vulnerabilities identified in Experiential Learning Activity 1: Vulnerability Assessment. (SD-0220)

g. Given a written examination, participants will describe what is included in the reporting and response elements of the surveillance detection plan. (SD-0130)

h. Given a written examination, participants will explain the aspects that must be considered to maintain operational security. (SD-0140)

Course Length: 3 days

Course Academic Hours: 19 hours, 20 minutes

Class Size

a. **Minimum:** 15

b. **Optimal:** 20

c. **Maximum:** 25

Class Iterations per Year: 20

Optimum Annual Participant Throughput: 400

Course Delivery Means

a. **Resident:** Not applicable

b. **Non-resident.** At the request of a jurisdiction, this course may be delivered non-resident by Office for Bombing Prevention (OBP) instructional Mobile Training Team (MTT) staff.

c. **Indirect.** This course may be delivered indirectly by Federal, state, local, tribal, and territorial (FSLTT) trainers certified through the OBP Train-the-Trainer (TtT) program.

Target Audience. The target audience consists of public safety and security professionals (local, state, and federal level) tasked with surveillance detection responsibilities plus their management.

Recommended Course Prerequisites

a. IS-100.b, *Introduction to the Incident Command System* or any of the other ICS-100 series courses

b. IS-200.b, *Incident Command System for Single Resources and Initial Action Incidents* or any of the other ICS-200 series courses

c. IS-914: *Surveillance Awareness: What You Can Do*

Job/Function Tasks Trained

Task Number	Tasks Title	Proficiency Level[1]
TAC-0130	Match terrorist operational tactics to the terrorist attack cycle step in which they occur	Familiarization
RMP-0110	Apply the DHS risk management process as it applies to surveillance detection	Part Task

SD-0210	Conduct a modified vulnerability assessment	Part Task
SD-0110	Identify the requirements for hostile surveillance	Familiarization
SD-0120	Describe the fundamentals of surveillance detection	Familiarization
SD-0220	Identify hostile surveillance and surveillance detection positions	Part Task
SD-0130	Identify the components of the reporting and response elements of the surveillance detection plan	Familiarization
SD-0140	Identify the aspects to maintaining operational security	Familiarization
SD-0230	Detect and report hostile surveillance	Part Task

[1]*Proficiency Levels = Familiarization, Part Task, Proficiency, or Reinforced*

Testing/Certification. Participants are administered a post-test to assess their level of learning. Participants who perform successfully (70% correct or above) on the post-test and achieve a "Go" rating on the performance assessment(s) are recognized with a training certificate. Participants who do not perform successfully on the post-test are issued a letter of attendance.

Continuing Education Units or Academic Equivalency. As an International Association of Continuing Education and Training (IACET) authorized provider, the CDP awards 2.0 continuing education units for this course under the American National Standards Institute (ANSI)/IAET standards.

Instructor Qualifications. Exceptions to these instructor qualifications may be granted on a case-by-case basis at the discretion of OBP Operations. A request for exception will be made through the appropriate Government contracting officer's representative (COR).

a. **Job Experience:** Participation in planning and/or conducting the security of a facility or planned or unplanned event, especially as it pertains to surveillance detection for bombing prevention.

b. **Instructor/Facilitator Experience.** All instructors delivering this course on behalf of the CDP must meet the basic instructor qualifications outlined in the performance work statement. All instructors delivering this course on behalf of the DHS OBP must meet OBP's organizational requirements for instructor qualification outlined in the Training Quality Assurance Guide.

Regulations, National Goals, Doctrine, Standards, and Capability Gaps Supported by the Course

a. **Regulations.** Response regulations will be determined by the local agency.

b. **National Goals.** This course reinforces the National Preparedness Goal by providing training to public safety and security professionals, supporting the prevention of terrorism or extremism, and identifying and mitigating the threat of hostile surveillance. This course supports the following core capabilities.

(1) Prevent Capabilities

(a) Vulnerability Assessment. Participants practice conducting a hasty vulnerability assessment on an assigned facility.

(b) Surveillance Detection. Participants determine the Red Zone and identify hostile surveillance positions and surveillance detection positions on an assigned facility.

(c) Surveillance Detection Plan. Participants practice developing and applying the first three components of a surveillance detection plan.

c. Doctrine: DHS Risk Management, PPD 17, and PPD 8

d. Standards: DHS Risk Management Process

e. Capability Gaps. The development of this course is in response to a gap in training that responds to surveillance detection, focusing on bombing prevention that supports national level policy and counteracts criminal and terrorist tactics, techniques, and procedures (TTPs). The greatest opportunity to prevent a bombing incident from occurring is during the criminal or terrorist's surveillance of the target. This course compliments other OBP counter improvised explosive device (C-IED) training by focusing on how to stop an incident before it occurs with a surveillance detection plan for bombing prevention.

Version Control Number Change History

Version Control Number	New, Minor or Major	Concise Description of Change(s)	Effective Date of Change
1.0	New	This is the creation of the course based on a needs assessment.	Unknown
2.0	Major	This is revision of an existing course based upon a needs assessment; review of course delivery feedback, and the need to place the course materials into the CDP-approved template.	August 2017

Additional Comments/Remarks: None

SECTION II
COURSE SUMMARY AND RECOMMENDED SCHEDULE

Course Executive Summary. The following is a concise overview for each learning activity within the program. Each activity is presented in the sequence in which it is recommended to be executed.

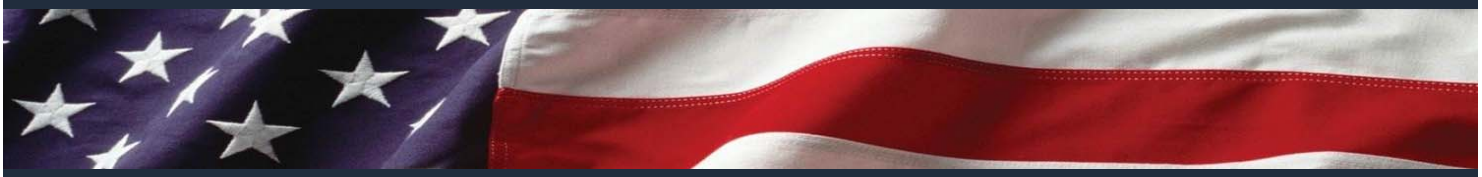
Activity Number	Activity Title	Activity Description	Total Time
Mod 1	Course Introduction and Overview	The purpose of this module is to provide an overview of the course, orient participants to the facilities, and introduce instructors and participants.	30 minutes
Mod 2	Overview of Hostile Operations	The purpose of this module is to provide an overview of hostile operations and the role of surveillance in the terrorist attack cycle.	1 hour, 30 minutes
Mod 3	Vulnerability Assessment	The purpose of this module is to provide participants with the steps involved in a vulnerability assessment (VA) based as it applies to surveillance detection.	1 hour
ELA 1	Vulnerability Assessment Activity	The purpose of this module is to provide participants the opportunity to conduct a vulnerability assessment as it applies to surveillance detection on an assigned venue.	4 hours
Mod 4	Hostile Surveillance Requirements	The purpose of this module is to introduce participants to the requirements for surveillance including the Red Zone and hostile surveillance positions.	45 minutes
Mod 5	Surveillance Detection Requirements and Fundamentals	The purpose of this module is to provide participants with an overview of methods for detecting hostile surveillance, including identifying surveillance detection positions and correlation of behavioral indicators.	1 hour, 45 minutes
ELA 2	Detection Fundamentals Activity	The purpose of this module is to provide participants an opportunity to identify hostile surveillance positions based on determining the Red Zone of a given facility, surveillance detection positions based on identified hostile surveillance positions, and determine profile versus signature of two observed individuals.	4 hours
Mod 6	Reporting and Response	The purpose of this module is to provide an overview of the final two elements of the surveillance detection plan. This module has an activity that allows the participants to practice their description skills.	1 hour

Activity Number	Activity Title	Activity Description	Total Time
Mod 7	Compromise and Deployment	The purpose of this module is to provide an overview of the operational security considerations and responses to various types of compromise faced during surveillance detection.	30 minutes
Exam 1	Course Exam	The purpose of this examination is to measure the participants' comprehension of the cognitive material presented during the course.	20 minutes
ELA 3	Capstone Activity	The purpose of this module is to allow participants to apply and receive feedback on the knowledge and skills presented in the course to an activity with role players conducting hostile surveillance on an assigned facility.	4 hours
Admin 1	Graduation and End-of-Course Evaluation	The purpose of this learning activity is to recognize participant achievement in completing the course and to collect participant end-of-course evaluation forms.	15 minutes

Recommended Course Schedule. This schedule illustrates the recommended sequencing by day for the administrative and academic learning activities. Every attempt will be made to maintain this sequencing of the academic learning activities to ensure maximum transfer of learning is achieved.

Activity Number	Activity Title	Hours
Module 1	Course Introduction and Overview	30 minutes
Module 2	Overview of Hostile Operations	1 hour, 30 minutes
Module 3	Vulnerability Assessment	1 hour
ELA 1	Vulnerability Assessment Activity	4 hours
	Day Two	
Module 4	Hostile Surveillance Requirements	45 minutes
Module 5	Surveillance Detection Requirements and Fundamentals	1 hour, 45 minutes
ELA 2	Detection Fundamentals Activity	4 hours
	Day Three	
Module 6	Reporting and Response	1 hour
Module 7	Compromise and Deployment	30 minutes
Exam 1	Course Exam	20 minutes
ELA 3	Capstone Activity	4 hours
Admin 1	Graduation and End-of-Course Evaluation	15 minutes
	Total Academic Time (excludes Admin time)	19 hours, 20 minutes
	Total Contact Hours	19 hours, 35 minutes

This page is intentionally left blank.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 1:
Course Introduction and Overview
Participant Workbook

This page is intentionally left blank.

Module 1
Supplemental Materials

This page is intentionally left blank.

Surveillance Detection for Bombing Prevention Course (PER-346)

Developed by the Office for Bombing Prevention, the Surveillance Detection for Bombing Prevention Course is designed to provide participants with fundamental knowledge and skills to recognize and respond to hostile surveillance at facilities and during events.

(Source: DHS)

Participant Requirements

This course is designed for public safety and security professionals (local, State, and Federal level) who are tasked with surveillance detection responsibilities and their management.

Course Format and Requirements

The Surveillance Detection for Bombing Prevention Course is a three day, instructor-led course designed for small group instruction of 20 participants. A classroom large enough to accommodate the registered participants with five easels for group activities is required. In addition, one to two field sites will be selected in conjunction with the course point of contact for conducting experiential learning activities. The following modules are provided during the course of instruction:

- Module 1: Course Introduction and Overview
- Module 2: Overview of Hostile Operations
- Module 3: Vulnerability Assessment
- Experiential Learning Activity 1: Vulnerability Assessment Activity
- Module 4: Hostile Surveillance Requirements
- Module 5: Surveillance Detection Requirements and Fundamentals
- Experiential Learning Activity 2: Detection Fundamentals Activity
- Module 6: Reporting and Response
- Module 7: Compromise and Deployment
- Experiential Learning Activity 3: Capstone Activity

Recommended Prerequisites

- FEMA ICS IS-100 series (Available at: https://training.fema.gov/is/searchis.aspx?search=ICS%20100)
- FEMA ICS IS-200 series (Available at: https://training.fema.gov/is/searchis.aspx?search=IS-200)
- IS-914: Surveillance Awareness: What You Can Do (Available at: https://training.fema.gov/is/courseoverview.aspx?code=is-914)

Scheduling Information

To request this course for your organization, please contact your local Protective Security Advisor (PSA) or email the Office for Bombing Prevention at: OBP@hq.dhs.gov.

Contact Information

For more information on the DHS Office for Bombing Prevention's Surveillance Detection for Bombing Prevention Course, please visit us at: http://www.dhs.gov/obp.

This page is intentionally left blank.

Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 2: Overview of Hostile Operations

Participant Workbook

This page is intentionally left blank.

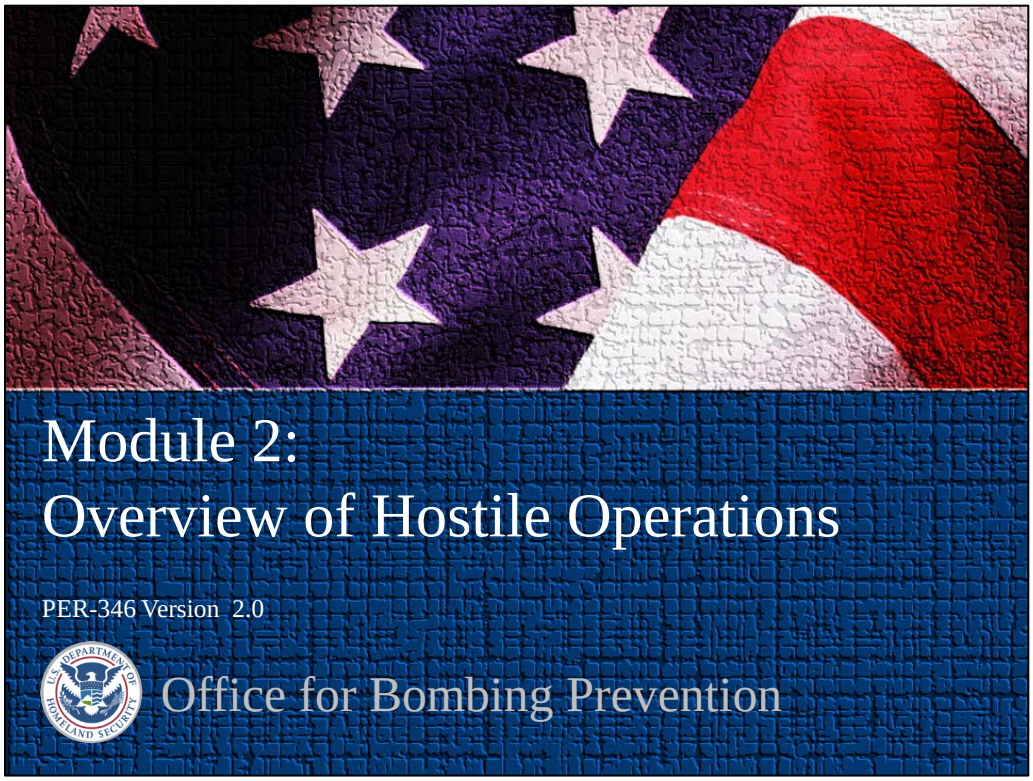
Number: Module 2

Title: Overview of Hostile Operations

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 2: Overview of Hostile Operations. The purpose of this module is to provide an overview of hostile operations and the role of surveillance in the terrorist attack cycle.

2. **Learning Objectives**

   a. **Terminal Learning Objective.** Given a written examination, participants will describe the role of surveillance in the terrorist attack cycle. (TAC-0130)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will differentiate between surveillance, hostile surveillance, and surveillance detection to achieve a minimum score of 70%. (TAC-0130a)

      (2) Given a written examination, participants will identify why hostiles conduct surveillance to achieve a minimum score of 70%. (TAC-0130b)

(3) Given a written examination, participants will identify what groups pose a threat to U.S. citizens and facilities to achieve a minimum score of 70%. (TAC-0130c)

(4) Given a written examination, participants will identify the tactics and vulnerabilities terrorists and criminals leverage to execute a bombing incident to achieve a minimum score of 70%. (TAC-0130d)

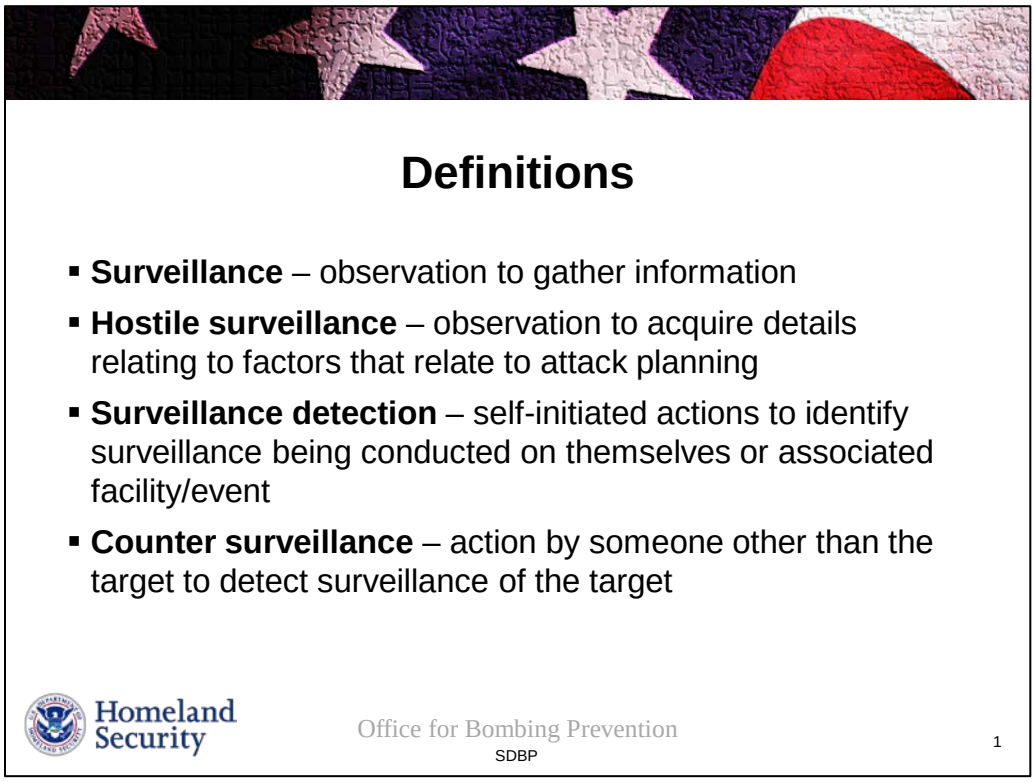
(5) Given a written examination, participants will indicate where in the terrorist attack cycle criminals and terrorists are most likely to conduct surveillance to achieve a minimum score of 70%. (TAC-0130e)

(6) Given an examination, participants will differentiate between elicitation and solicitation to achieve a minimum score of 70%. (TAC-0130f)

BODY

LECTURE/DISCUSSION ***1 hour, 25 minutes*** ***1:20***

Media 1



3. Definitions

a. Surveillance: observation of a place, person, group, or ongoing activity to gather information (Dictionary.com n.d.)

(1) Systematic. Webster defines systematic as methodical in procedure or plan. When conducted properly, surveillance is done in a methodical and well-orchestrated manner to ensure all three rings of security have been adequately observed. It is not haphazard or random. (Merriam-Webster 2017)

(2) Discreet. Webster defines discreet as “intentionally unobtrusive.” Thus, the observation is not obvious to the target. (Merriam-Webster 2017)

b. Hostile surveillance: act of keeping persons, facilities, or vehicles under observation for the purpose of acquiring details relating to vulnerability, patterns, and any other factors that relate to attack planning

(1) Can be systematic and discreet

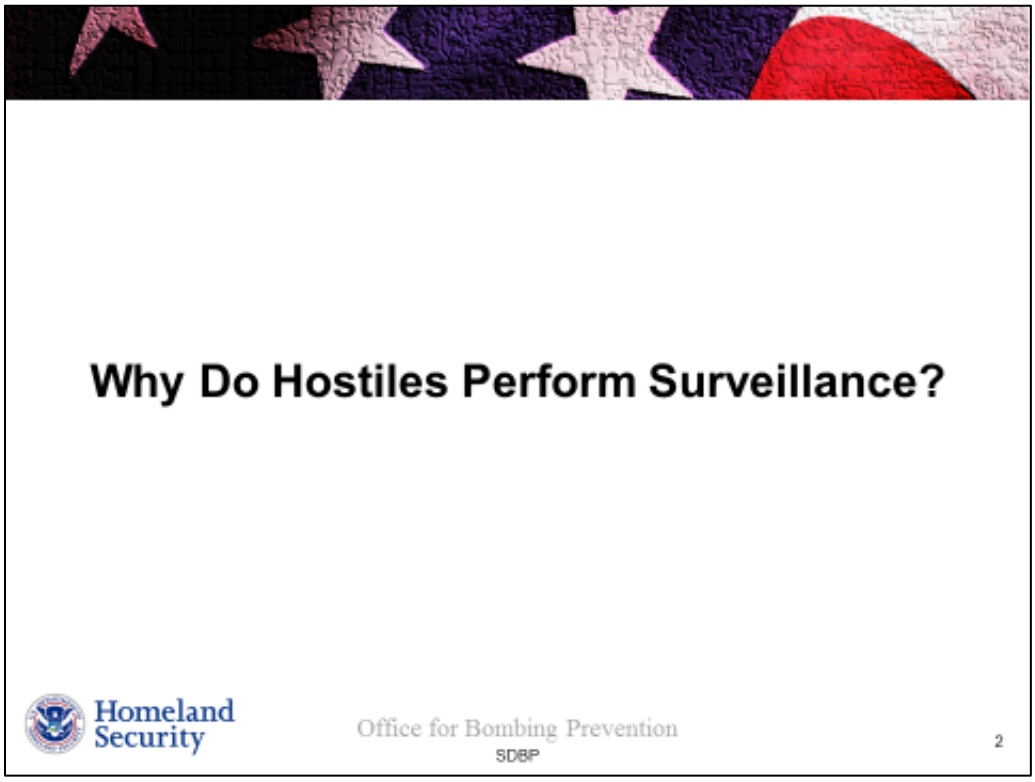
(2) For the purposes of this course, discreet hostile surveillance can only be effective when the target is unaware that they are under surveillance. To obtain enough

information to inform the target analysis and patterns of behavior, the surveillant must remain undetected for enough time to accomplish this task.

c. **Surveillance detection:** self-initiated actions taken by a person to identify surveillance being conducted on themselves or an associated facility/event

d. **Counter surveillance:** action taken by someone other than the target to detect the presence of surveillance of the target

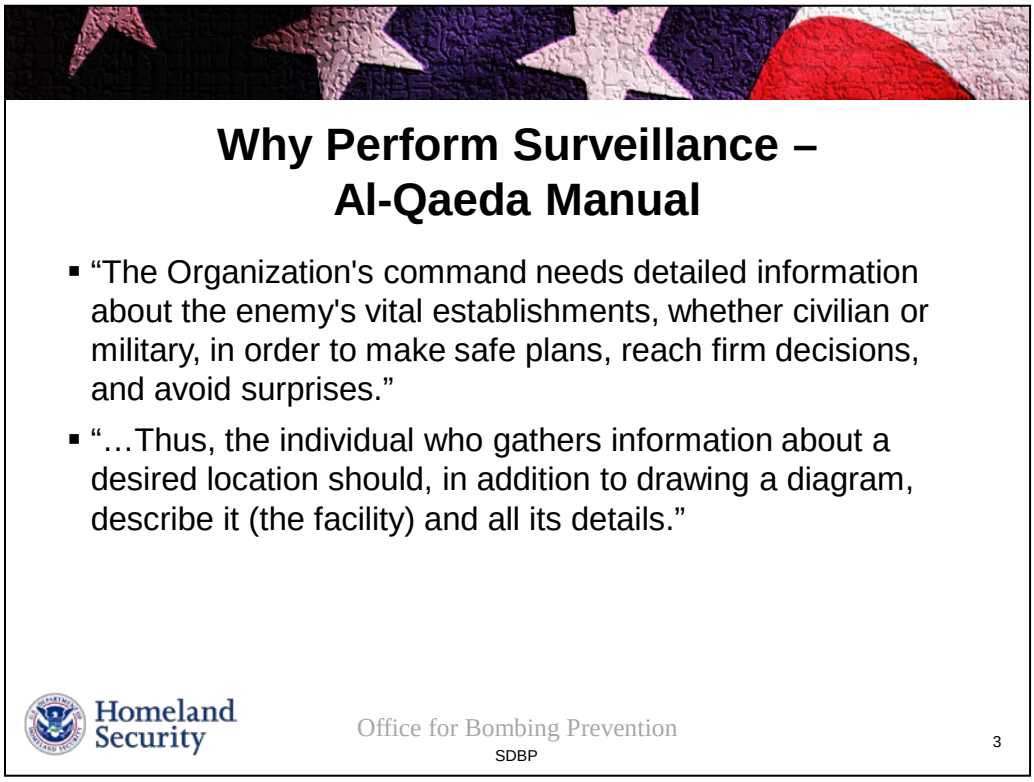
Media 2



4. Why Do Hostiles Perform Surveillance?

Take any notes you feel necessary below.

Media 3

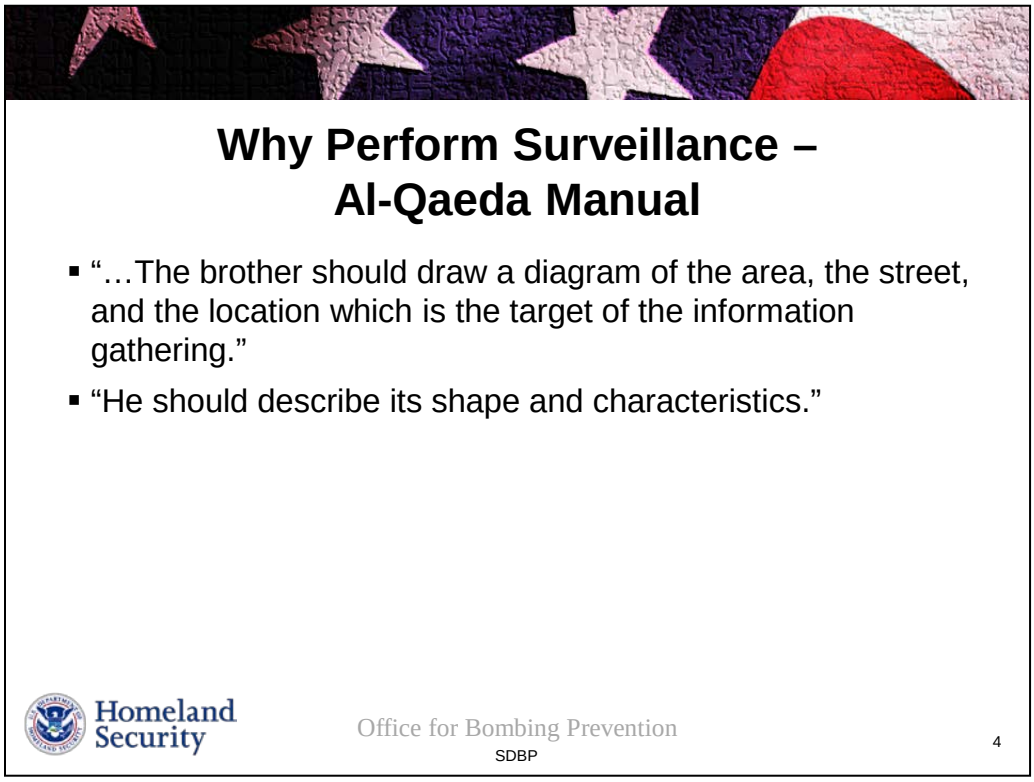


a. Why Perform Surveillance – Al-Qaeda Manual: According to Lesson 12: Information Gathering (Al Qaeda 2001):

(1) "The Organization's command needs detailed information about the enemy's vital establishments, whether civilian or military, in order to make safe plans, reach firm decisions, and avoid surprises."

(2) "…Thus, the individual who gathers information about a desired location should, in addition to drawing a diagram, describe it (the facility) and all its details."

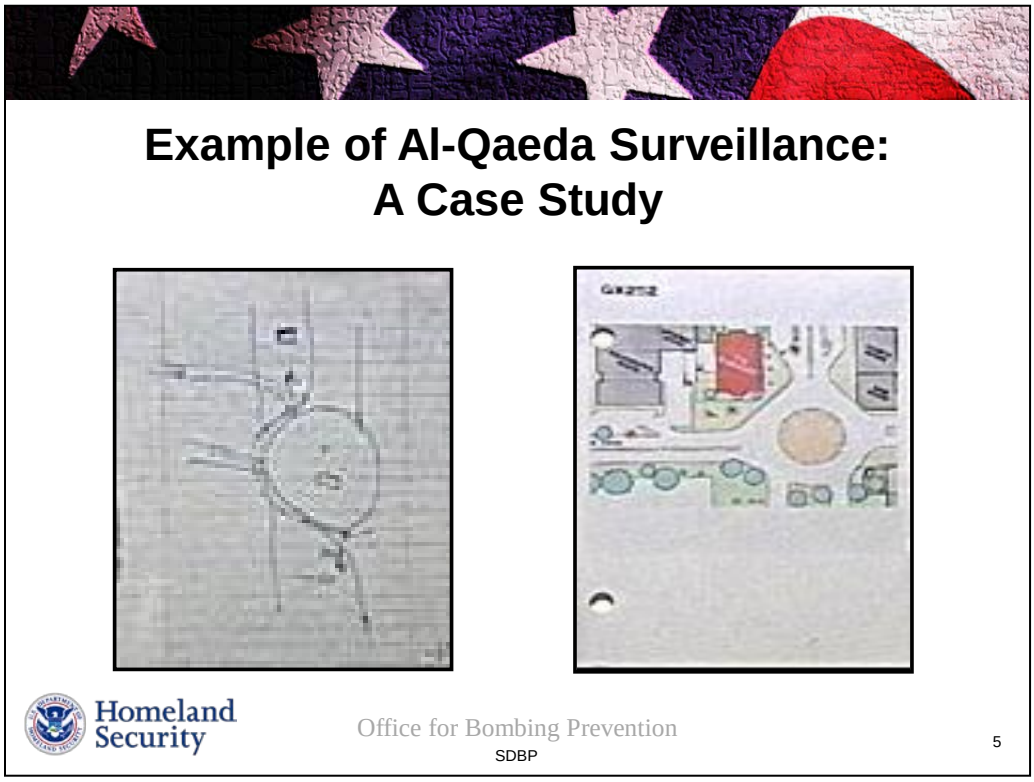
Media 4



(3) "…The brother should draw a diagram of the area, the street, and the location which is the target of the information gathering."

(4) "He should describe its shape and characteristics."

Media 5



b. Example of Al-Qaeda Surveillance: A Case Study. (Federal Bureau of Investigation 1998) Al-Qaeda conducted surveillance in preparation for the dual vehicle-borne improvised explosive device (VBIED) attacks launched against the U.S. embassy in Nairobi, Kenya on August 7, 1998, the eighth anniversary of the arrival of U.S. troops in Saudi Arabia for Desert Storm staging. The attack in Nairobi used 2,000 pounds of TNT in a work van that forced its way into the rear entrance of the embassy. That attack resulted in 213 fatalities (12 American).

Attacks on the U.S. embassy in Dar es Salaam, Tanzania were also carried out that same day. The attack in Tanzania resulted in 224 fatalities (12 American) and 4,500 injured.

Media 6

Example of Al-Qaeda Surveillance (cont.)

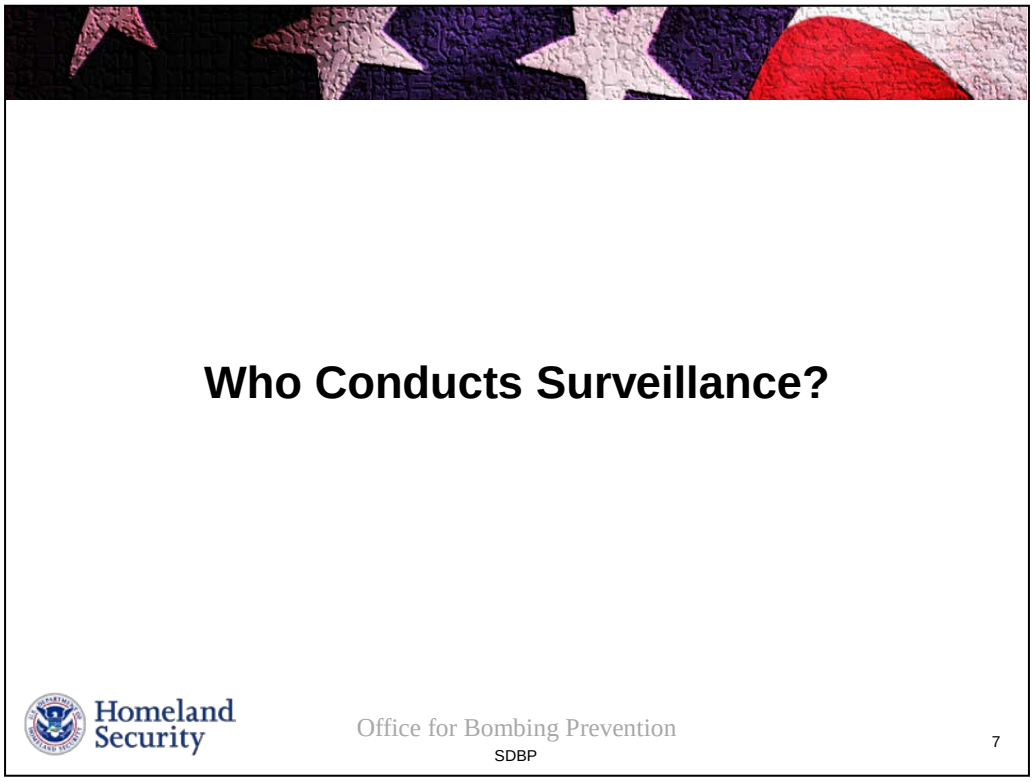
Homeland Security

Office for Bombing Prevention

SDBP

6

Media 7



Take any notes you feel necessary below.

Media 8

5. Who Conducts Surveillance

a. Terrorists. Terrorists are both international and domestic.

(1) International

(a) ISIS

(b) Hamas

(c) Al-Qaeda

(d) Hezbollah

(2) Domestic

(a) National Alliance (white separatist political organization based in West Virginia)

(b) Aryan Nation (far right supremacist organization)

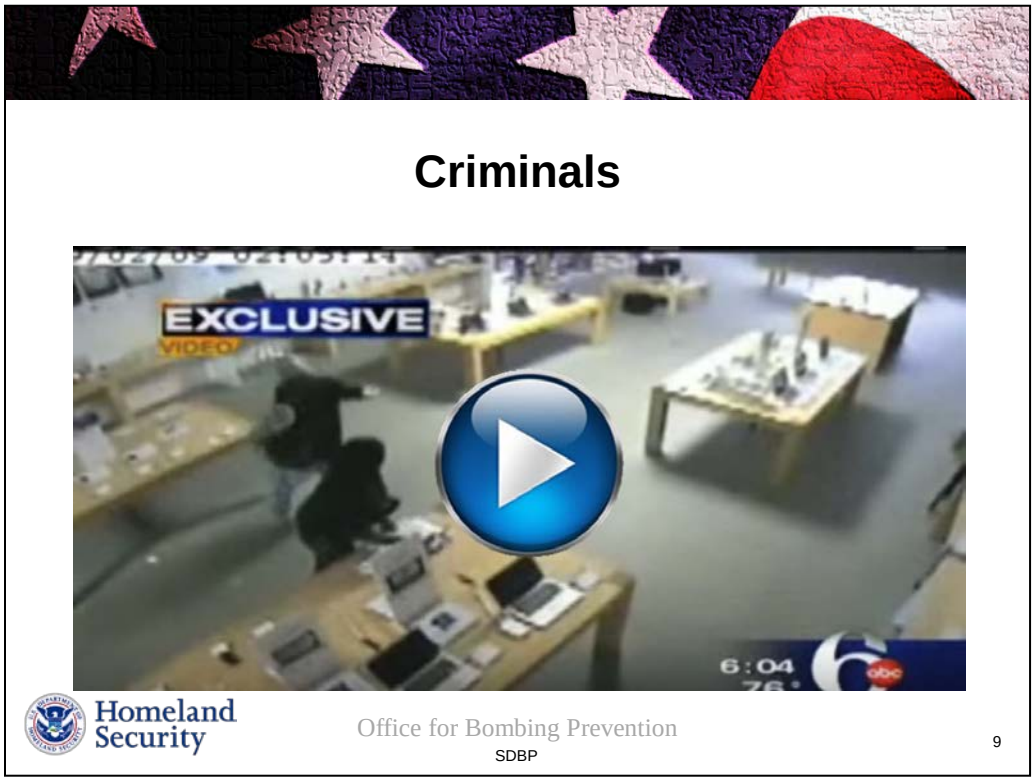
(c) Earth Liberation Front (ELF)

(d) Sovereign Citizens

(3) Researching and understanding the tactics, techniques, and procedures (TTPs) of our threat groups from the national level down to the sector-specific level attack

provides information on what they are looking for when they are conducting surveillance.

Media 9



b. Criminals. All criminals, even those at the lowest level (e.g., pick pockets) conduct surveillance to assess their target's vulnerabilities and weaknesses, the surrounding area, and what security is in place before they attack.

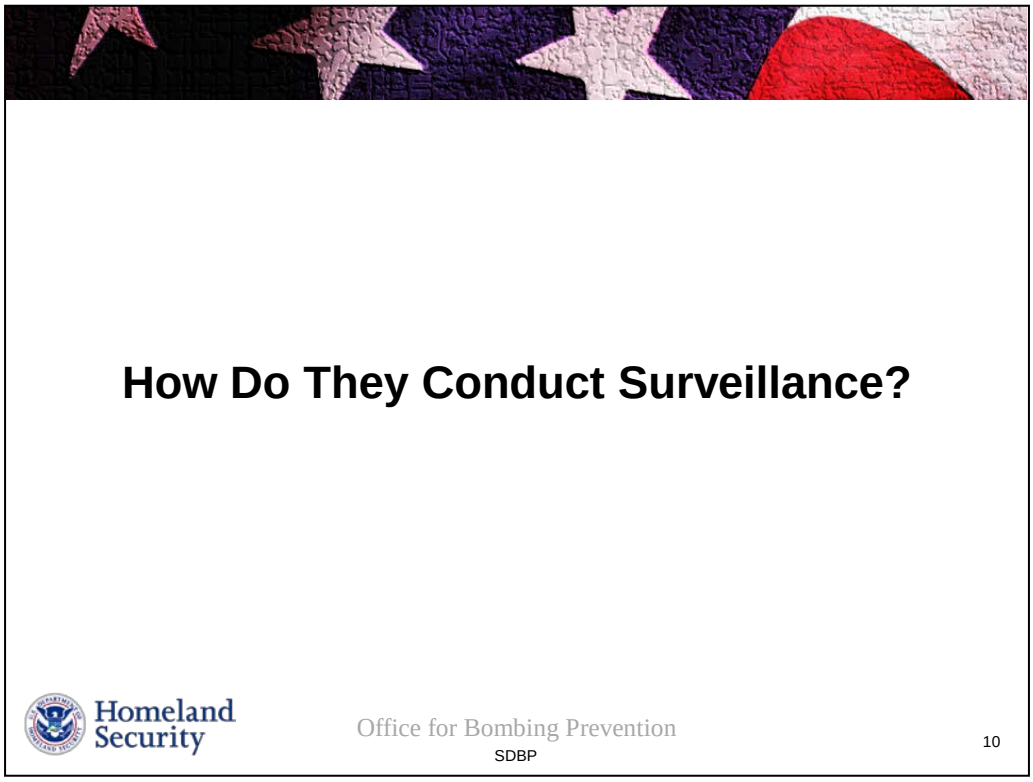
(1) In September 2009, five robbers broke into the Apple Computer store in Marlton, NJ at 2:05 AM.

(2) They broke a plate glass window with one blow from a blunt object and motioned to a security guard that they had a gun.

(3) In 31 seconds, they took 31 Mac Book Pros, 14 iPhones, and 9 iPod Touches.

Take any notes you feel necessary below.

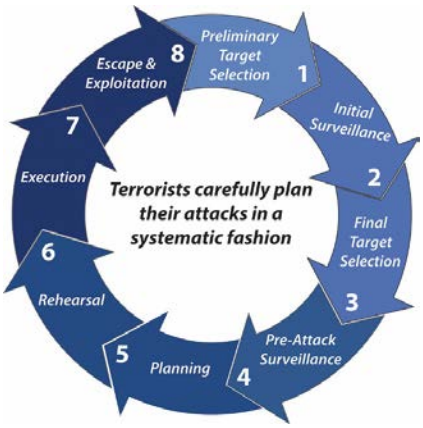
Media 10



Take any notes you feel necessary below.

Media 11

The Terrorist Attack Cycle



- Conceptual model
- Demonstrates terrorist operational planning
- Also applies to many criminals

Homeland Security

Office for Bombing Prevention

SDBP

11

Media 12

6. Steps of the Terrorist Attack Cycle

a. Step 1: Preliminary Target Selection. Several factors are considered during the preliminary target selection step.

(1) Goal/objectives of the extremist/criminal

(a) Political

(b) Ideological

(c) Financial

(2) Accessibility

(a) One must be able to gain access to the potential target.

(b) Targets with easier access are potentially of greater interest to an attacker.

(3) Criticality

(a) The target is important from an economic, industrial, or social perspective.

(b) The larger the target's role is in the functioning of society, the more crucial it potentially is. The more critical the target is, the greater interest it is to the attacker.

(4) Recognizability: The attacker may be likely to pick an obvious target that is immediately recognizable. For example, the White House is immediately recognizable even to those who have never been to Washington, DC.

(5) Symbolic value: The target holds special symbolic meaning. For example, the Statue of Liberty is well-known to the world and is a symbol of American freedom, so an attack on such a site may have symbolic value above other potential targets.

(6) Extremist capabilities

(a) The attacker(s) must be capable of attacking the location.

(b) A target that is desirable may be outside the attackers' capabilities due to insufficient funding, personnel, or expertise or because the chances of detection and failure make it too risky.

(7) Vulnerability

(a) Vulnerability is a function of both the target and the attackers' capabilities.

(b) Attackers look for the best combination of target vulnerabilities that match to their capabilities.

Media 13

b. Step 2: Initial Surveillance. Initial surveillance is conducted to determine viable targets based on maximum impact and greatest chance for success. It may be conducted from one of two approaches.

(1) The attacker is looking at security measures to identify vulnerabilities and then develop attack plans.

(2) The attacker has a specific tactic in mind and looks for targets that are vulnerable to that tactic.

Surveillance to gather intelligence occurs over a period of time. It usually goes on for weeks to months, depending on the targets.

Media 14

(3) **Singapore Case Study.** (TRIPwire n.d.) In 2001, Singapore was home to 17,000 U.S. citizens, almost 200 U.S. companies that employed about 2,000,000 local residents, and a regular port of call of the U.S. Navy. It had lax laws for fighting terrorism, making it a target-rich environment for terrorists.

Media 15

(a) The surveillance video was made in Singapore by Al-Qaeda operatives and delivered to a regional leader of the extremist group Jemaah Islamiah. In the subsequent investigation, the original tape was recovered. Narration on the tape was done subsequent to the actual taping.

(b) The video describes planning for attacks in Singapore and led to the recovery of further planning documentation.

(c) The investigation in response to the video recovered a target list. Targets included facilities and buildings, mass transit systems, residential areas, and commercial and military facilities.

1 Buses: Yishun bus stop frequented by U.S. sailors

2 Office establishments:

a U.S. and Israeli embassies

b British and Australian High Commission

3 U.S. residential areas and recreational facilities (focus on security)

a Restaurants: McDonald's and Kentucky Fried Chicken

b Military: Pava Lebar Air Base (50 photos of planes)

c Port/shipping: Kill zone along coast for attacking U.S. ships

d Economy/international trade: List of nearly 200 U.S. companies with three highlighted

(d) The narration on the tape commented on the targets and discussed potential methods of attacking the target.

1 On the footage of the bus stop, the narrator mentions the number of U.S. Navy sailors who frequented the location and focuses on a bicycle stand where they could place a bicycle with explosives attached. “There are a lot of bicycles here, so ours will not be suspicious. No one will even know it is there.”

2 The commentator also discusses some large columns and how best to knock them out to cause more loss of life. “These pillars look strong. Hmm. It will take a lot to bring them down.”

(e) The fact that the original tape had no sound while the second tape had narration dubbed in indicates the terrorists were studying the potential targets and subsequently dubbed in their thoughts and comments. This gives an indication of the detailed planning involved.

(f) On the portion of the tape in which the U.S. Embassy is considered, the narrator points out the number of trucks parked along the street near the embassy and offers the opinion that it will be easy to bring in a truck loaded with explosives and position it near the embassy. When a guard looks in the direction of the surveillant, the commentator laughs, seeming to indicate that the guard is oblivious to the surveillance. Again, the camera is obviously concealed and held by someone with good cover, perhaps awaiting a bus or standing near a kiosk.

(g) The potential attackers were aware of supposedly covert efforts by the U.S. and friendly governments to detect surveillance and made an attempt to study and pass information among themselves on the conducting of that surveillance.

(h) After this tape was made, Al-Qaeda operatives purchased four tons of ammonium nitrate. The ammonium nitrate was not found.

Take any notes you feel necessary below.

_____
_____
_____
_____
_____
_____
_____

Media 16

c. Step 3: Final Target Selection

(1) Soft targets and public gatherings are now much more prevalent choices than hard targets because:

(a) There is minimal or no access control.

(b) There may be no security, or security may be limited (e.g., unarmed security personnel).

(c) They provide a mass gathering of people.

(d) They are high media value targets.

(e) There are often minimal physical security measures.

(2) Examples that meet the criteria for a soft target are:

(a) Malls/shopping areas

(b) Schools

(c) Theaters

(d) Churches

(e) Restaurants/clubs

(f) Indoor and outdoor sporting events

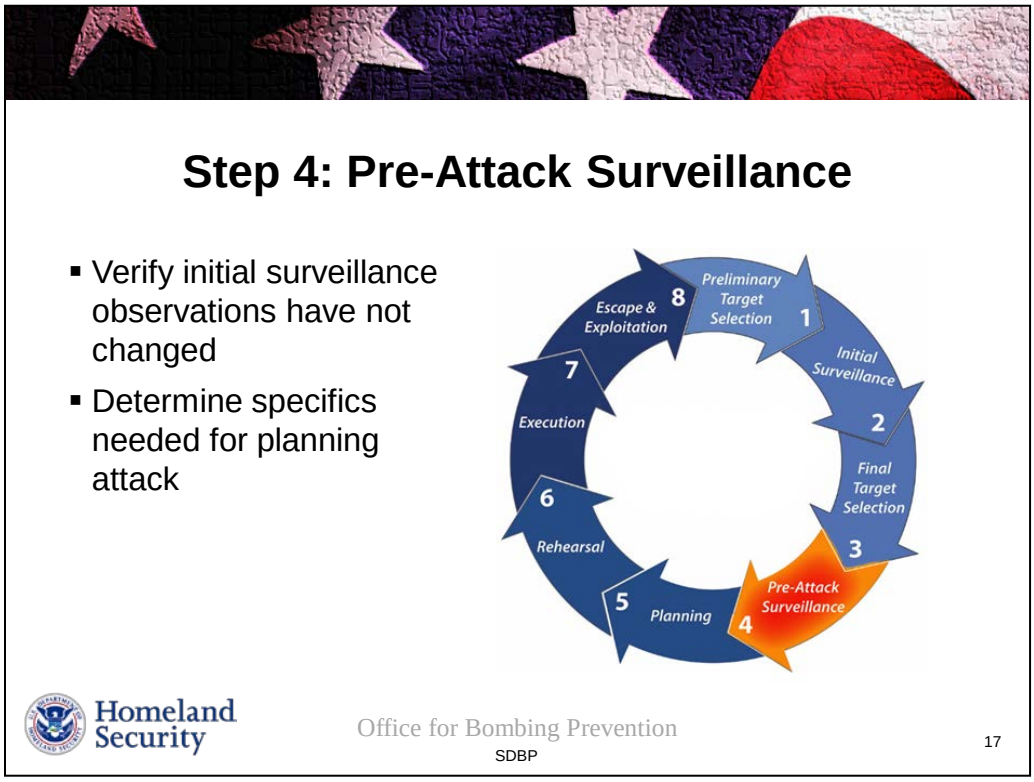
(g) Indoor and outdoor concerts

(h) Public gatherings

(i) Fairs

(j) Farmers' markets

Media 17

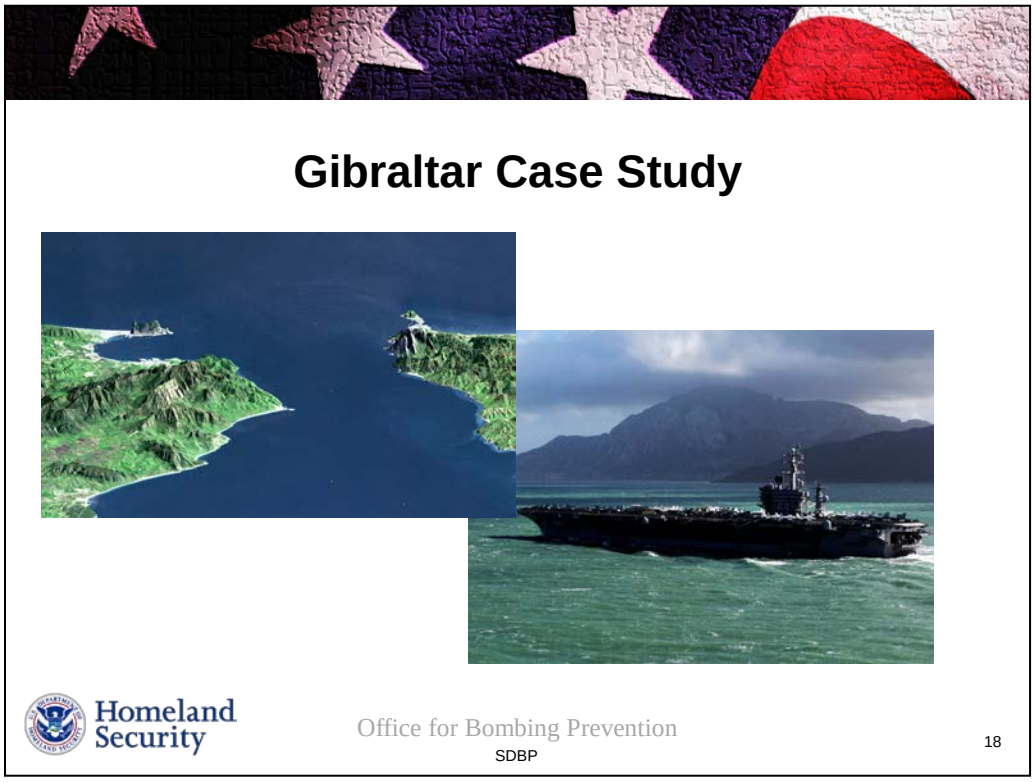


d. Step 4: Pre-Attack Surveillance. During this step, the would-be attacker intensifies the surveillance on the target selected. This step repeats many of the same elements of Step 2: Initial Surveillance.

(1) Pre-attack surveillance is conducted to confirm information gathered during the initial surveillance step, including identifying any changes from previous surveillance and determining if the target is still valid.

(2) Pre-attack surveillance is necessary because time has passed.

Media 18



(3) **Gibraltar Case Study** (Frantz 2002)

(a) Three Saudis were planning an attack on American or British warships similar to the attack on the USS Cole.

(b) They had integrated into the Moroccan society with well-established covers as an importer of fabrics and spare parts, the founder of a small employment agency, and a land speculator. They had married Moroccan women.

(c) The suspects conducted surveillance from January to April 2002, traveling twice to Gibraltar to identify landing areas along the beach and collect information on NATO ship movements.

(d) The plan was to purchase small Zodiac boats and load them with explosives to attack an American or British warship in the Strait of Gibraltar. They also planned attacks inside Morocco, including Marrakech.

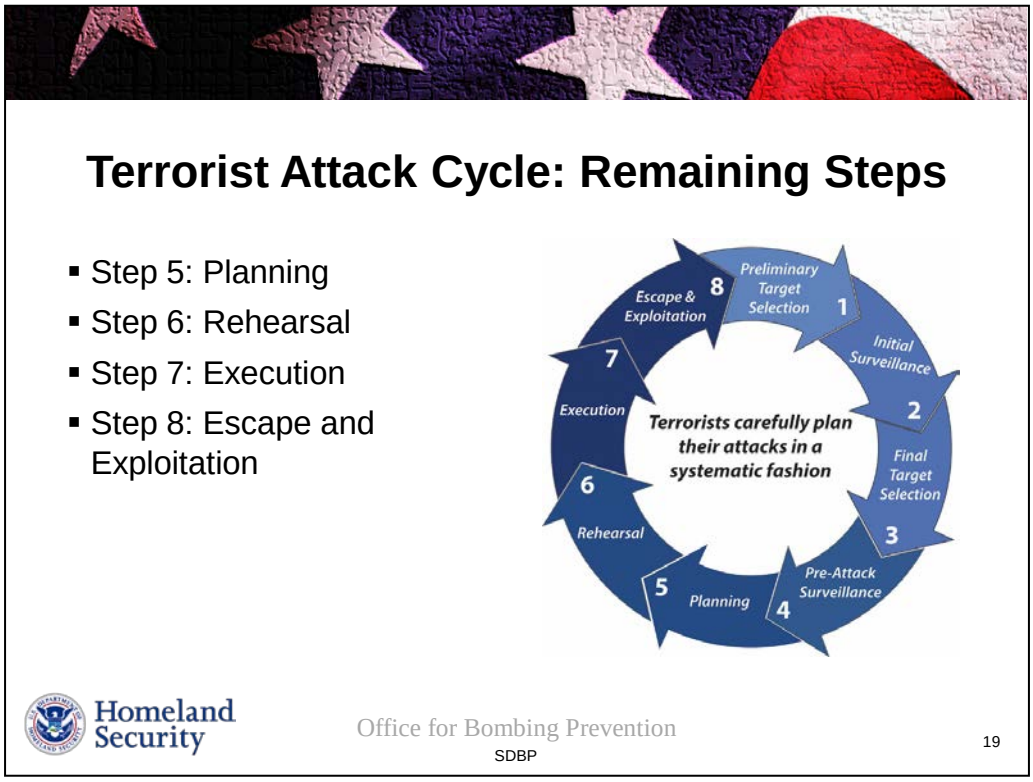
(e) In early 2002 the Director of the Central Intelligence Agency (CIA) went to Morocco to secure the kingdom's help in stopping future terror attacks. He had bits of information gained from suspects being held at Guantanamo Bay that Al-Qaeda operatives were in Morocco and possibly planning attacks.

(f) Within days, Moroccan intelligence agents were at Guantanamo Bay helping question Moroccan prisoners. They gained a sketchy portrait of a senior Al-

Qaeda operative believed to be orchestrating a plot in Morocco. That operative was identified from monitored telephone conversations and e-mail messages.

(g) They were arrested in March and May of 2002. Two of the wives were also arrested for transporting funds.

Media 19



e. Terrorist Attack Cycle: Remaining Steps. The surveillance that occurs in Steps 1 and 2 as discussed above support the remaining steps of the terrorist attack cycle.

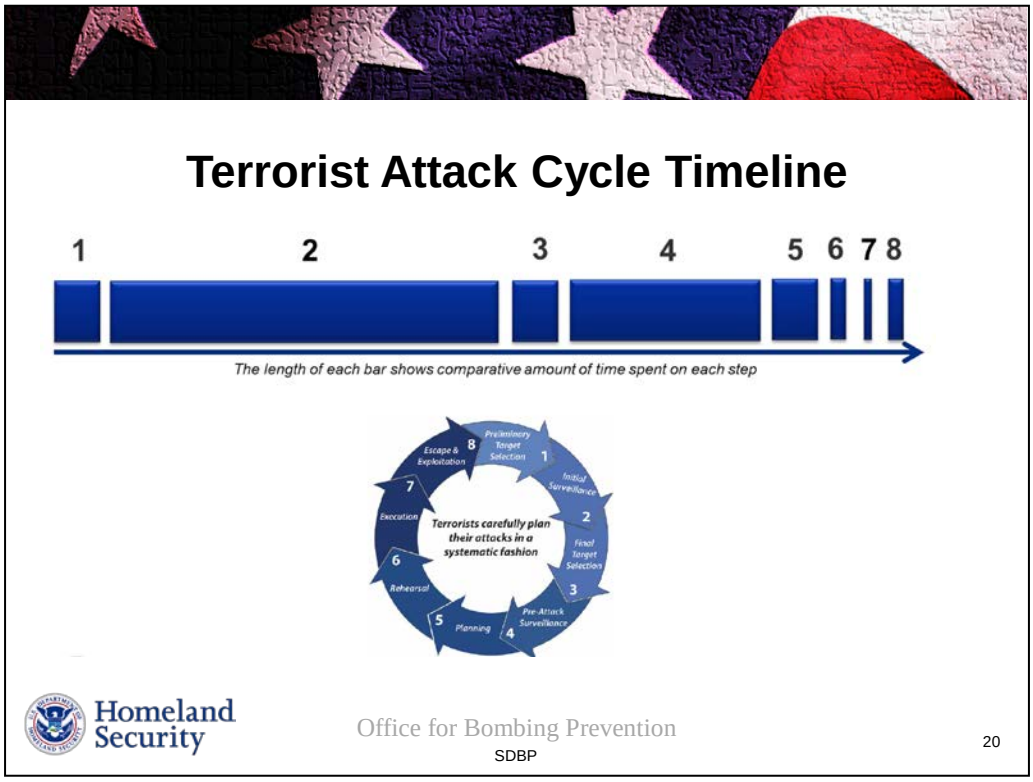
(1) **Step 5: Planning.** The attack is formulated/planned based on the surveillance data.

(2) **Step 6: Rehearsal.** The attackers rehearse to refine the planning and increase the probability that the attack will go as planned. The rehearsal is used to confirm that planning assumptions are realistic.

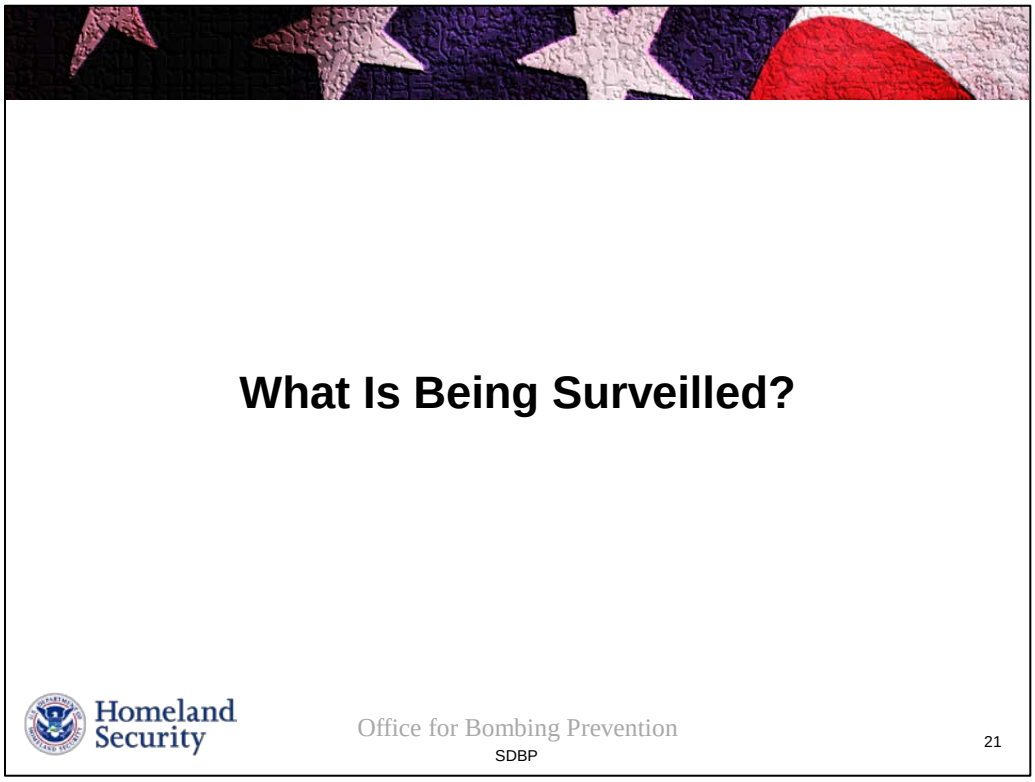
(3) **Step 7: Execution.** The attack team is deployed, and the attack is executed or aborted based on conditions.

(4) **Step 8: Escape and Exploitation.** Attackers use pre-planned escape routes that have been determined during surveillance, unless the plan is to commit suicide and the escape route is not important. Exploiting the attack is aimed at creating a media sensation to further political, personal, and/or financial goals. The attacker may leave videos or documents behind to increase media sensation.

Media 20

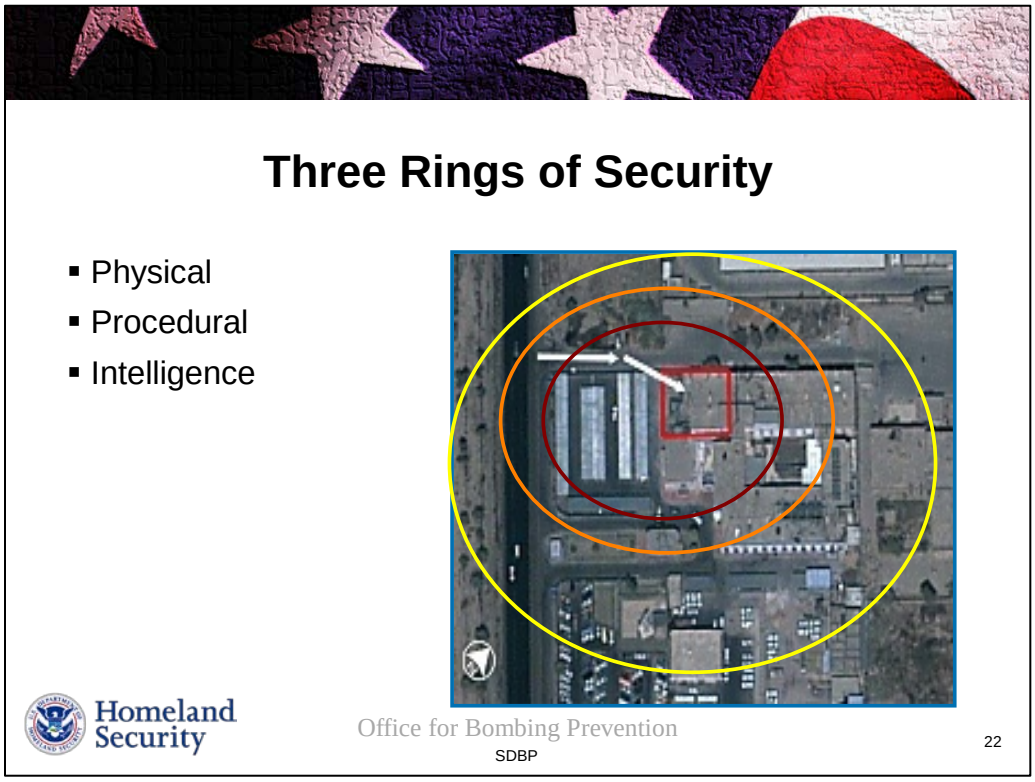

Terrorist Attack Cycle Timeline
1
2
3
4
5
6
7
8
The length of each bar shows comparative amount of time spent on each step
Preliminary Target Selection
Initial Surveillance
Final Target Selection
Pre-Attack Surveillance
Planning
Rehearsal
Execution
Escape & Exploitation
Terrorists carefully plan their attacks in a systematic fashion
Homeland Security
Office for Bombing Prevention
SDBP
20

Media 21



Take any notes you feel necessary below.

Media 22



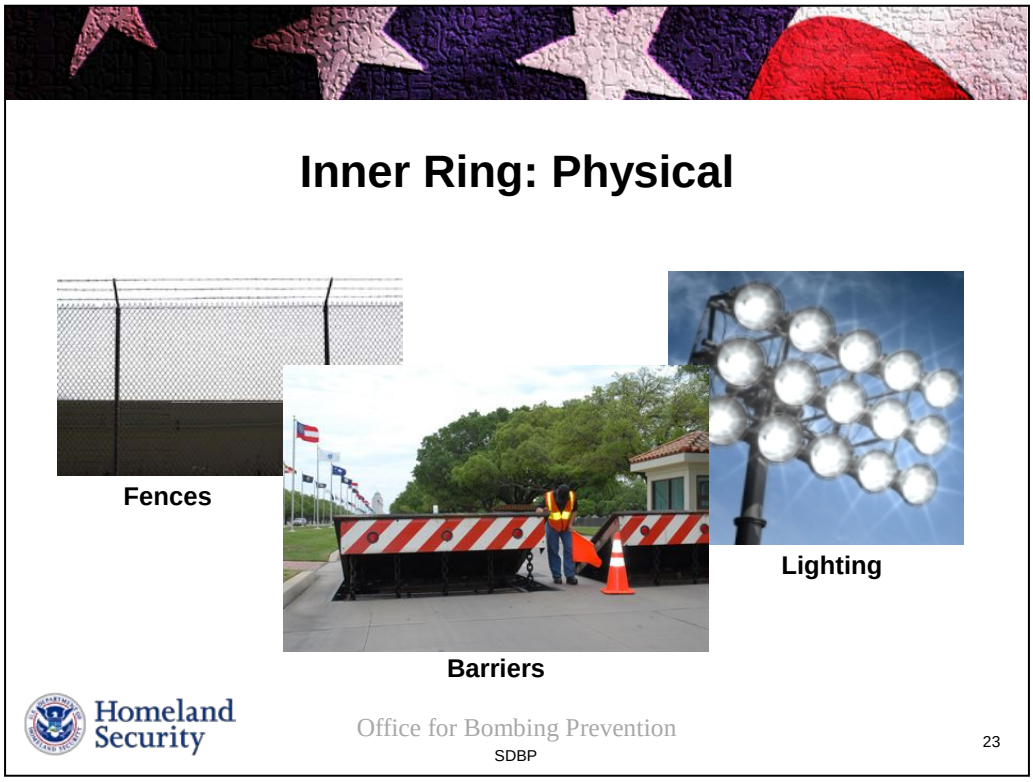
f. Three Rings of Security. Hostile surveillance seeks to assess and exploit what the attacker(s) can see in all three rings of security around a facility or event, so surveillance detection policies must address all three rings. The hostile surveillant is only going to exploit what can be seen and select the target based on that knowledge.

(1) Inner Ring (Red): Physical

(2) Middle Ring (Orange): Procedural

(3) Outer Ring (Yellow): Intelligence

Media 23



(4) **Inner Ring: Physical.** The inner ring is designed to safeguard personnel and areas from espionage, sabotage, damage, and theft.

(a) Structures that have been built to keep an area safe

1 Security gates and controlled parking entries

2 Entry and exit placement

3 Lighting

(b) Physical objects and the natural environment to reduce and manage risk

1 Landscaping

2 Fences

3 Bollards

4 Planters

(c) CCTV

1 Type (e.g., digital, thermal imaging)

2 Placement (perimeter coverage)

(d) External intrusion detection systems designed to prevent unauthorized access to equipment, installations, and areas

1 Buried line sensors

2 Fence-associated

3 Freestanding

4 Video motion activated

Media 24

(5) **Middle Ring: Procedural.** The middle ring encompasses the policies and procedures related to a facility's/event's security. These policies and procedures address a variety of things.

(a) Access control

1 Deliveries

2 Access screening (use of personal identity verification for entrance into parking areas or buildings, identification of visitors)

3 Managing very important people (VIPs)

(b) Use of technological devices such as closed circuit television (CCTV) and external intrusion devices

1 Tape retention time

2 Storing of videos

3 Responding to potential breaches of security

(c) Functioning of security forces

1 Gate security screening of visitors and deliveries

2 Monitoring existing technological devices

3 Security rounds/random anti-terrorism measures

Media 25

(6) **Outer Ring: Intelligence.** The outer ring is the intelligence security. Attackers do not know what the facility knows and will attempt to gather information on intelligence security through elicitation, solicitation, and other means such as social media and Internet searches.

(a) Elicitation is questioning individuals or otherwise gaining information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations security procedures, etc. in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. (Insititute for Intergovernmental Research 2016)

(b) Solicitation is the act of trying to obtain by usually urgent requests or pleas. (Merriam-Webster 2017)

(c) Searching social media and other indirect methods (like Internet searches) are also used to gain information on a target's intelligence ring.

Media 26

Homeland Security

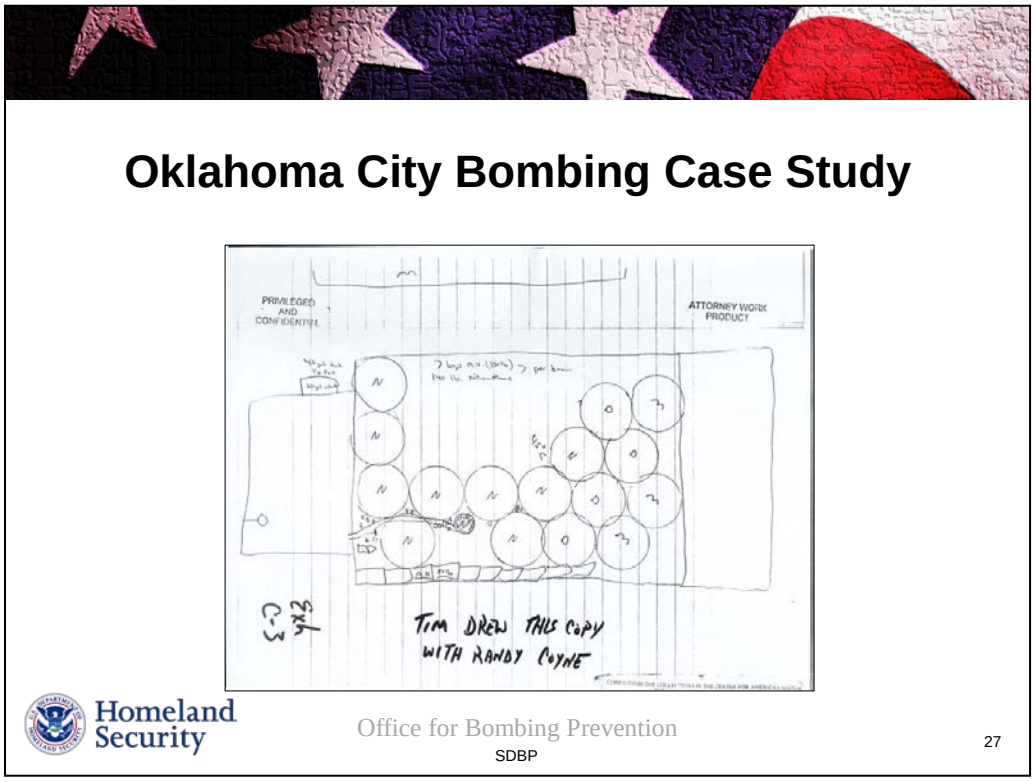
Office for Bombing Prevention

SDBP

26

Take any notes you feel necessary below.

Media 27



7. **Oklahoma City Bombing Case Study.** (TRIPwire n.d.) On April 19, 1996, Timothy McVeigh and his accomplices bombed the Murrah Federal building, which resulted in 168 deaths and more than 680 non-fatal injuries.

   a. On October 20, 1994, McVeigh and Terry Nichols conducted surveillance on the Murrah building prior to selecting it as a target. Their surveillance included timing of a possible egress route from the building to determine where McVeigh would be when the bomb detonated.

   b. The Murrah Federal Building was chosen because it:

   (1) Housed several Federal agencies.

   (2) Had a glass façade that made it especially vulnerable and was expected to shatter under the impact of the blast.

   (3) Was adjacent to a large, open parking lot across the street, which was expected to absorb force and protect occupants of nearby non-federal buildings.

   (4) Provided good camera angles for the media.

   (5) Had no surveillance detection in place.

   (6) There were no protective measures in place around the building since this type of attack was believed to be impossible to occur in the U.S. at the time.

c. In December of 1994, McVeigh and Michael Fortier (another accomplice) conducted a secondary surveillance by driving around the building twice, noting the structural integrity of the elevator shaft. They observed that the reinforced construction of the elevator shaft would keep the building from collapsing. They then drove through an alley and loitered in the Murrah Federal Building parking lot, looking at the building from several angles for approximately 20 minutes to discuss the bombing.

d. McVeigh avoided the building during the week prior to the bombing.

Media 28

8. **Barot Bombing Plot Case Study.** (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) Dhiren Barot was a British citizen born in India in December 1971. At age 20, he announced his conversion from Hinduism to Islam and came under the influence of the radical London cleric.

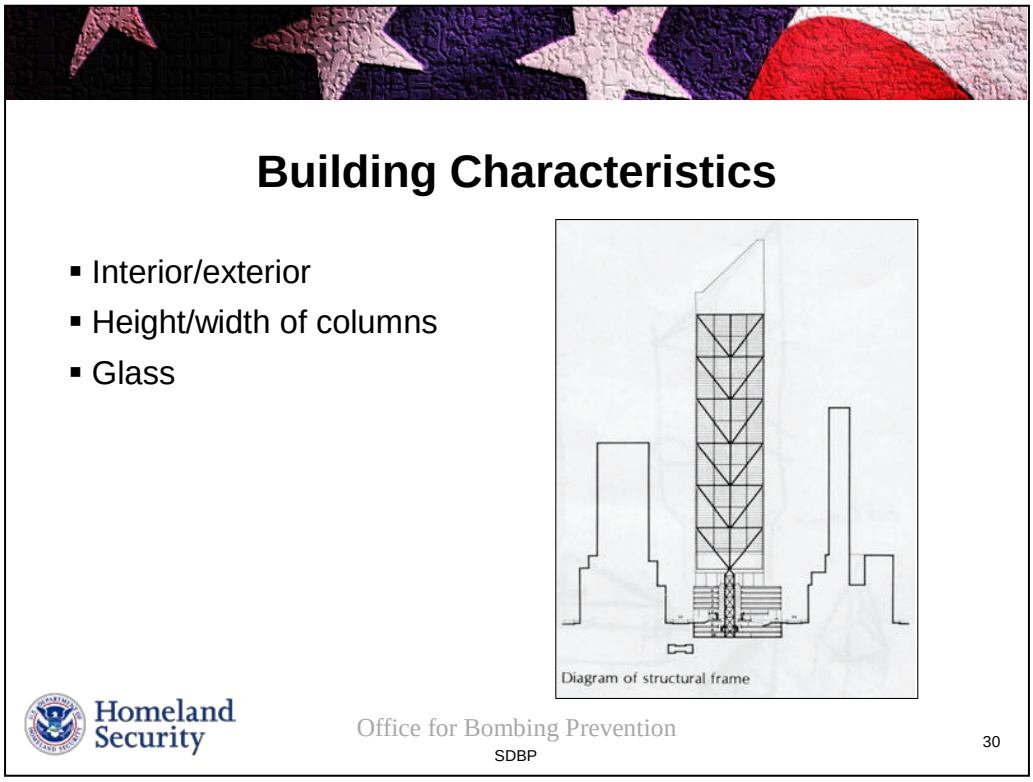
   He cased financial targets in the New York City and Washington, D.C. areas and developed highly detailed casing reports during two visits from 17 August to 14 November 2000 and 11 March to 8 April 2001. His reports contained both written descriptions of the target facilities and video surveillance.

   His activities in the United States went undetected until British authorities found files on a laptop computer in his London garage that contained casing reports on five buildings housing prominent U.S. and international financial institutions.

Media 29

Take any notes you feel necessary below.

Media 30



a. Building Characteristics. (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) Barot described each of the buildings he surveilled in detail. His descriptions included:

(1) The interior and exterior features.

(2) The buildings' facades, structural supports, and parking structures.

(3) Estimates of the height and width of building columns and their capability to withstand a vehicle-borne improvised explosive device (VBIED) attack.

(4) Which buildings were close enough to the street to target with a VBIED.

(5) Calculations of the distance between exterior columns to determine the optimal size of a VBIED that could be driven between them.

(6) The potential for glass shards to injure or kill people in and around the target building.

In one report, he recorded the exact number of windows and their approximate square footage, and he repeatedly stressed the potential destruction an attacker could cause by driving a VBIED through atriums and large windows.

Media 31

b. Traffic and Pedestrian Patterns. (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) He observed and analyzed the traffic patterns and pedestrian activity in the vicinity of the prospective target buildings. His observations included:

(1) The number and direction of adjacent lanes and the traffic volumes at various times of day.

(2) Features affecting how close to a building a vehicle could park.

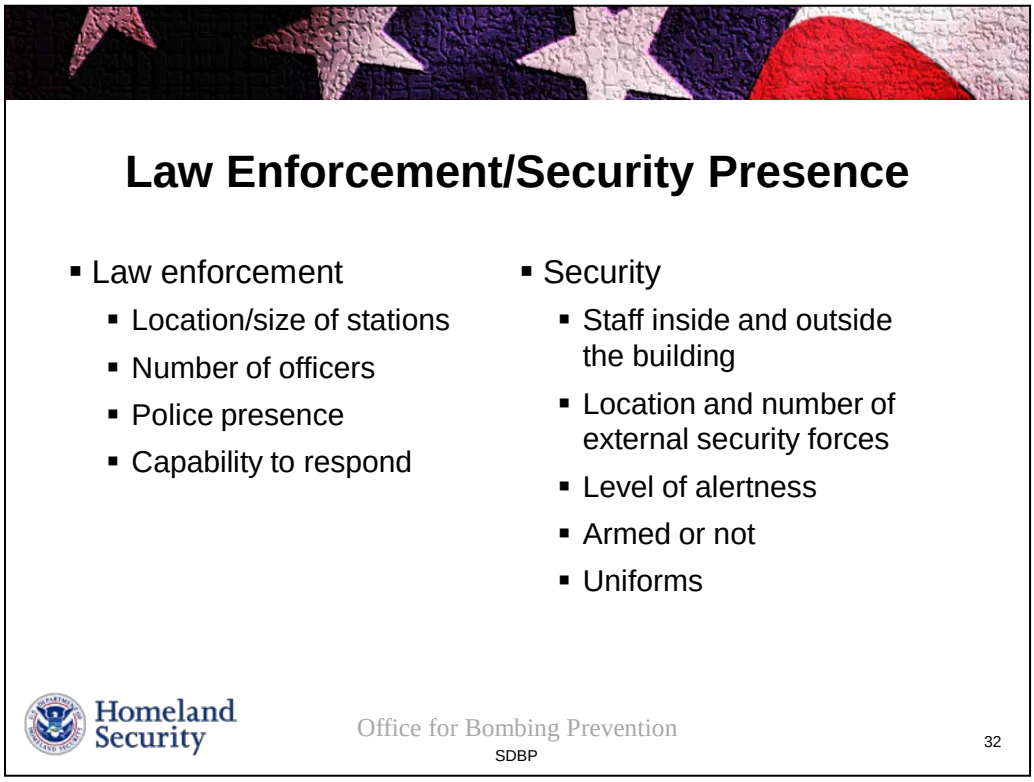
(3) Which traffic lanes were blocked and the types of vehicles that typically parked in lanes adjacent to a facility.

(4) The number of people who passed by a building's entrances, apparently to determine the places and times at which attacks could achieve the maximum number of casualties.

(5) The flow of pedestrians in the vicinity of a targeted facility and the period of peak pedestrian presence.

His observations of automobile traffic tied directly into his analysis of police and other responders' ability to react to an attack.

Media 32



c. Law Enforcement/Security Presence. (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) He made careful observations and estimates of law enforcement and security presences.

(1) Law enforcement

(a) The location and size of police stations and their distance from the target facility.

(b) The number of officers visible at each station and, in some cases, photographs of the station.

(c) The level of police presence around the prospective target facility, including how many police cars would pass by it.

(d) An estimate of the capability of a station to respond to an incident, based on the size of the station and its distance from the target facility, assuming that smaller or more distant stations would be less capable of responding quickly.

(2) Security

(a) The security staff posted inside and outside the buildings.

(b) The location and number of external security forces and their respective roles.

(c) The security officers' level of alertness.

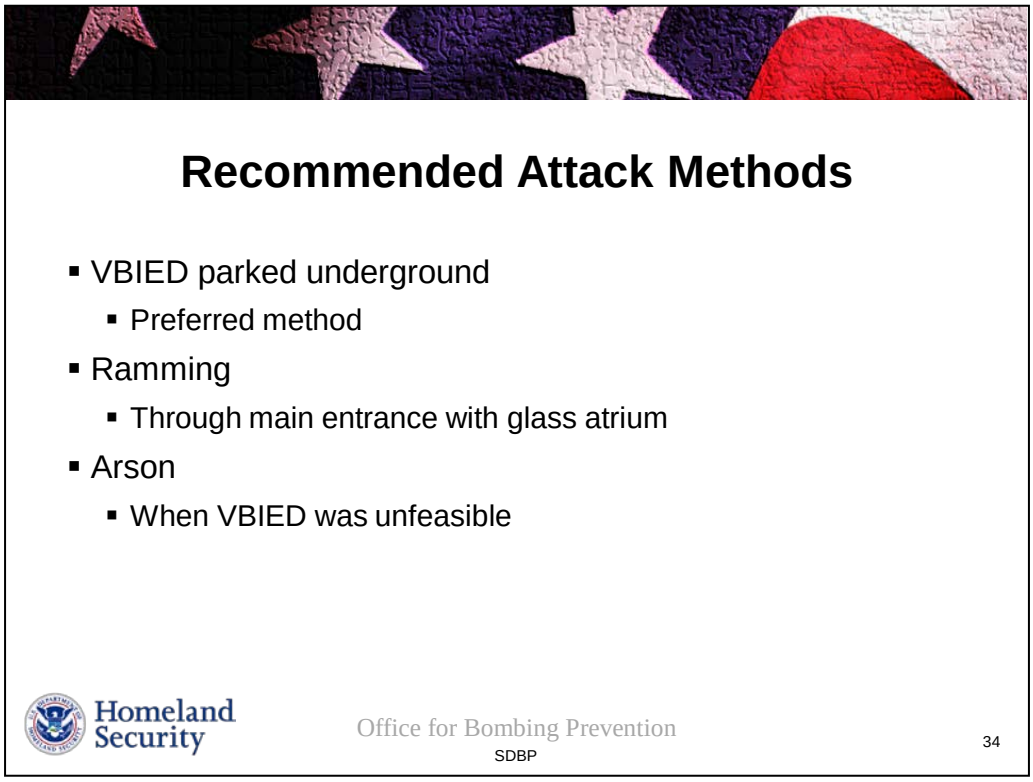
(d) Whether security staff were armed.

(e) The security officer's uniforms.

Media 33

d. Security Cameras. (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) Barot recorded the physical description of each camera he was able to identify. He noted their size and shape and assessed that physically longer cameras must be used for “long-range surveillance.” Barot commented that the numerous camera housings with opaque or black-tinted covers he observed would allow controllers to conceal from public view the direction in which they were pointed.

Media 34



e. Recommended Attack Methods. (U.S. Department of Homeland Security, Office of Intelligence and Analysis 2009) Barot recommended three potential methods of attack.

(1) VBIED parked underground. This was his preferred method. He recommended it be transported in a limousine or a service or delivery truck to minimize undue attention or suspicion by security personnel. His reports recommended parking a bomb-laden limousine beneath a building after gaining access by deception or by compromising security personnel.

(a) He described routes that would permit a non-suicidal attack team to escape before the device detonated.

(b) He cited the importance of carefully considering the structural elements of the building, particularly its columns. He calculated what he determined as a layman to be the optimal distance at which a VBIED could be parked to weaken or bring down the building.

(2) Ramming. As an alternative to a VBIED, he proposed ramming a truck, such as an oil tanker or a medium-size panel van, through the main entrance of a target building with a large glass atrium. He noted that this method was especially applicable to one surveilled facility that had a main front entrance that did not have a raised curb to block a vehicle.

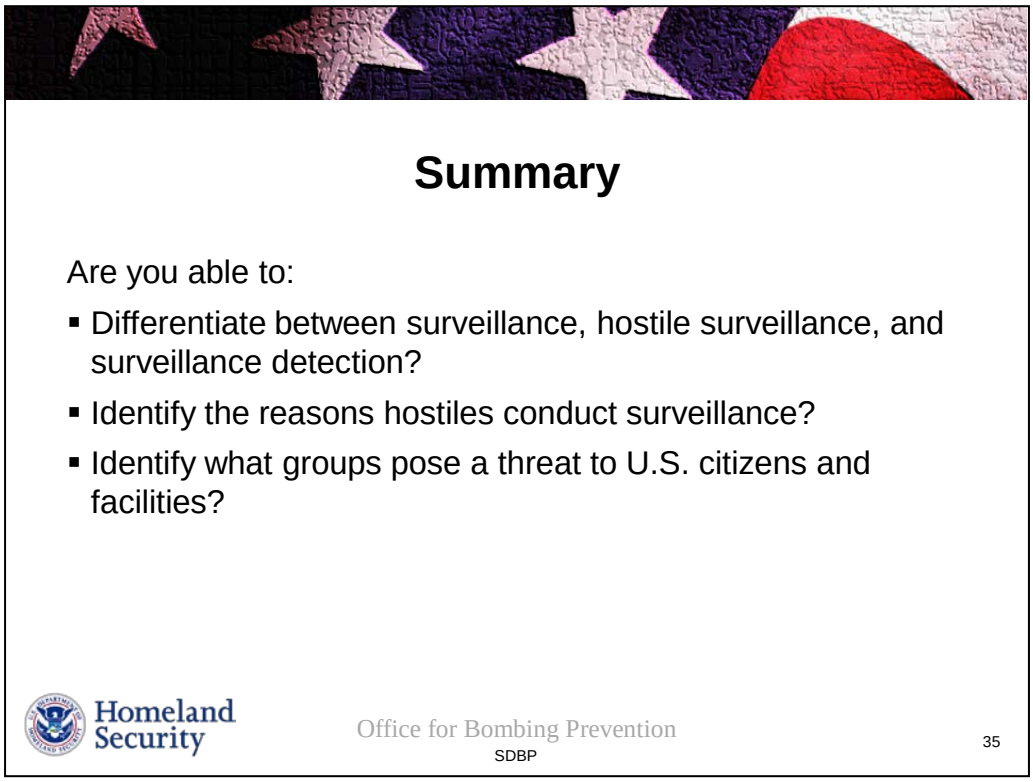
(3) Arson. He suggested arson for facilities where a VBIED was unfeasible. He noted that most office buildings use suspended ceilings, and it would be easy to hide

incendiary devices. He suggested publicly accessible bathrooms on each floor as the best location for igniting a fire.

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 35



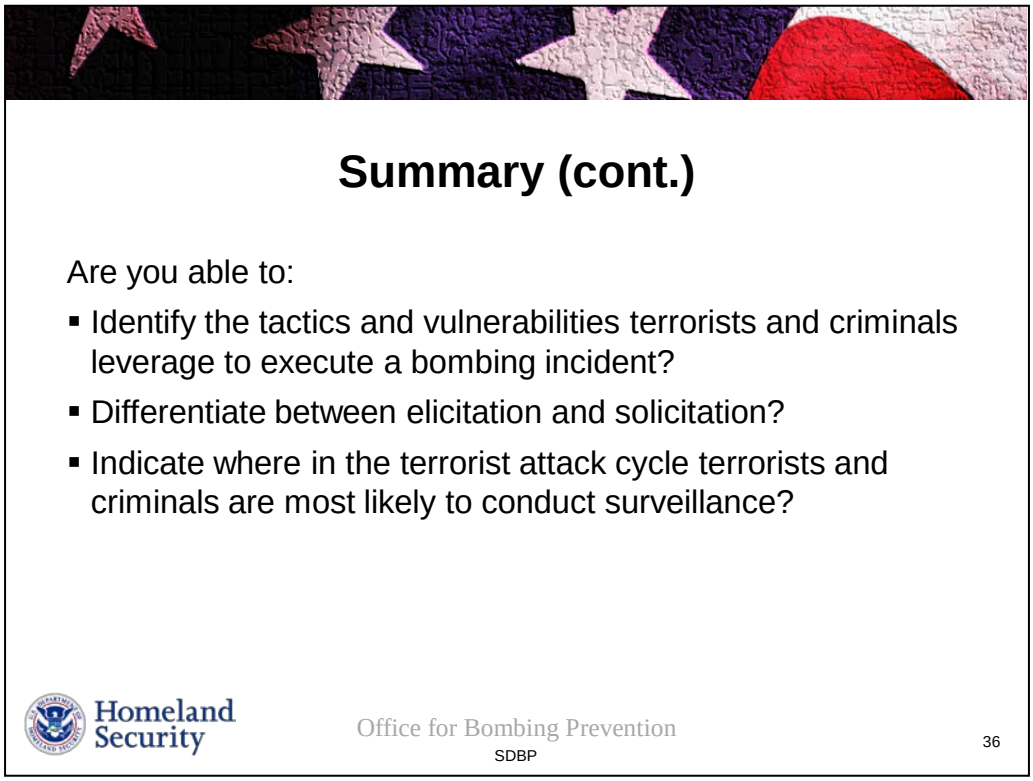
9. Summary. This module served to introduce you to an overview of hostile operations. Are you able to:

a. Differentiate between surveillance, hostile surveillance, and surveillance detection?

b. Identify the reasons hostiles conduct surveillance?

c. Identify what groups pose a threat to U.S. citizens and facilities?

Media 36

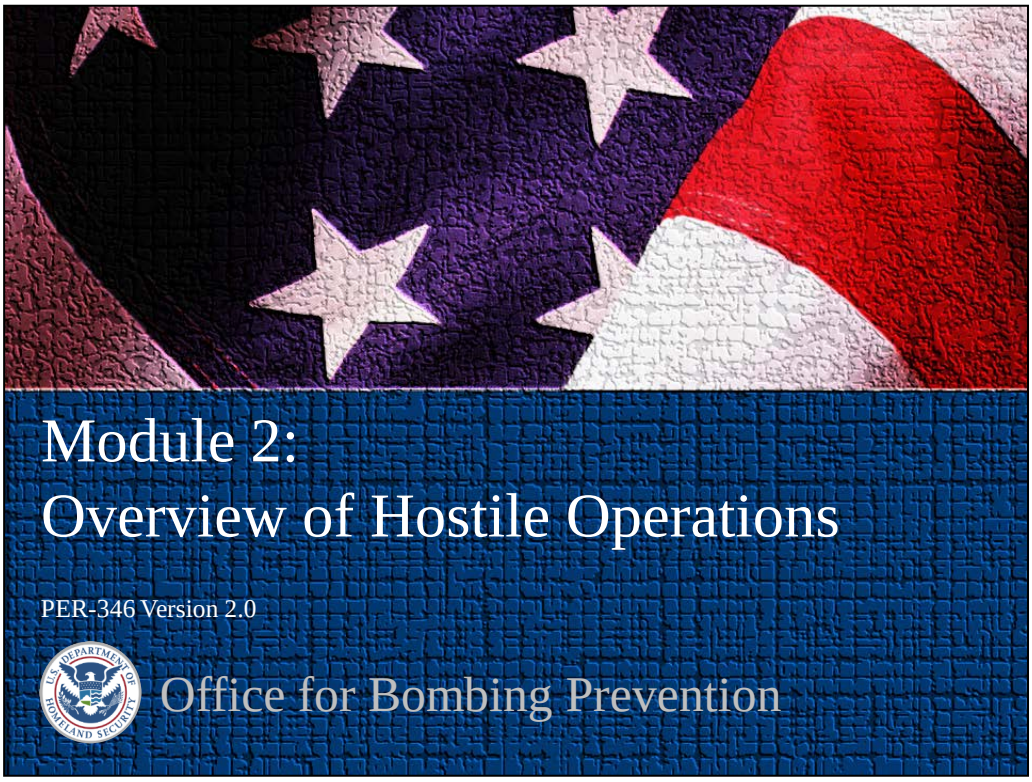


d. Identify the tactics and vulnerabilities terrorists and criminals leverage to execute a bombing incident?

e. Differentiate between elicitation and solicitation?

f. Indicate where in the terrorist attack cycle terrorists and criminals are most likely to conduct surveillance?

Media 37


Module 2:
Overview of Hostile Operations
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

Al Qaeda. 2001. *Cryptome.* December 8. Accessed April 1, 2017. http://cryptome.org/alq-terr-man.htm.

Dictionary.com. n.d. "surveillance." *The American Heritage® Science Dictionary.* Houghton Mifflin Company. Accessed March 5, 2017. http://www.dictionary.com/browse/surveillance.

Federal Bureau of Investigation. 1998. *Bombings of the Embassies of the United States of America at Nairobi, Kenya and Dar Es Salaam, Tanzania.* Executive Summary, Washington, D.C.: U.S. Department of Justice.

Frantz, Douglas. 2002. "U.S. Enlists Morocco's Help to Counter Terrorist Plots." *The New York Times.* New York City, June 24. http://www.nytimes.com/2002/06/24/world/us-enlists-morocco-s-help-to-counter-terrorist-plots.html.

Insititute for Intergovernmental Research. 2016. "Resources." *Nationwide SAR Initiative (NSI).* February. Accessed July 31, 2017. https://nsi.ncirc.gov/documents/SAR_Indicators_One-Pager.pdf.

Merriam-Webster. 2017. *Merriam Webster Dictionary.* Accessed July 27, 2017. https://www.merriam-webster.com/dictionary/threat.

TRIPwire. n.d. *Technical Resource for Incident Prevention.* Department of Homeland Security. Accessed March 1, 2017. tripwire.dhs.gov.

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0246-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Introduction." (U/FOUO).

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0247-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Attack Methods." (U/FOUO).

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0248-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Automobile and Pedestrian Traffic Patterns." (U/FOUO).

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0249-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Building Characteristics." (U/FOUO).

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0250-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Police and Security Forces." (U/FOUO).

U.S. Department of Homeland Security, Office of Intelligence and Analysis. 2009. "(IA-0251-09) Preoperational Surveillance: Dhiren Barot Casing Reports - Security Cameras." (U/FOUO).

This page is intentionally left blank.

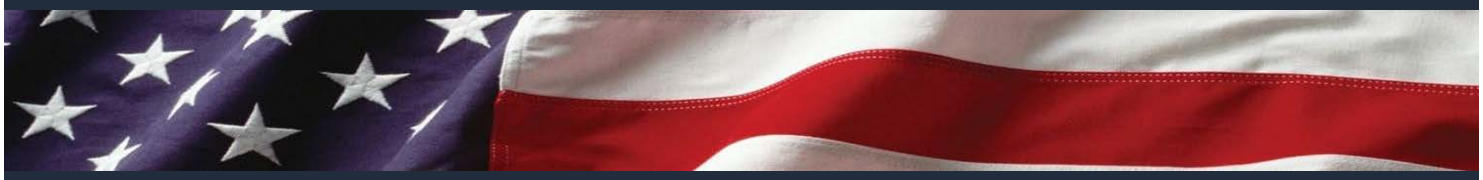
Module 2
Supplemental Materials

This page is intentionally left blank.

Suspicious Activity Reporting
Indicators and Behaviors

Tools for Analysts and Investigators

Behaviors	Descriptions
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.
Potential Criminal or Non-Criminal Activities Requiring Additional Information During Vetting *Note: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.*	
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/ Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 3: Vulnerability Assessment

Participant Workbook

This page is intentionally left blank.

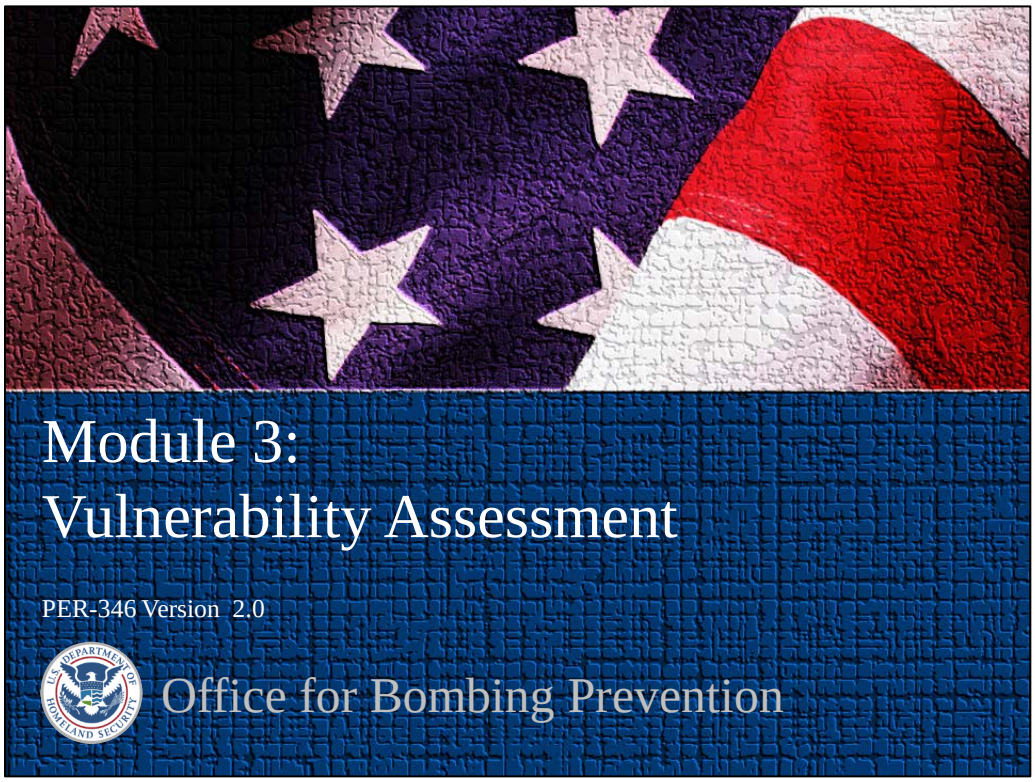
Number: Module 3

Title: Vulnerability Assessment

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 3: Vulnerability Assessment. The purpose of this module is to provide the steps for completing a modified vulnerability assessment (VA) based on the DHS risk management process.

2. **Learning Objectives**

   a. **Terminal Learning Objective.** Given a written examination, participants will describe the key considerations included in the vulnerability assessment as it applies to surveillance detection according to the criteria discussed in class. (RMP-0110)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will identify the purpose of conducting a vulnerability assessment as it relates to surveillance detection to achieve a minimum score of 70%. (RMP-0110e)

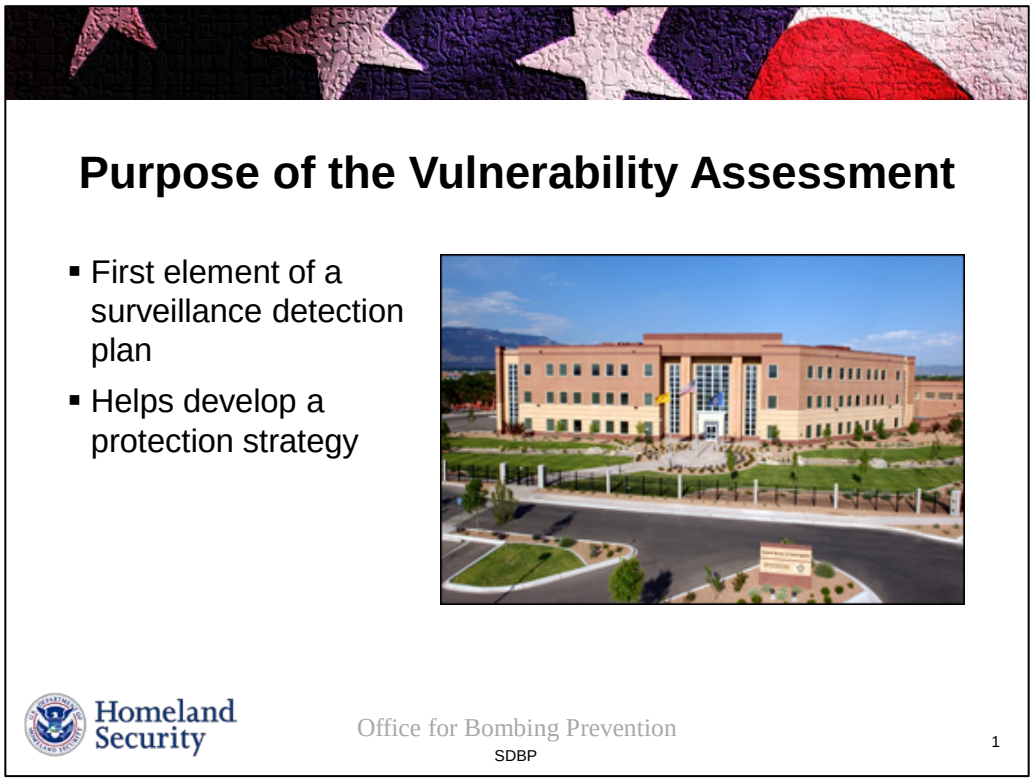
(2) Given a written examination, participants will identify the key considerations included in the vulnerability assessment as it applies to surveillance detection to achieve a minimum score of 70%. (RMP-0110f)

(3) Given an image, participants will identify strengths and weaknesses of a facility/area according to the key considerations included in the vulnerability assessment discussed in class. (RMP-0110g)

BODY

LECTURE/DISCUSSION ***55 minutes*** ***1:20***

Media 1

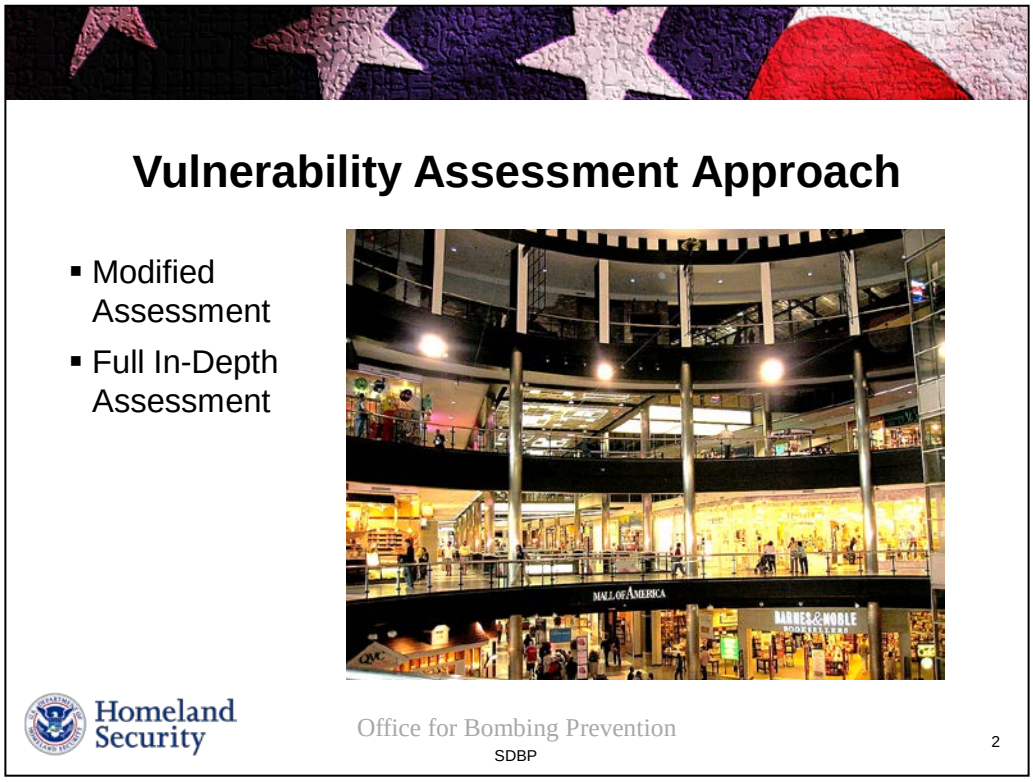


3. **Purpose of the Vulnerability Assessment.** Conducting the vulnerability assessment is the first element of the surveillance detection plan. The vulnerability assessment is part of the risk management process for any facility, system, or event.

   a. Adversaries attempt to identify vulnerabilities by conducting surveillance on a facility or area to fill knowledge gaps regarding the physical and procedural security or to confirm known data to exploit those vulnerabilities and develop the best course of action to ensure a successful attack.

   b. Knowing your vulnerabilities helps you develop a protection strategy.

Media 2



c. Vulnerability Assessment Approach (Department of Homeland Security Office of Risk Management and Analysis and Office of Policy 2011)

(1) This course focuses on a *modified vulnerability assessment* as it applies to surveillance detection.

(2) If you need a *full in-depth vulnerability assessment* of a facility or site, it will require additional time and resources. Work with your Protective Security Advisor (PSA) to complete it.

(3) Hostile surveillants will assess an area broadly to gather information regarding adjacent targets, avenues of approach, etc. The facility security should assess for the same.

(4) Take on the mindset of the hostile surveillant and conduct the vulnerability assessment from the outside looking in.

(a) Conducting the vulnerability assessment from this standpoint allows you to prioritize limited resources and helps you narrow the focus to the vulnerabilities potentially known by the adversary.

(5) The vulnerability assessment, as it applies to surveillance detection, is used to determine:

(a) Facility vulnerabilities

(b) Predictable activity associated with the facility/site, which includes routines, people coming and going, and security rounds

Media 3

4. **Key Considerations in a Vulnerability Assessment** (Ouyang 2012)

   a. **Facility/Site Design.** You should assess several aspects of the facility/site design.

      (1) **Location**

      (2) **Shape**

         (a) The shape of the building can affect the blast effects from an explosion.

      (3) **Number of stories**

         (a) The number of stories may indicate the number of people working inside.

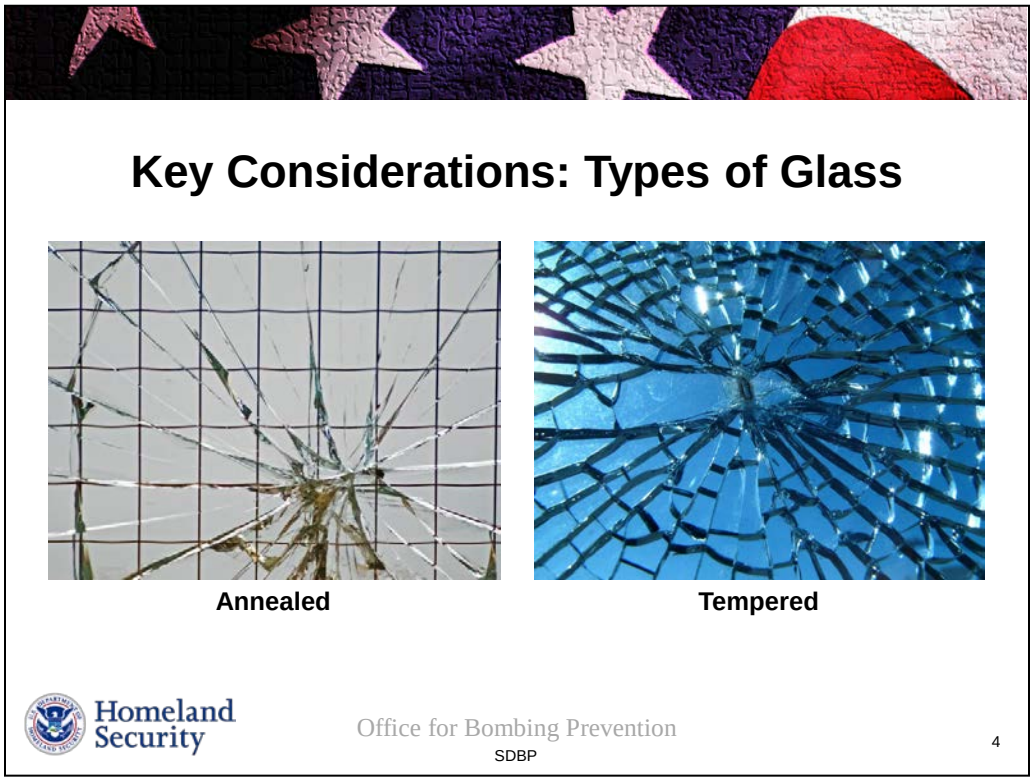
      (4) **Construction material used** (concrete, steel support, fire resistant)

         (a) Concrete and steel are more likely to maintain building integrity.

         (b) The number of column supports and placement can affect the potential for collapse.

      (5) **Opportunities for good cover and concealment**

Media 4



(6) **Types of Glass.** Different types of glass have varying degrees of vulnerability. Glass types include thermoplastic/polycarbonate, laminated, tempered, and annealed.

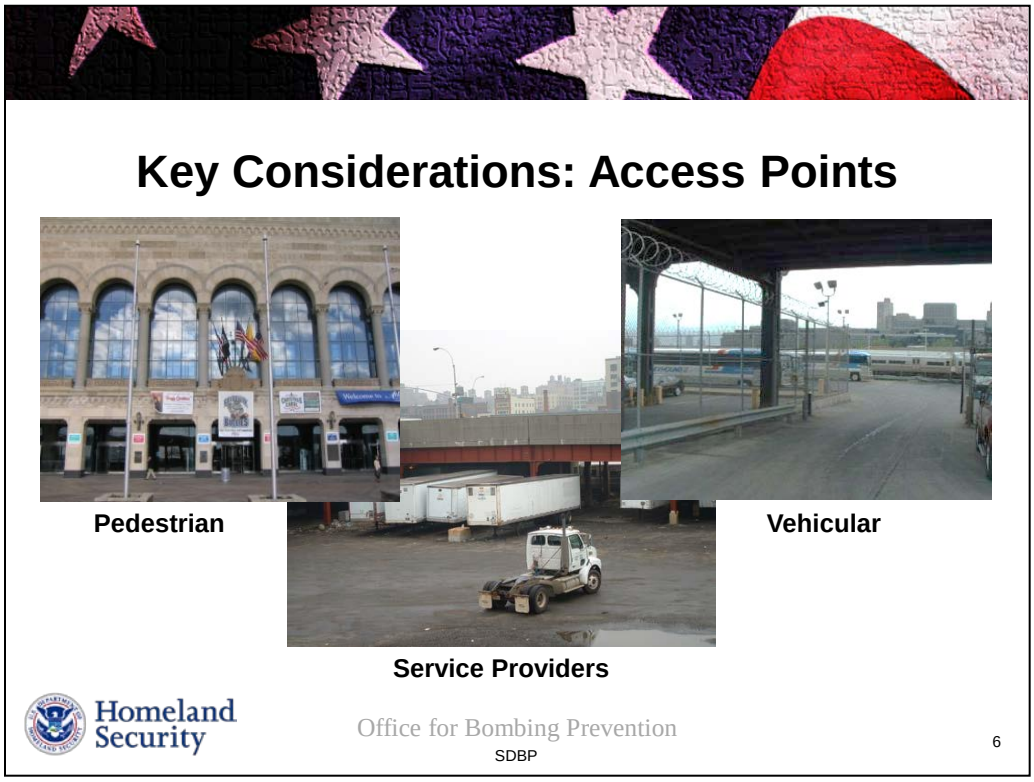
(a) Annealed is the most common type of glass used, but it is the most vulnerable. When broken, it adds sharp pieces of wire in the shards.

(b) Thermoplastic/polycarbonate is the strongest, but it is very expensive. Use of this glass may indicate that the building was built with safety in mind.

Media 5

Take any notes you feel necessary below.

Media 6



b. Access Points. It is important to assess all of the access points to the facility.

(1) **Entry/exit points.** Assess available entry/exit points for pedestrians, vehicles, and service providers (include anyone who needs to access the facility for it to operate, like for maintenance, repairs, or re-supply).

(a) Underground parking/subways that are close or run under/through the site

(b) Opportunities for good cover and concealment

(c) Procedures used at access points

1 Security guards controlling entry and exit

2 Security guards armed or unarmed

3 Vehicle searches conducted

4 Separate entrances for employees

5 Badge system/ID checks

Media 7

(2) **Visitor Access.** Consider supervision of the entry and exit of people who are not part of the facility's staff

Media 8

(3) **Minimized Areas.** These areas will have security measures designed to minimize access/entry of unauthorized personnel through the use of procedures like the following:

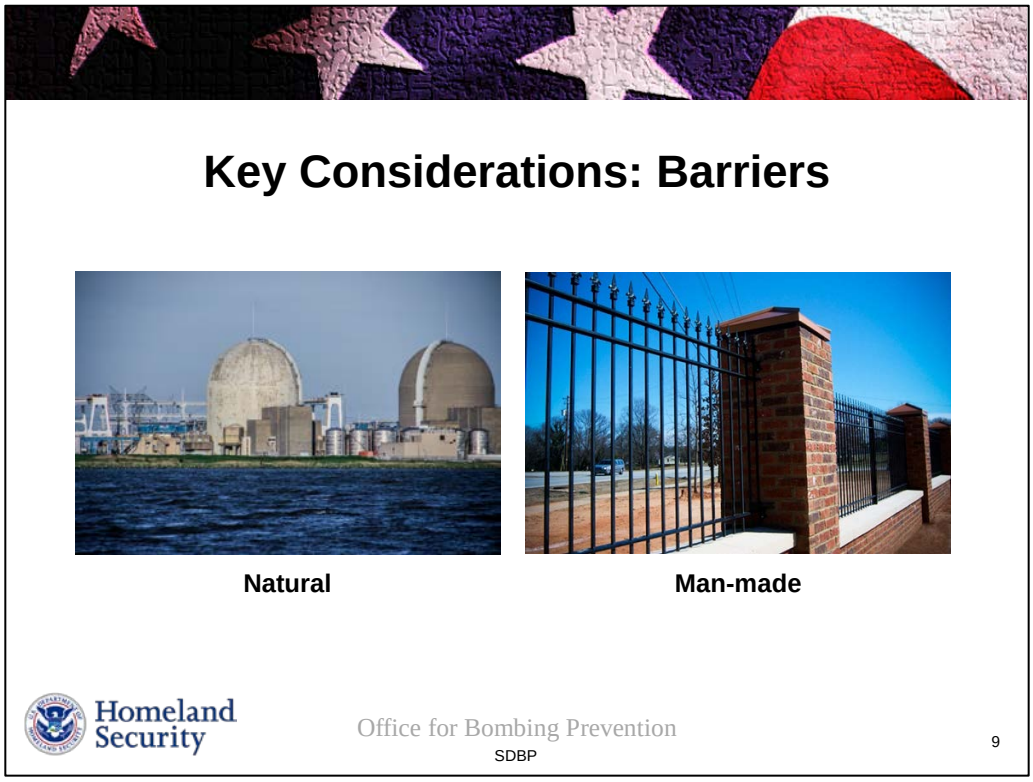
(a) Identification inspection

(b) Bag inspection

(c) Vehicle inspection

(d) Badge identification system

Media 9



(4) **Barriers.** Barriers are solid, joined, or stand-alone physical elements designed and placed to restrict access or improve the safety of a facility. Placement of barriers should consider stand-off distances. They can be natural or man-made.

(a) Natural (e.g., creeks, waterways, cliffs)

(b) Installed (e.g., fences, gates, bollards)

Media 10

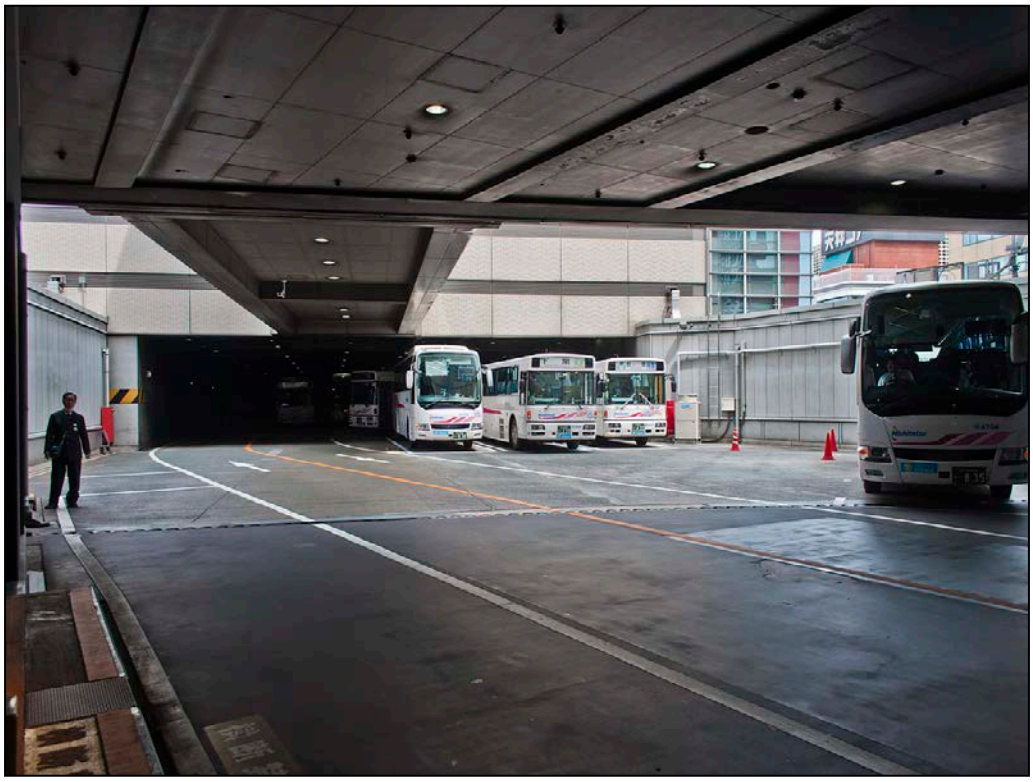
(5) **Uncontrolled Areas.** Uncontrolled areas may provide:

(a) Access to the building or property

(b) Cover or concealment opportunities

(c) Entry and exit

Media 11



Take any notes you feel necessary below.

Media 12

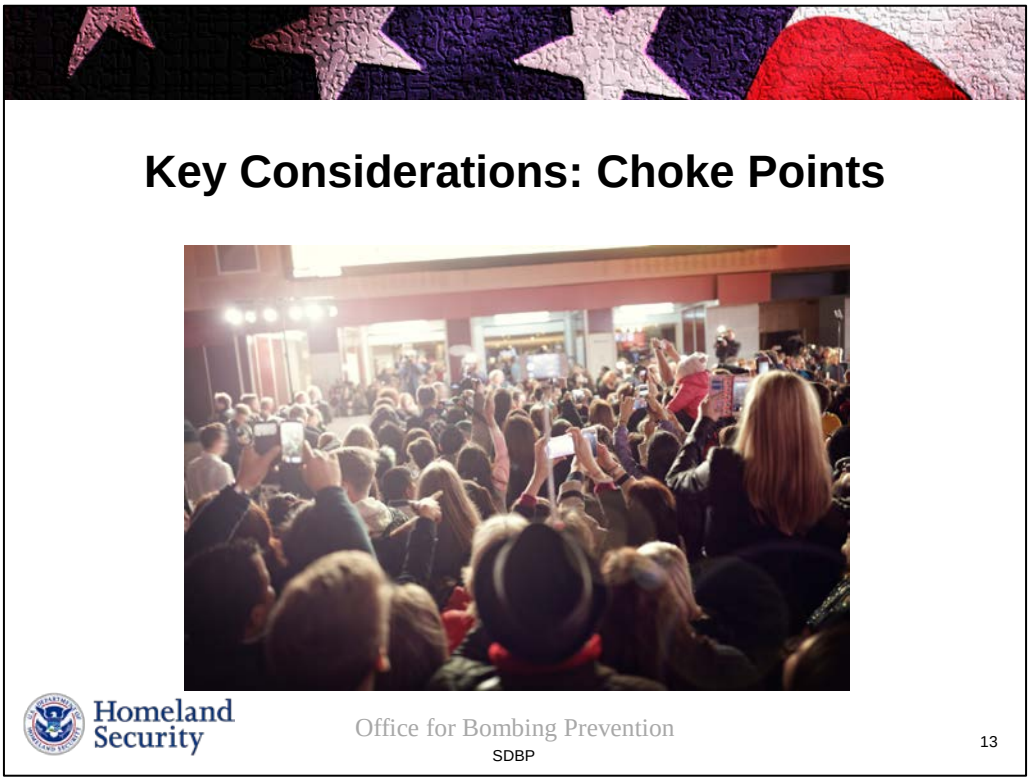
(6) **Areas of Denial.** Areas of denial prohibit access of unauthorized personnel.

(a) Hostile surveillants may park in areas with do not enter/park signs to conduct surveillance.

(b) High fences, key card access gates, and physical security guards decrease the vulnerability of the facility, making it less desirable as a point of entry for attackers.

(c) Hostile surveillants will not draw attention to themselves, so areas of denial are less desirable places to conduct surveillance.

Media 13



(7) **Choke Points.** Entries and exits in buildings become choke points when masses of people are trying to get through them. They are extremely vulnerable and create areas of high injury/fatality potential for an attacker. Examples of significant choke points are arena entrances/exits and limited exits from theaters/clubs.

(a) **Clearly Marked Evacuation Routes.** Evacuation routes that are clearly marked may also become a logical site for a secondary device.

Media 14

(8) **Mass Gathering Points**

(a) Mass gathering points in or near a facility or at an event create the potential for several vulnerabilities.

(b) Examples of mass gathering points include transportation centers, public events, concerts, and stadium events.

Take any notes you feel necessary below.

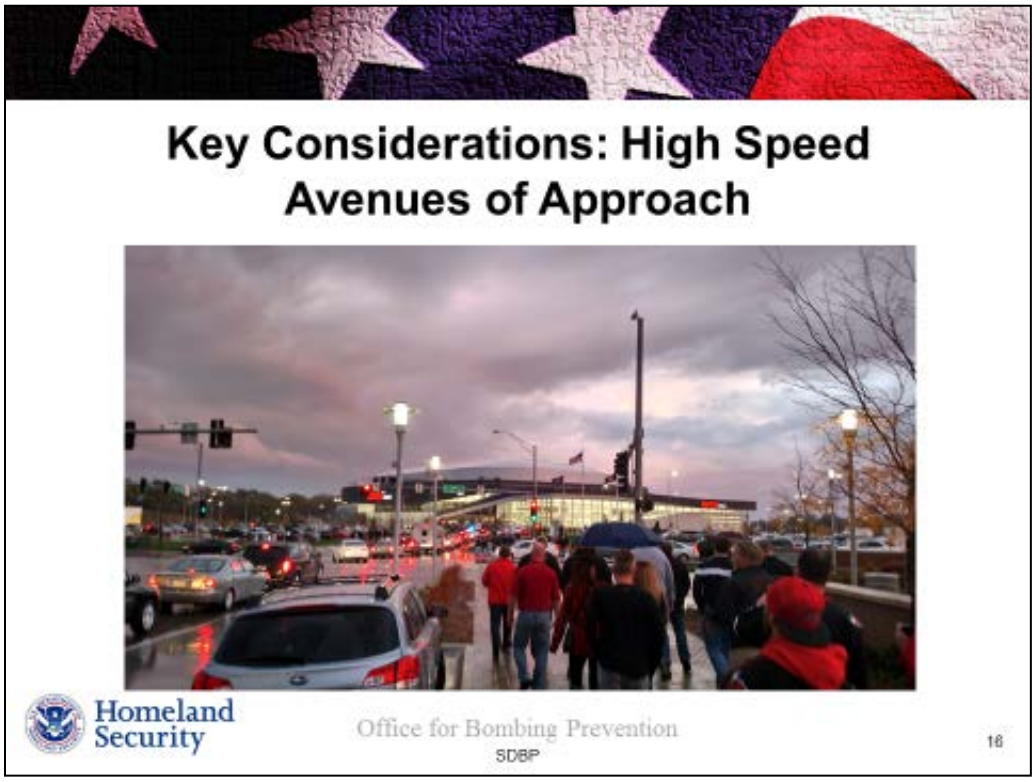
Media 15

c. Closed Circuit Television

(1) It can have fixed or pan, tilt, zoom (PTZ) cameras.

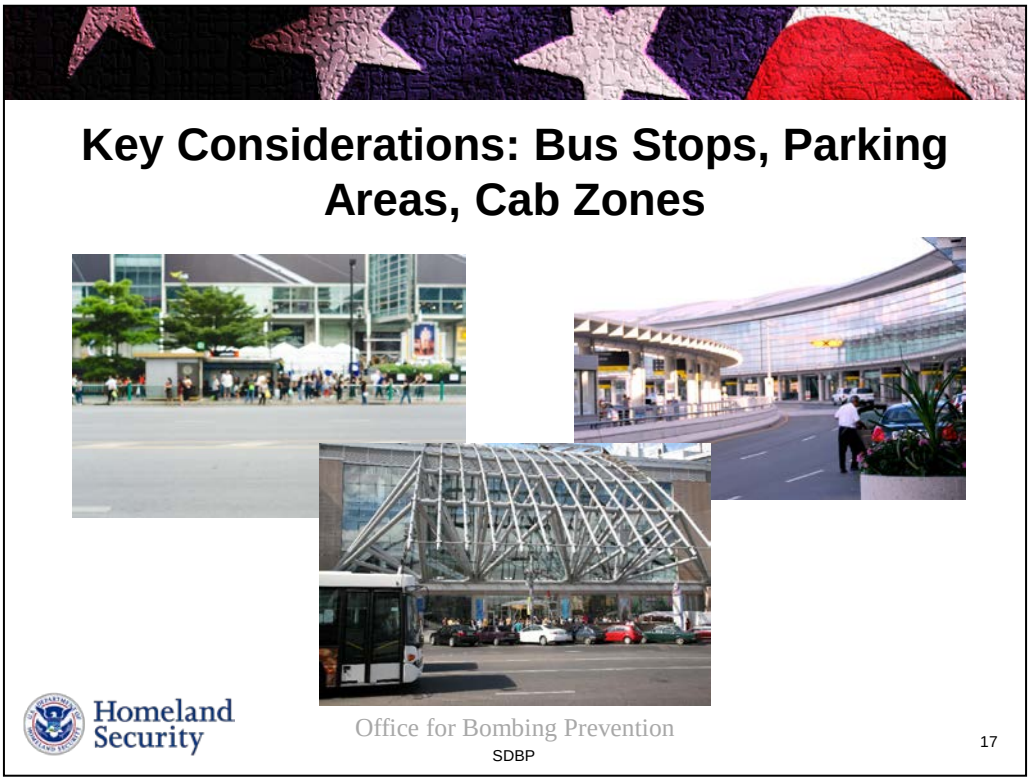
(2) If it goes unmonitored, it makes the facility more vulnerable.

Media 16



d. High Speed Avenues of Approach. Be aware of paths vehicles can take to strike a target (e.g., people or a facility) at a high rate of speed without barriers in the way.

Media 17



e. Bus Stops, Parking Areas, Cab Zones. These locations can be vulnerabilities for attack as well as possible locations for hostile surveillants to surveil and gather intelligence.

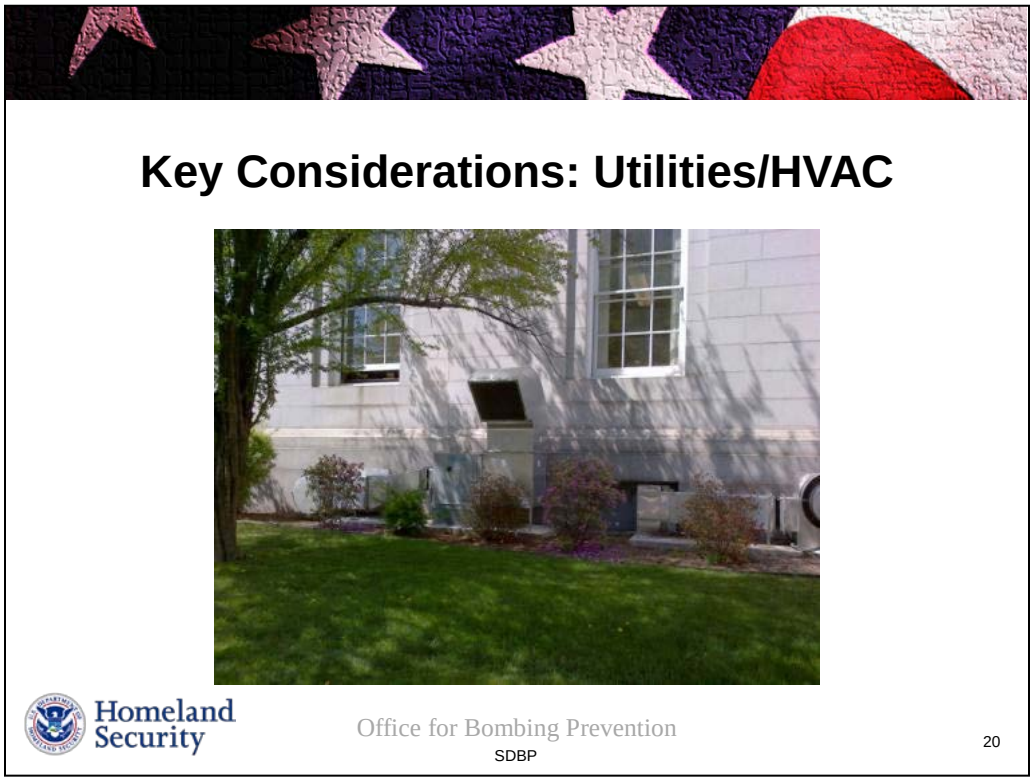
Media 18

f. Location of Benches and Seating. These locations can be vulnerabilities for attack as well as possible locations for hostile surveillants to surveil and gather intelligence.

Media 19

g. Location of Trash Cans. Trash cans can be used to conceal improvised explosive devices (IEDs) and add shrapnel to the explosion. In particular, look for trash can locations near places where people gather or enter or exit a facility.

Media 20



h. Utilities/HVAC

Take any notes you feel necessary below.

Media 21

Key Considerations: Other Vulnerabilities

- Presence and use of security and law enforcement
- Predictable site activity
- Hours of operation
- Upcoming events
- High media coverage areas

Homeland Security

Office for Bombing Prevention

SDBP

21

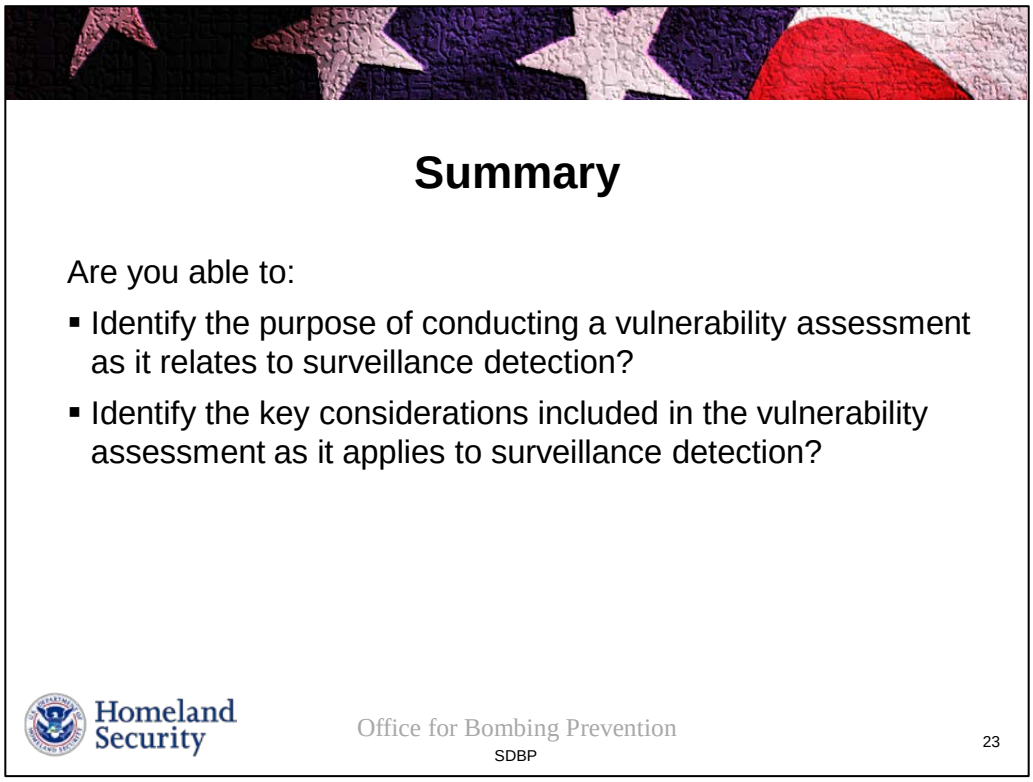
Media 22

Take any notes you feel necessary below.

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 23

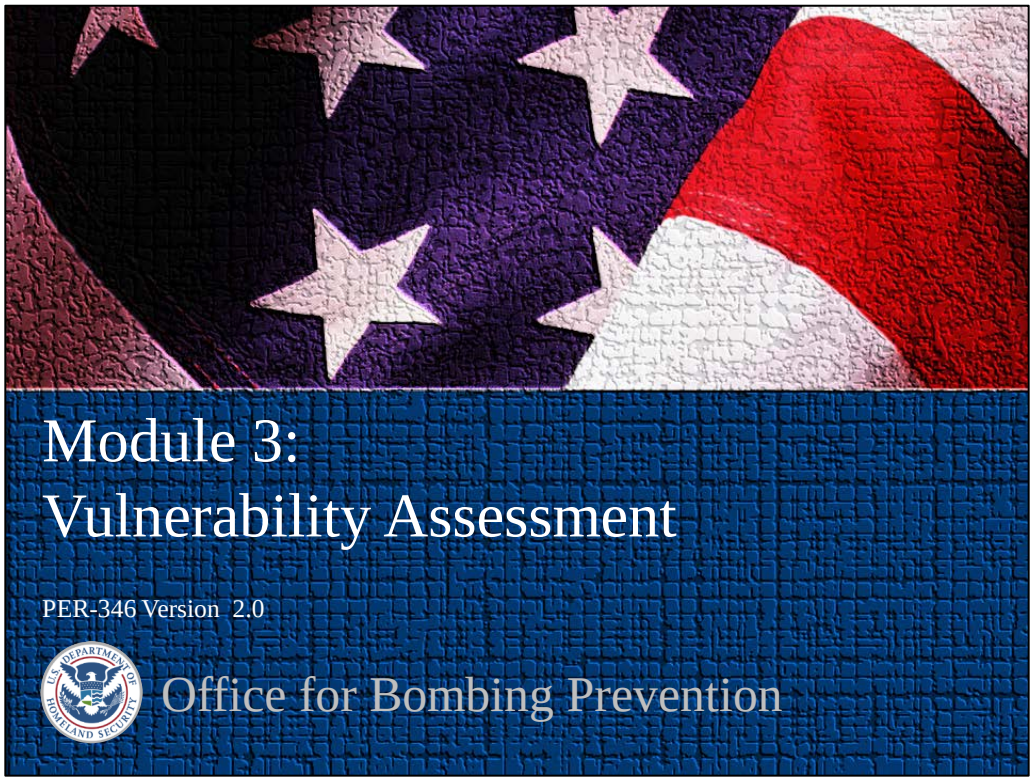


5. **Summary.** This module introduced you to the steps involved in the vulnerability assessment of a facility, system, or event as it applies to surveillance detection. Are you able to:

   a. Identify the purpose of conducting a vulnerability assessment as it relates to surveillance detection?

   b. Identify the key considerations included in the vulnerability assessment as it applies to surveillance detection?

Media 24


Module 3:
Vulnerability Assessment
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

Department of Homeland Security Office of Risk Management and Analysis and Office of Policy. 2011. "Risk Management Fundamentals." *Department of Homeland Security.* April. Accessed 31 2017, July. https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

Ouyang, A. 2012. *CISSP Common Body of Knowledge Review: Physical (Environmental) Security Domain Version: 5.9.* March 4. Accessed July 31, 2017. https://www.slideshare.net/aouyang/6-physical-security.

Module 3
Supplemental Materials

This page is intentionally left blank.

Modified Vulnerability Assessment Checklist

Use this checklist as a reference to ensure you are making notes and observing items in every vulnerability assessment category.

Facility/Site Design

- Location
- Shape
- Number of stories
- Construction material used
- Type of glass

Access Points

- Entry/exit points
- Opportunities for good cover and concealment
- Any procedures used at access points
- Minimized areas
- Barriers
- Uncontrolled areas
- Areas of denial
- Choke points
- Mass gathering points

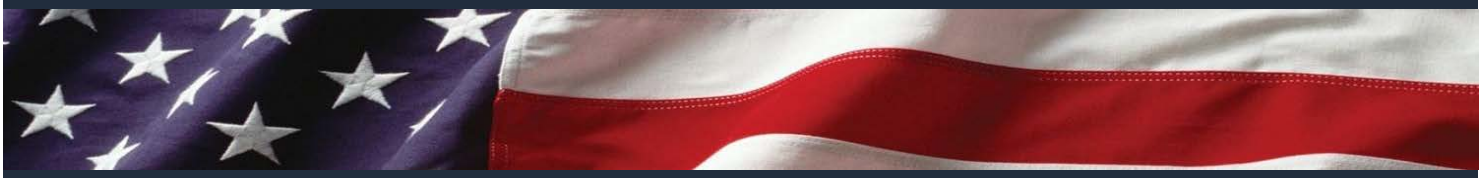
Closed Circuit Television

- Fixed or pan-tilt-zoom (PTZ)
- Observations on whether cameras are monitored

Other Vulnerabilities Noted

- High speed avenues of approach
- Bus stops/parking areas/cab zones
- Location of benches and seating
- Location of trash cans
- Utilities/Heating, ventilation, and air conditioning (HVAC) systems
- Presence and use of security and law enforcement
- Predictable activity associated with the facility/site
- Hours of operation
- Upcoming events
- High media coverage areas

This page is intentionally left blank.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Experiential Learning Guide Activity 1: Vulnerability Assessment Activity

Participant Workbook

This page is intentionally left blank.

Number: Experiential Learning Activity (ELA) 1

Title: Vulnerability Assessment Activity

Purpose. The purpose of this activity is to provide an opportunity to apply the procedures for conducting a vulnerability assessment of a facility as it applies to surveillance detection.

Learning Objectives

a. **Terminal Learning Objective.** Given an assigned facility, participants will identify the vulnerabilities of that facility in accordance with the key considerations provided in class. (SD-0210)

b. **Enabling Learning Objectives**

(1) Given an assigned facility, participants will work as a team to communicate identified vulnerabilities. (SD-0210a)

(1) Given an assigned facility, participants will draw a schematic of that facility in black on an easel pad. (SD-0210b)

(2) Given an assigned facility, participants will mark the identified vulnerabilities on their schematic in another color. (SD0201c)

Learning Event Description. During this learning event, you will conduct a vulnerability assessment on an assigned facility.

Activity Instructions

a. Team leaders can conduct the facility vulnerability assessment however they want (e.g., assign specific steps to each team member, assign team members specific areas to assess different categories, etc.).

b. You can use Module 3 Handout 1: Modified Vulnerability Assessment Checklist to ensure you assess all categories.

c. You can support the assessment with photographs, sketches, and drawings.

d. You have three hours to complete the vulnerability assessment. The three hours includes lunch and travel time.

e. Before going out to the field, you need to complete an open source search and information gathering on the target location.

f. Upon returning to the classroom, you will draw a schematic of the facility in black on an easel pad and identify the vulnerabilities of your assigned facility in green. You will have 30 minutes to complete your schematic.

g. Select a spokesperson to report out to the class.

SAFETY BRIEF

Risk Assessment: Moderate. This activity involves controlled practical application requiring substantial exertion. Moderate risk exists for injury to personnel or damage to equipment.

Safety Precautions and Control Measures

a. Physiological stressors such as exertion, heat, cold, or hydration may have significant effects upon some individuals. If you or a fellow participant experience adverse physiological effects, inform an instructor immediately.

b. Psychological stressors may have significant effects upon some individuals. If you or a fellow participant experience adverse psychological effects, inform an instructor immediately.

Cease Training Procedures. If at any time an instructor or participant feels that an unsafe condition exists during an activity, an individual may request for training to stop by contacting the team leader who will contact the instructor. The instructor will assess the situation. The instructor will not commence training until an identified unsafe situation has been resolved and/or appropriate control measures have been implemented to mitigate the risk.

Participant Responsibility for Activity Safety. Along with the instructors and staff, each participant is also responsible for the safety of the activity.

a. Participant Responsibility for Activity Safety

(1) Be vigilant in your observance of safety precautions and associated control measures, and bring any potential concern to the attention of the nearest instructor or staff member as soon as observed.

(2) If a fellow participant or a staff member needs assistance, please aid him/her to the best of your ability without inappropriately risking your own health and/or safety until designated personnel arrive.

(3) You have the option to not participate in a training event if you feel you are physically or emotionally unable to perform the designated actions or skills. Immediately notify an instructor should you have concerns about participating in a training event.

(4) A participant may be prohibited from participating in a training event if perceived by any staff member as being physically and/or cognitively impaired by drugs, alcohol, or other substances.

b. Safety Takes Priority Over Activity Events

(1) If directed by an instructor or other designated personnel to stop training, evacuate an area, assist a staff member or participant, etc., immediately do so to the best of your ability. The safety of all personnel will take priority over the training activity.

(2) If you sense yourself or others becoming overly fatigued, dehydrated, or otherwise compromised to an unsafe extent, contact an instructor and mitigate the situation as soon as possible.

Inclement Weather. In the event of inclement weather, such as excessive heat or cold, tornadoes, thunderstorms, etc., safety protocols may determine changes in training activities and their locations. This practice is to ensure the safety of all participants and provide a safe environment to complete event objectives.

Hazards. Due to the unique training environment, there may be a wide array of walking/working surfaces and hazards. All participants must be aware of hazards that may cause slips, trips, falls, collisions, etc. within the training area. Any participant identifying a hazard requiring mitigation should notify an instructor.

Participant Behavior. Aggressive behavior will not be tolerated during the event. Examples of aggressive behavior may include hostile communications, excessive use of force, or inappropriate use of response equipment.

Additional rules for the activity are included in the Threat Portfolio Briefing. These include:

a. Never enter your assigned facility through illegal or deceptive means.

b. Conduct all activities within the public areas of the facility only, and do not disrupt operations at the facility.

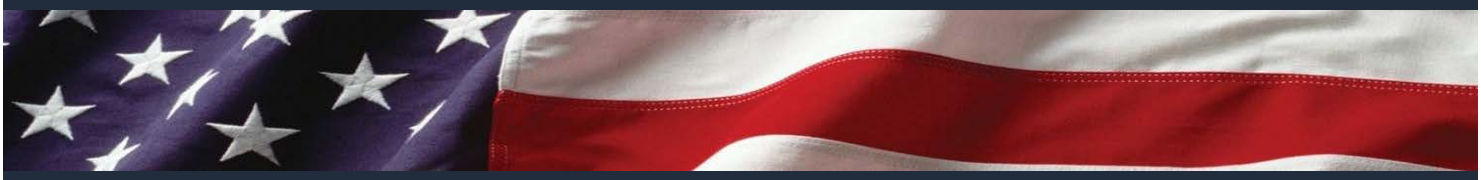
c. Do not engage or otherwise alert potential hostile surveillants to surveillance detection (SD) efforts in area unless presented with exigent circumstances (disrupt an attack, prevent loss of life, etc.).

d. Do not overtly engage or otherwise communicate with contracted security personnel, employees, law enforcement officers (LEOs), or other SD team members (unless it is part of your cover).

e. If you experience any emergency (medical or criminal), contact 911, then contact the instructor.

f. Follow established agency/department policy if you encounter illegal activity.

This page is intentionally left blank.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 4: Hostile Surveillance Requirements

Participant Workbook

This page is intentionally left blank.

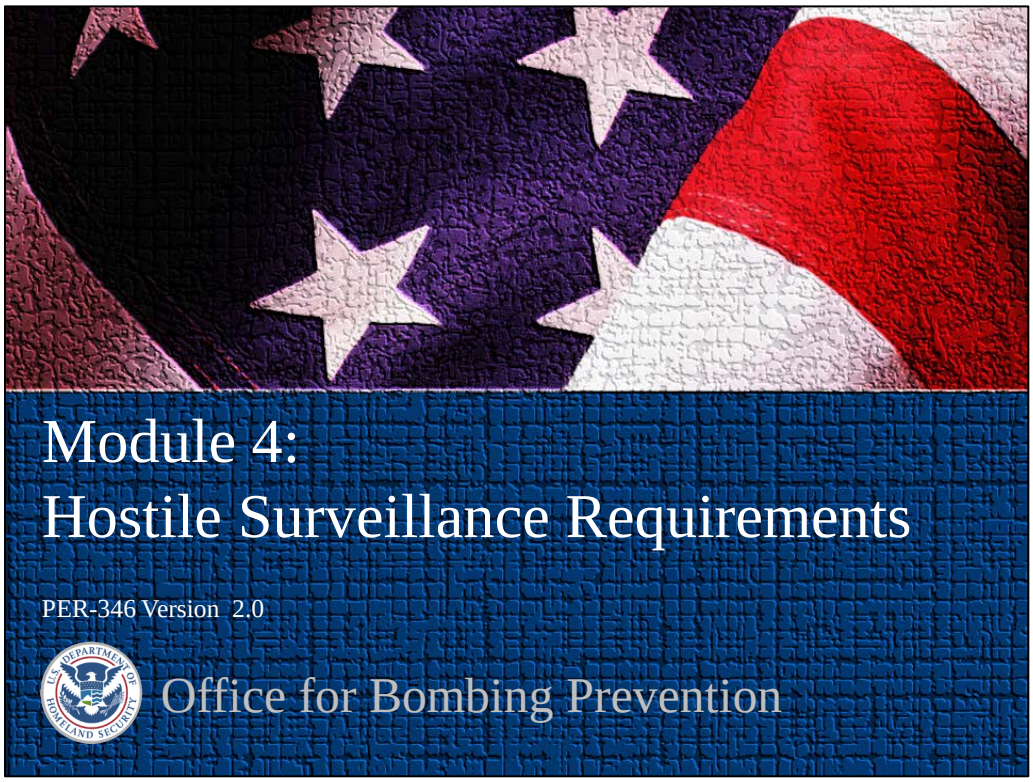
Number: Module 4

Title: Hostile Surveillance Requirements

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 4: Hostile Surveillance Requirements. The purpose of this module is to introduce the requirements for hostile surveillance including the Red Zone and hostile surveillance positions.

2. **Learning Objectives**

   a. **Terminal Learning Objective.** Given a written examination, participants will describe the three major requirements for hostile surveillance of a facility according to the guidelines provided in class. (SD-0110)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will describe the Red Zone of a facility to achieve a minimum score of 70%. (SD-0110a)

(2) Given a written examination, participants will define hostile surveillance positions to achieve a minimum score of 70%. (SD-0110b)

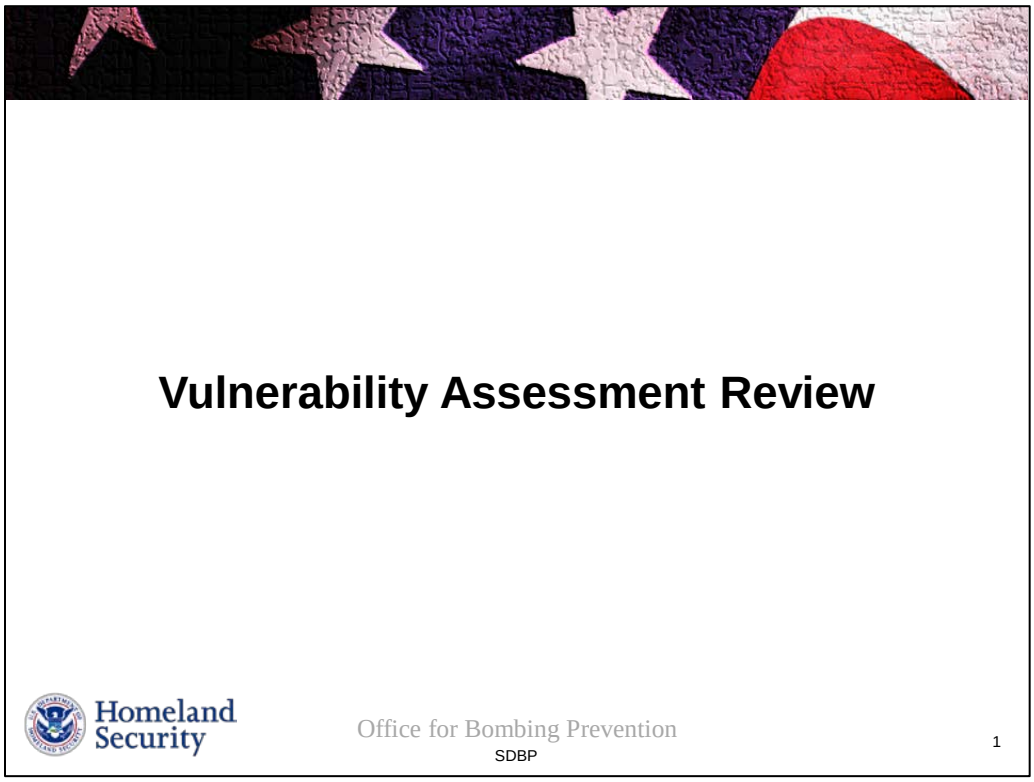
(3) Given a written examination, participants will describe the requirements for adequate cover and concealment to achieve a minimum score of 70%. (SD-0110c)

(4) Given a written examination, participants will describe the parameters for logical entry and exit to achieve a minimum score of 70%. (SD-0110d)

BODY

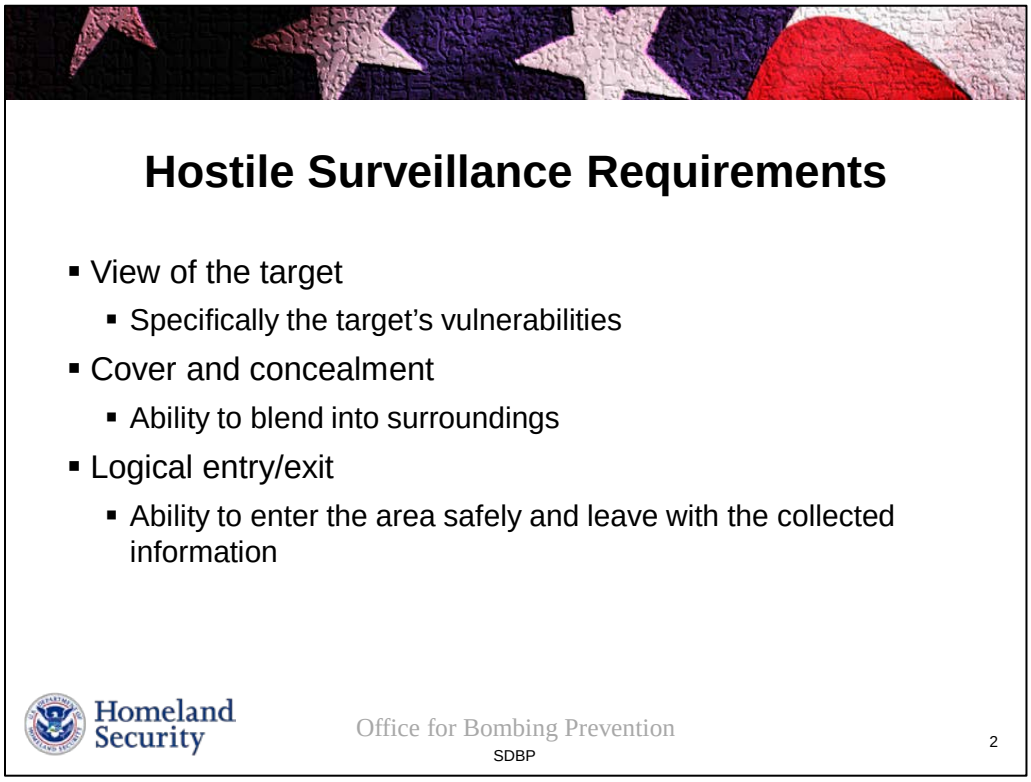
LECTURE/DISCUSSION ***40 minutes*** ***1:20***

Media 1



Take any notes you feel necessary below.

Media 2



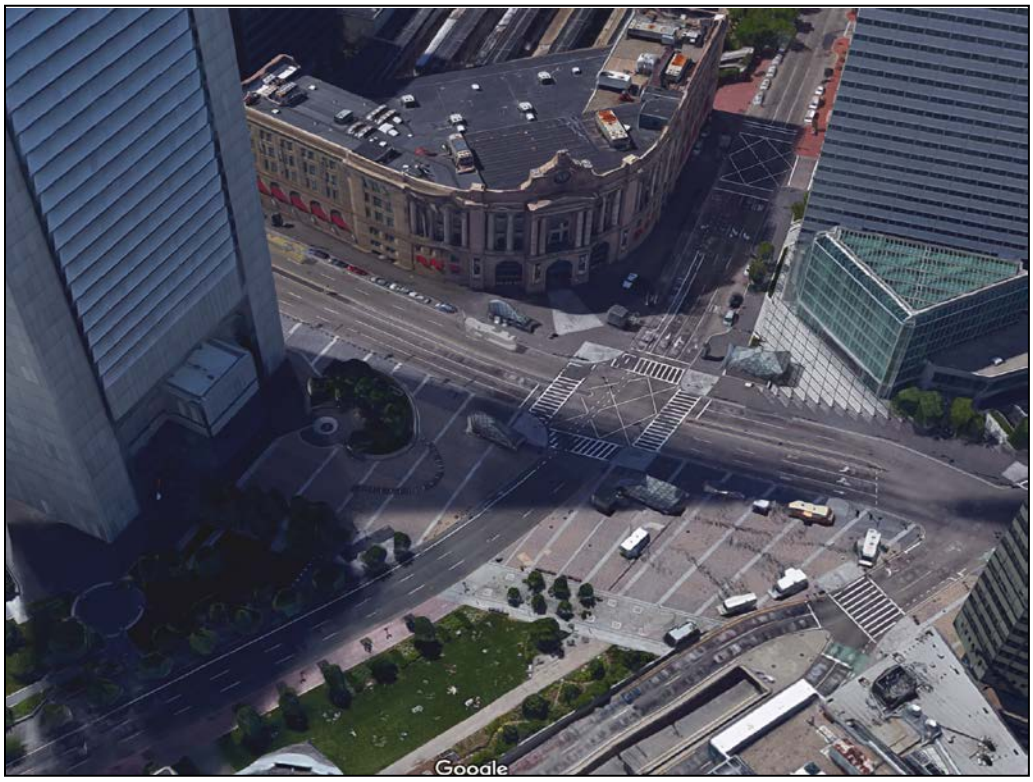
3. **Hostile Surveillance Requirements.** To gain knowledge regarding a target, the hostile surveillant requires:

   a. **View of the target**, specifically the target's vulnerabilities.

   b. **Cover and concealment** to blend into the surroundings.

   c. **Logical entry/exit** to enter the area safely and leave with the collected information.

Media 3

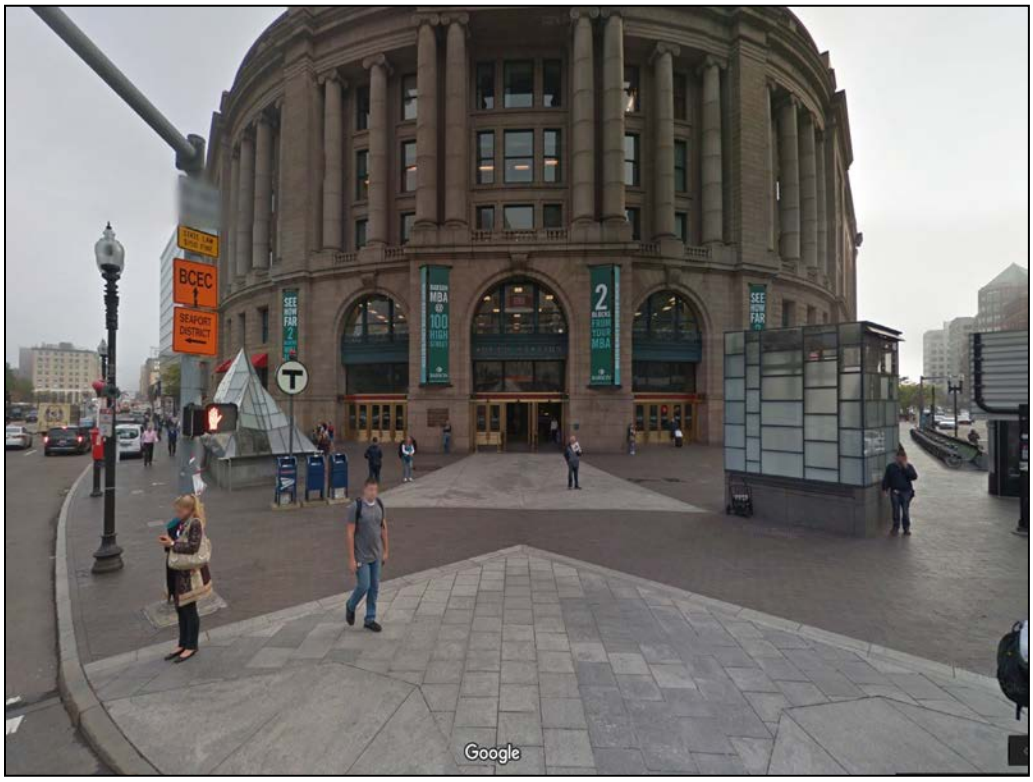


4. **View of the Target.** The hostile surveillant needs an unobstructed, line-of-sight view of the target's vulnerabilities from his/her surveillance position to collect information.

Take any notes you feel necessary below.

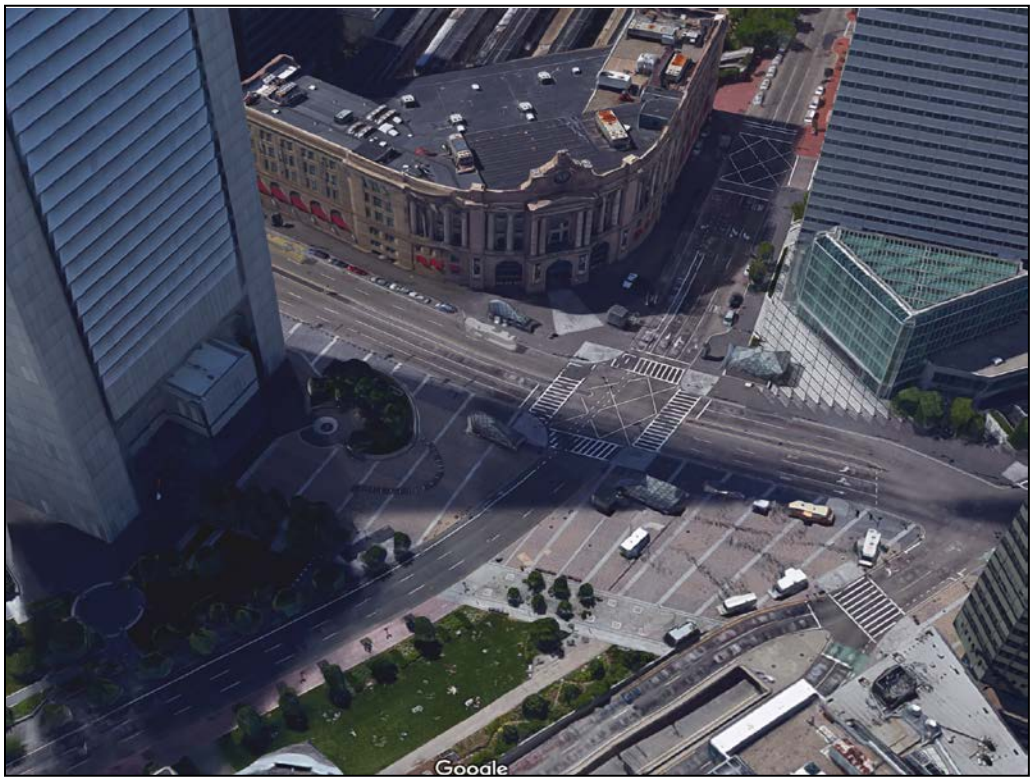
_____
_____
_____
_____
_____
_____
_____

Media 4



Take any notes you feel necessary below.

Media 5



Take any notes you feel necessary below.

Media 6

View of the Vulnerability

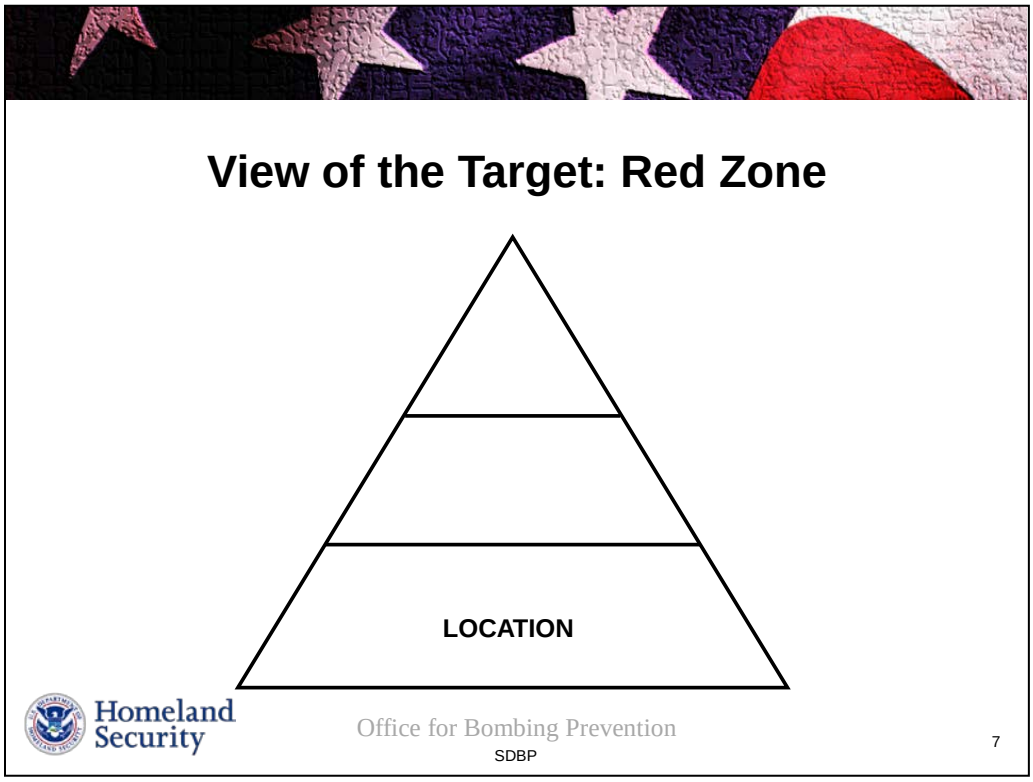
Homeland Security

Office for Bombing Prevention

SDBP

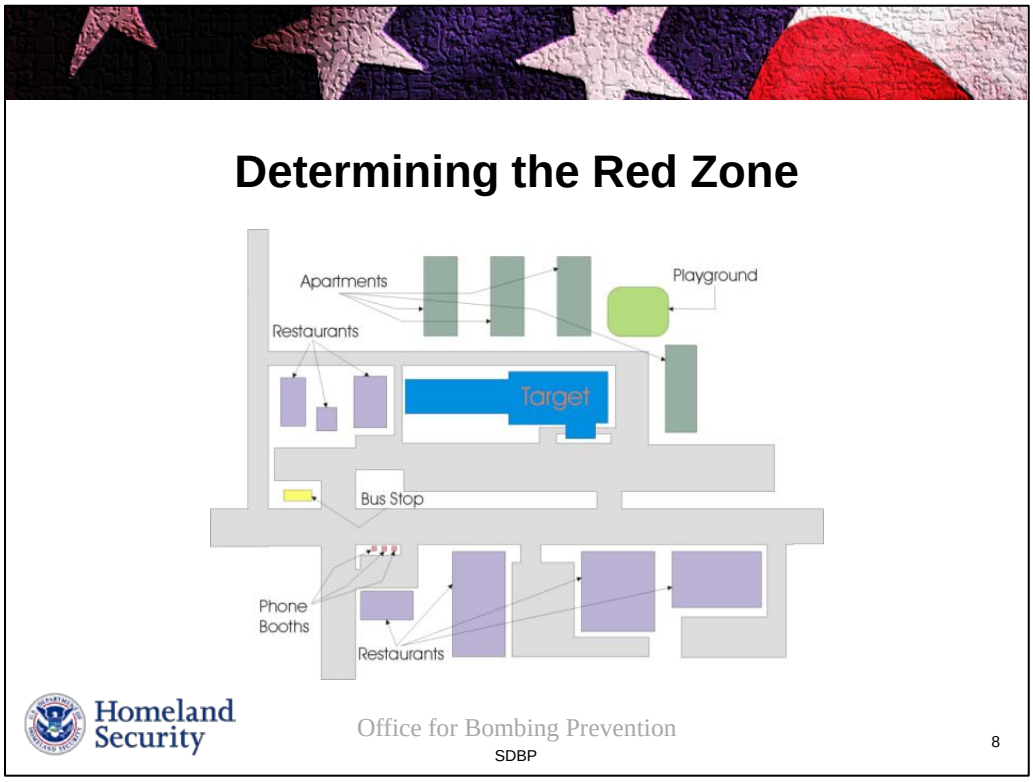
6

Media 7

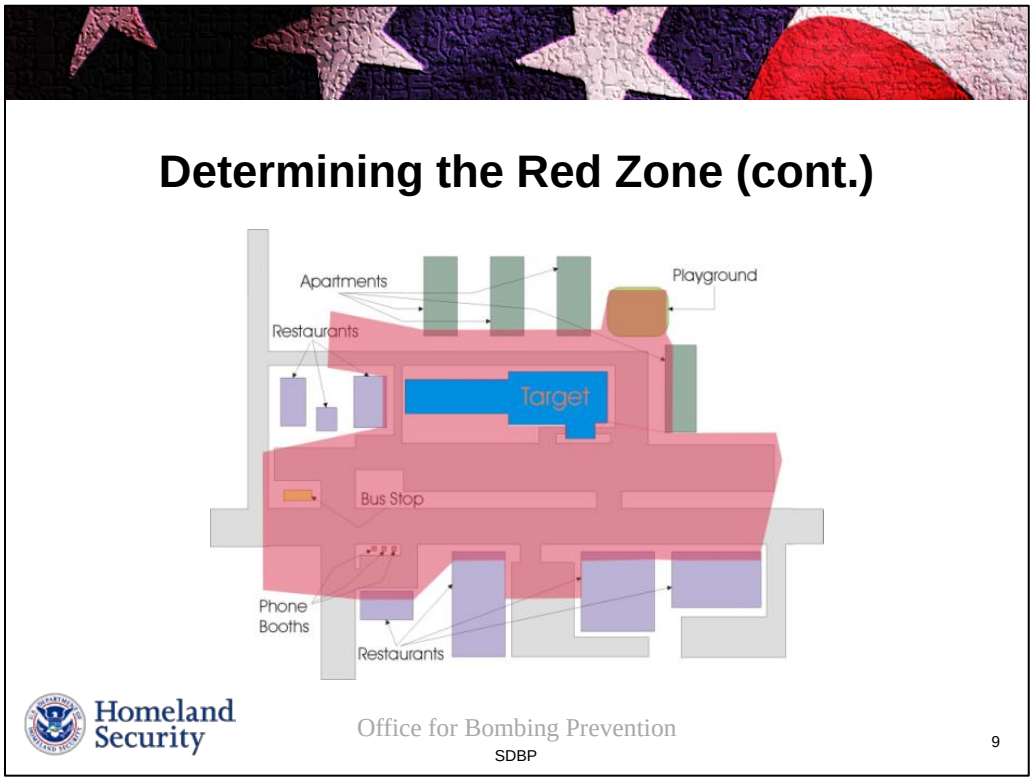


a. View of the Target: Red Zone. The Red Zone is the bottom level of the surveillance detection pyramid: Location. The Red Zone is defined as anywhere you can see the target.

Media 8

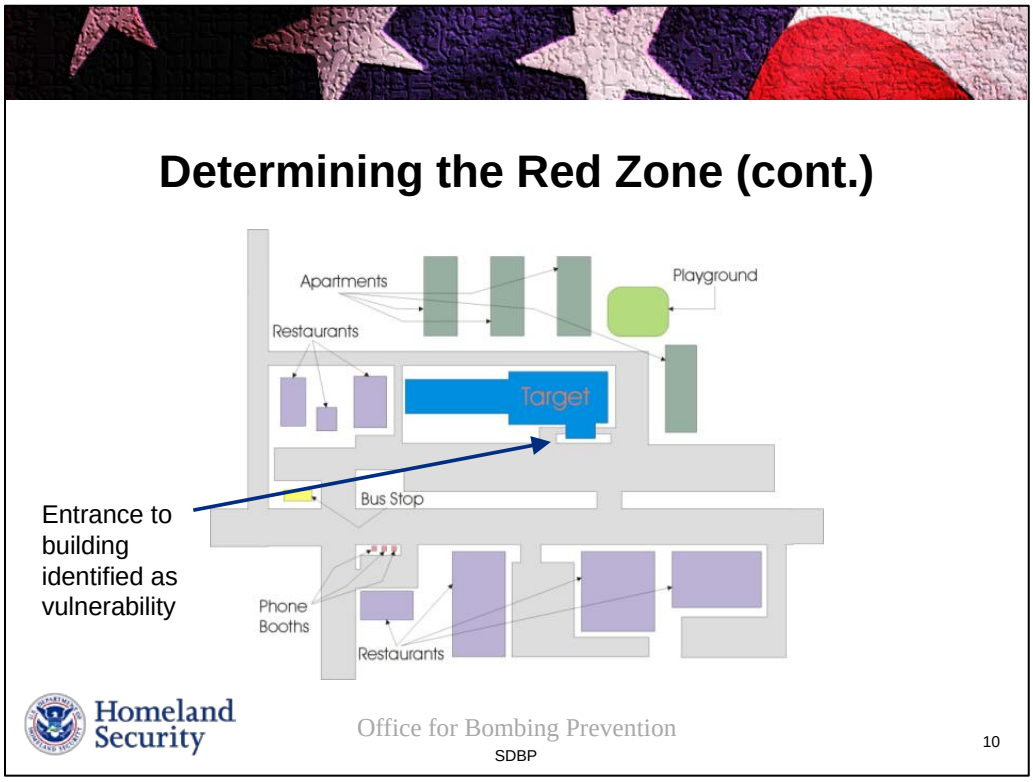

Determining the Red Zone
Apartments
Playground
Restaurants
Target
Bus Stop
Phone
Booths
Restaurants
Homeland
Security
Office for Bombing Prevention
SDBP
8

Media 9



Take any notes you feel necessary below.

Media 10



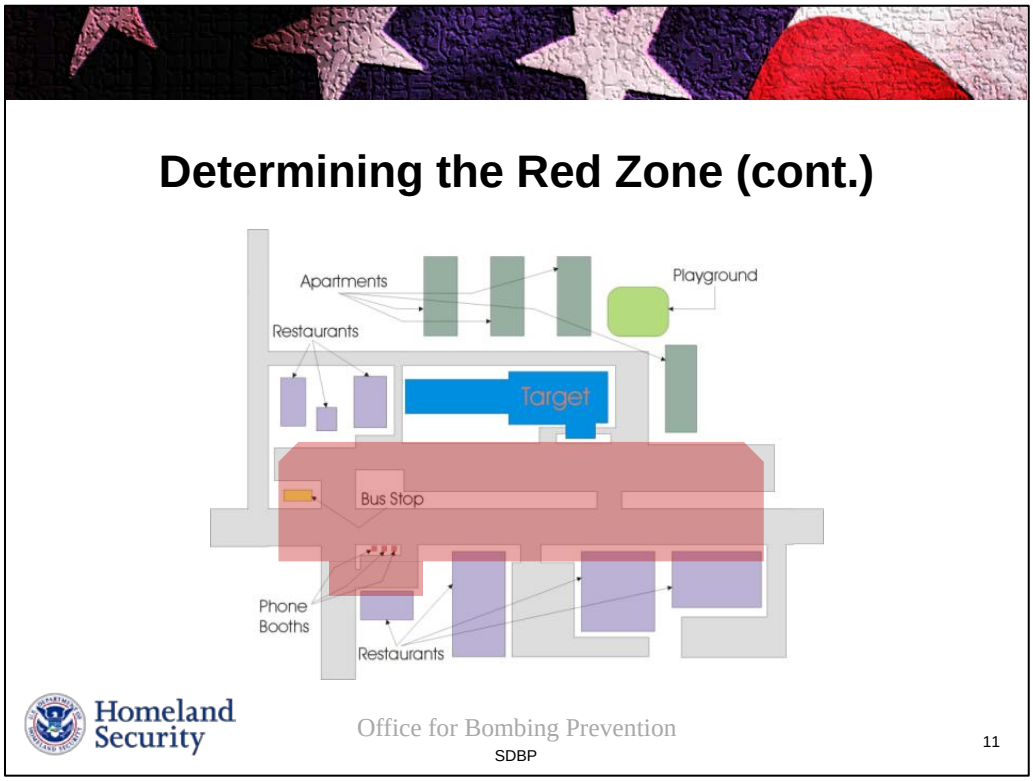
b. Assessment of the Red Zone. The assessment of the Red Zone goes from a broad assessment to a more narrow assessment, based on the view of the target vulnerability.

Each vulnerability at a facility has its own red zone.

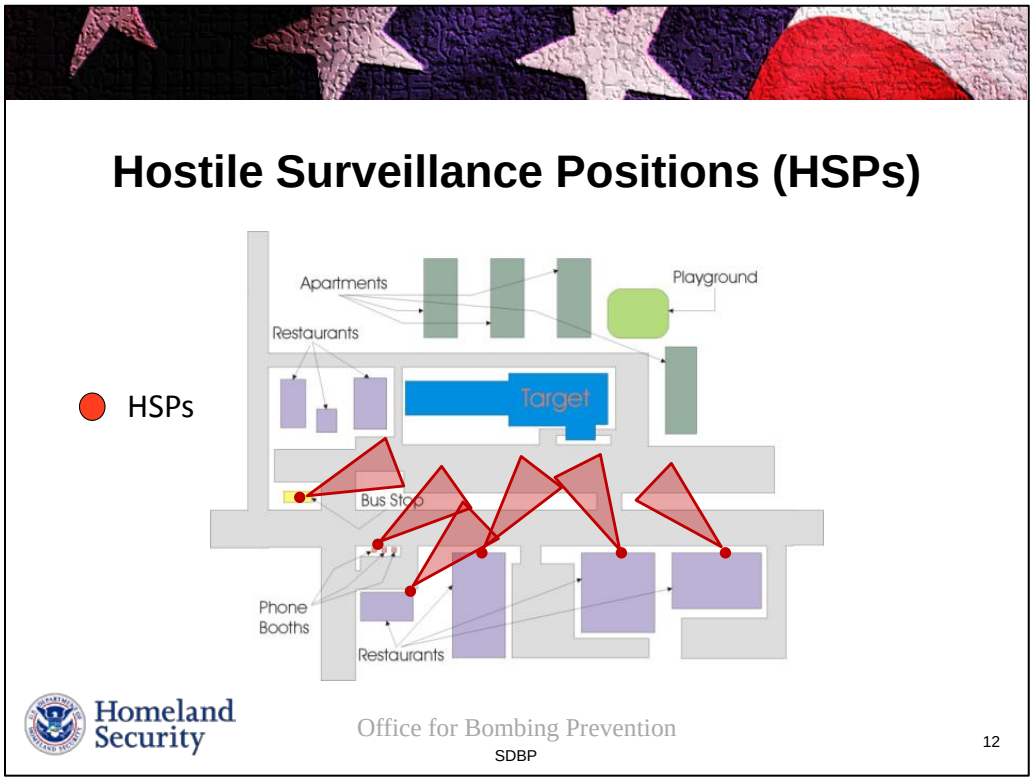
Take any notes you feel necessary below.

_____
_____
_____
_____
_____
_____
_____

Media 11


Determining the Red Zone (cont.)
Apartments
Playground
Restaurants
Target
Bus Stop
Phone
Booths
Restaurants
Homeland
Security
Office for Bombing Prevention
SDBP
11

Media 12



c. **Hostile Surveillance Positions (HSPs).** There are only certain places that make sense to view the target's vulnerabilities. Therefore, HSPs are specific locations, usually providing cover and/or concealment, which can be used to perform surveillance on the target's vulnerabilities, avenues of approach, and nearby activities that may aid in planning/carrying out an attack.

(1) HSPs are narrowed by identifying the target's vulnerabilities.

(2) HSPs are points within the Red Zone that provide a clear line of sight to the target's vulnerability. If the view is blocked, there are fewer positions available to surveil the vulnerability.

(3) HSPs must also support a cover story, both the type of cover and the time needed to support the cover story.

Determining HSPs is the second element of the surveillance detection plan.

Take any notes you feel necessary below.

_____
_____
_____
_____
_____
_____
_____

Media 13

Take any notes you feel necessary below.

Media 14

5. **Cover and Concealment.** Once the HSP is identified, the surveillant needs to remain undetected to conduct effective surveillance. The hostile surveillant must be able to blend into the surroundings.

   a. Cover means to conceal something illicit from notice. The cover needs to be accurate, thorough, and believable for the position the surveillant assumes. Good cover is researched by the surveillant to blend into the surroundings and not stand out.

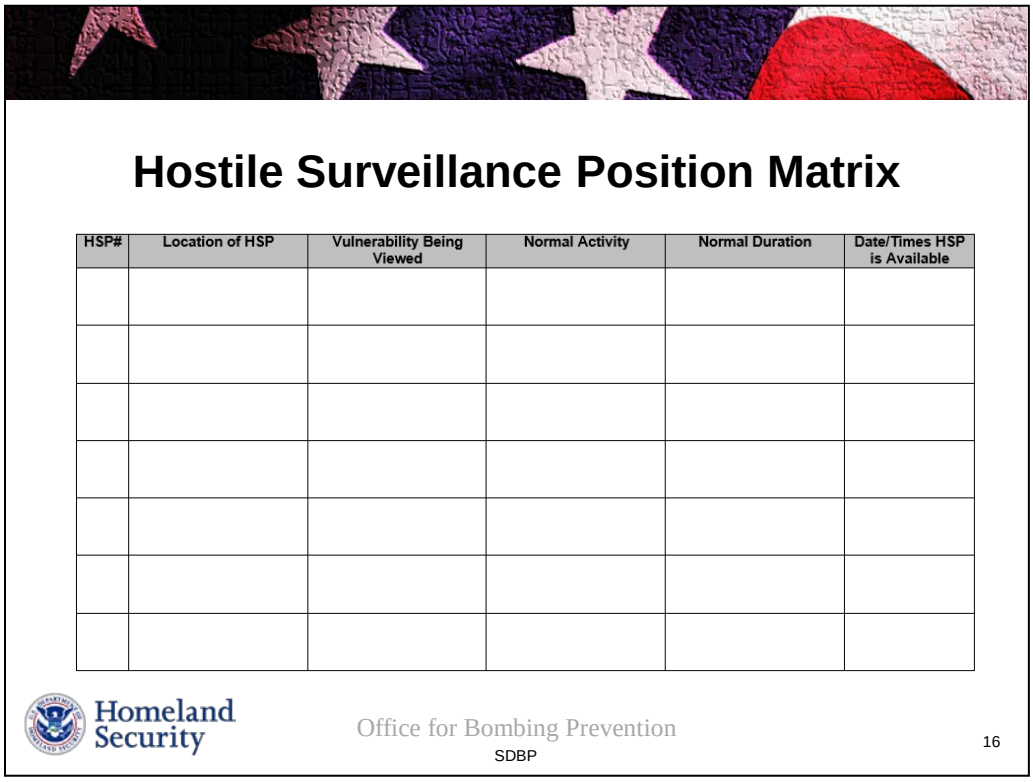
   b. The hostile surveillant needs cover for action. Cover for action means establishing a plausible reason for being or doing something in a particular location and for remaining in that place for extended periods of time.

Media 15

6. **Logical Entry and Exit.** The reason for entering/exiting a facility should be logical and not draw attention. The surveillant needs to blend into the crowd and enter and exit through authorized areas. It should not require any kind of secretive action. It also needs to align with the surveillant's cover. This may include unmonitored entry and exits, such as a subway or train station.

   The logical entry and exits should be documented in the surveillance detection plan since they are not going to change.

Media 16



7. **HSP Matrix.** The HSP matrix is a tool that should be a part of all surveillance detection plans. The purpose of the matrix is to keep information on potential hostile surveillance all in one place. This provides a summary of the history of various HSPs for all the members of the surveillance detection team to reference and analyze. Relevant observed activity and information should be added to the matrix during each surveillance detection shift. Ongoing surveillance based on repeated entries may help to determine if a surveillant may be part of a cell of attackers or is a lone wolf, or it may help to identify the primary vulnerability of a target. The matrix can also serve as a training resource for new personnel, as it provides a road map of where the HSPs are located and what has transpired in the past. This allows new personnel to acclimate much quicker.

   The HSP matrix should include:

   a. **HSP number and location of HSP.** Each location should be given a number. The locations in relationship to given vulnerabilities and numbers need to be identified in the surveillance detection plan so new people know where they are.

   b. **Vulnerability being viewed.** Describe the vulnerability that can be viewed. Examples include gates, service entrances, or a main entrance.

   c. **Normal activity.** Record activities that are normal for that location. For example, if a restaurant, record how long people normally stay and eat

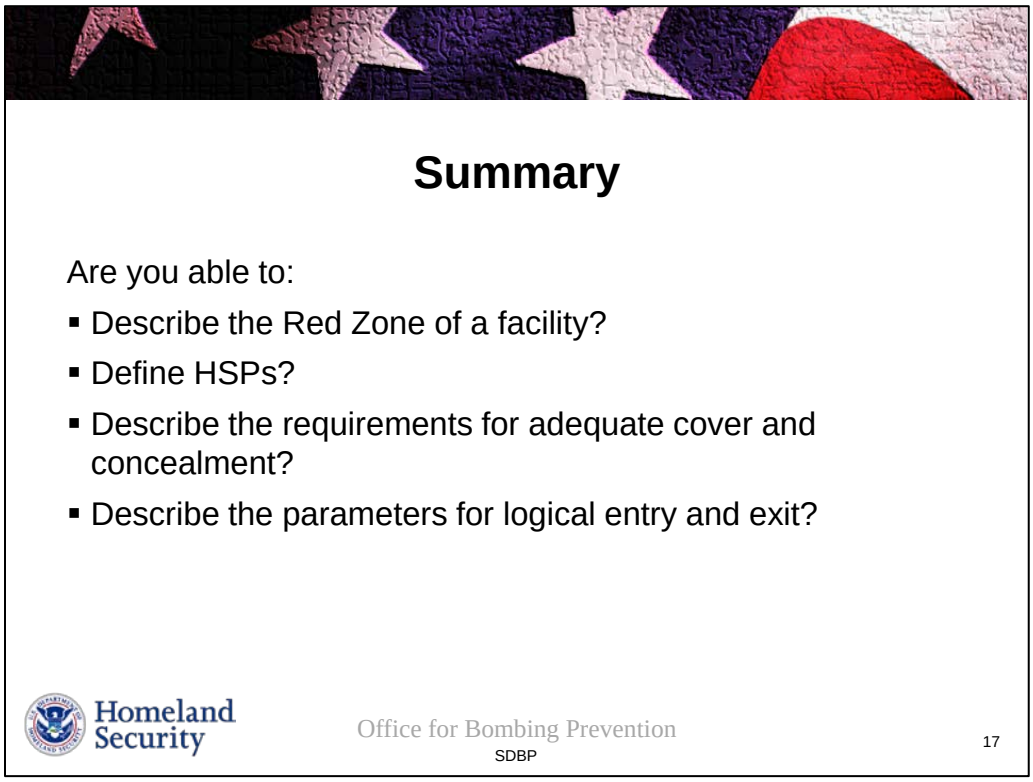
   d. **Normal duration.** Record how long people normally stay in that location. For example if a restaurant, a normal duration is probably an hour to an hour and 15 minutes.

e. **Dates/Times HSP is available.** Record the normal hours of operations of the vulnerability. For example, a restaurant may only be open from 11:00 AM to 10:00 PM.

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 17



8. Summary. This module served to introduce you to the requirements for hostile surveillance. Are you able to:

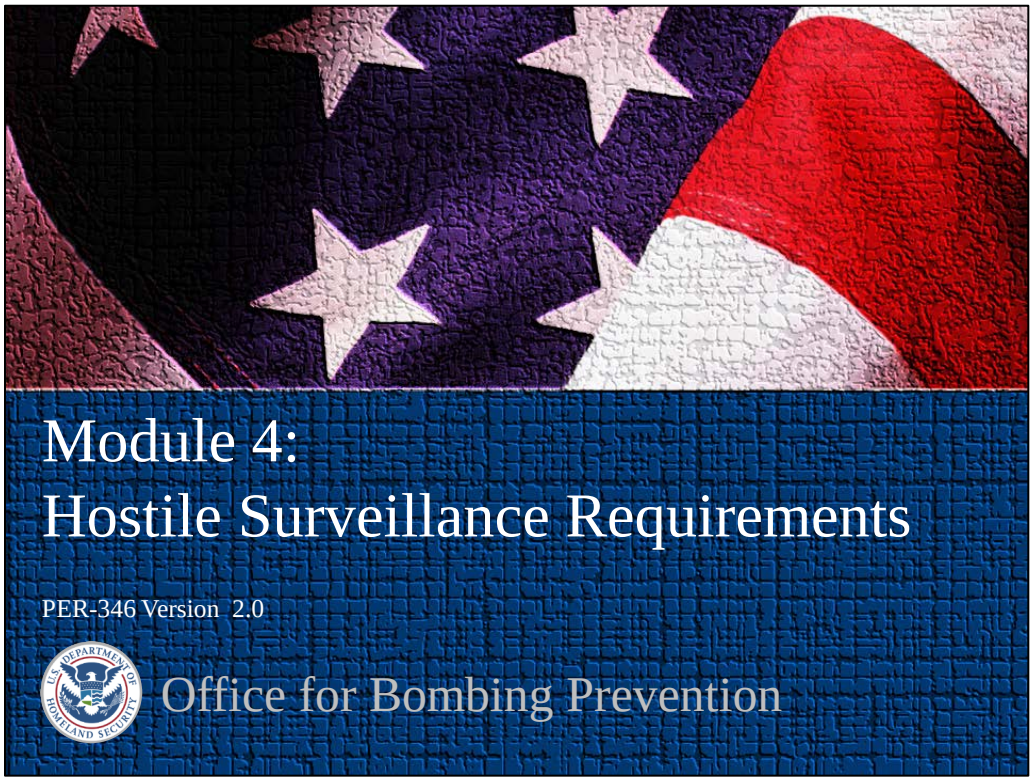
a. Describe the Red Zone of a facility?

b. Define HSPs?

c. Describe the requirements for adequate cover and concealment?

d. Describe the parameters for logical entry and exit?

Media 18


Module 4:
Hostile Surveillance Requirements
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

Sommer, Dan. 2004. "Surveillance Detection Theory PowerPoint Presentation."

Toben, Ami. 2013. *A Very Brief Introduction to Hostile Surveillance.* August 9. Accessed 5 2017, May. https://protectioncircle.org/2013/08/09/a-very-brief-introduction-to-hostile-surveillance/.

—. 2013. *Surveillance Indicators.* March 20. Accessed May 5, 2017. https://protectioncircle.org/2014/03/20/surveillance-indicators/.

Module 4
Supplemental Materials

This page is intentionally left blank.

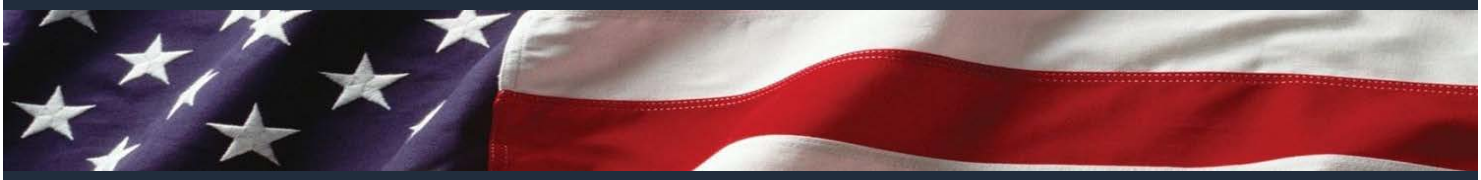
Homeland Security

Hostile Surveillance Position Matrix

Use this matrix to document descriptions of hostile surveillance positions.

HSP#	Location of HSP	Vulnerability Being Viewed	Normal Activity	Normal Duration	Date/Times HSP is Available

HSP#	Location of HSP	Vulnerability Being Viewed	Normal Activity	Normal Duration	Date/Times HSP is Available



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 5: Surveillance Detection Requirements and Fundamentals

Participant Workbook

This page is intentionally left blank.

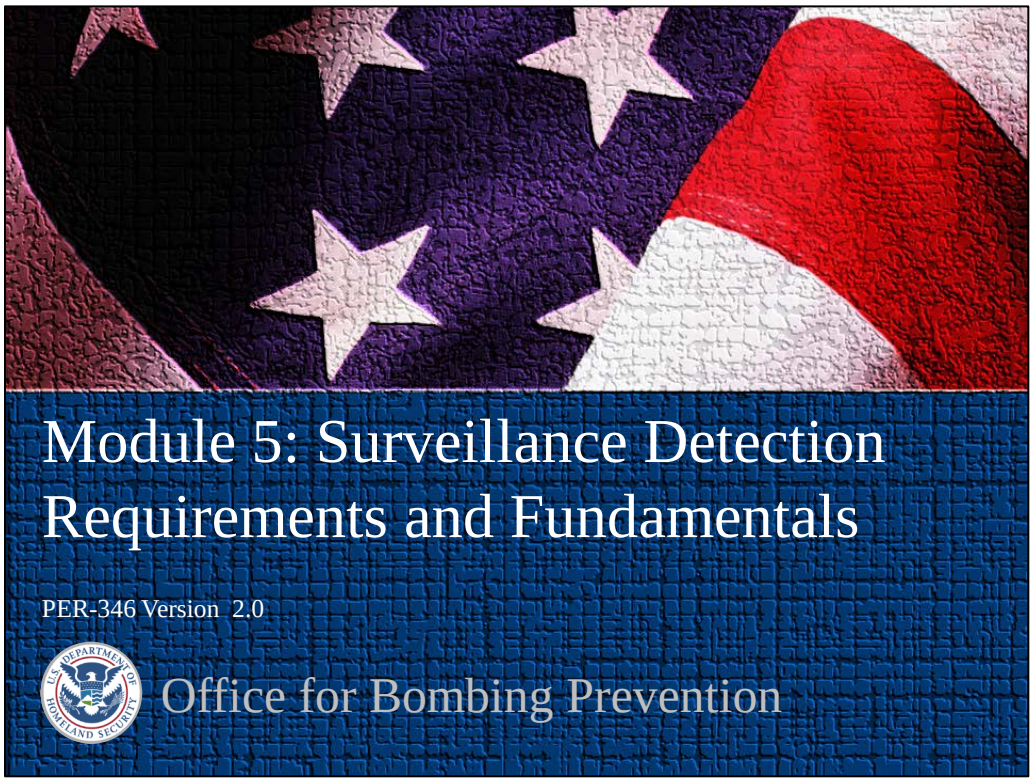
Number: Module 5

Title: Surveillance Detection Requirements and Fundamentals

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 5: Surveillance Detection Requirements and Fundamentals. The purpose of this module is to provide an overview of methods for detecting hostile surveillance, including identifying surveillance detection points and correlating behavioral indicators.

2. **Learning Objectives**

   a. **Terminal Learning Objective.** Given a written examination, participants will describe the fundamentals of surveillance detection for bombing prevention according to the guidelines provided in class. (SD-0120)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will describe how to identify surveillance detection points to achieve a minimum score of 70%. (SD-0120a)

(2) Given a written examination, participants will identify the levels of the surveillance detection pyramid to achieve a minimum score of 70%. (SD-0120b)

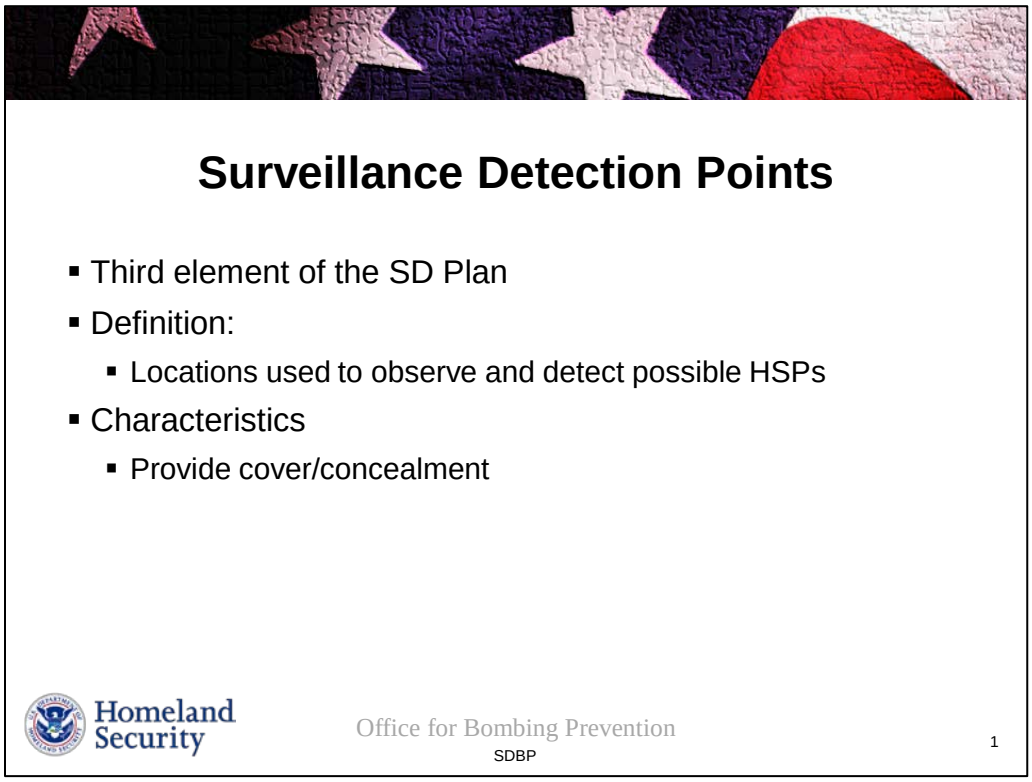
(3) Given a written examination, participants will describe the parameters for correlation to achieve a minimum score of 70%. (SD-0120c)

(4) Given a written examination, participants will identify actions to take to interrupt hostile surveillance to achieve a minimum score of 70%. (SD-0120d)

BODY

LECTURE/DISCUSSION ***1 hour, 40 minutes*** ***1:20***

Media 1

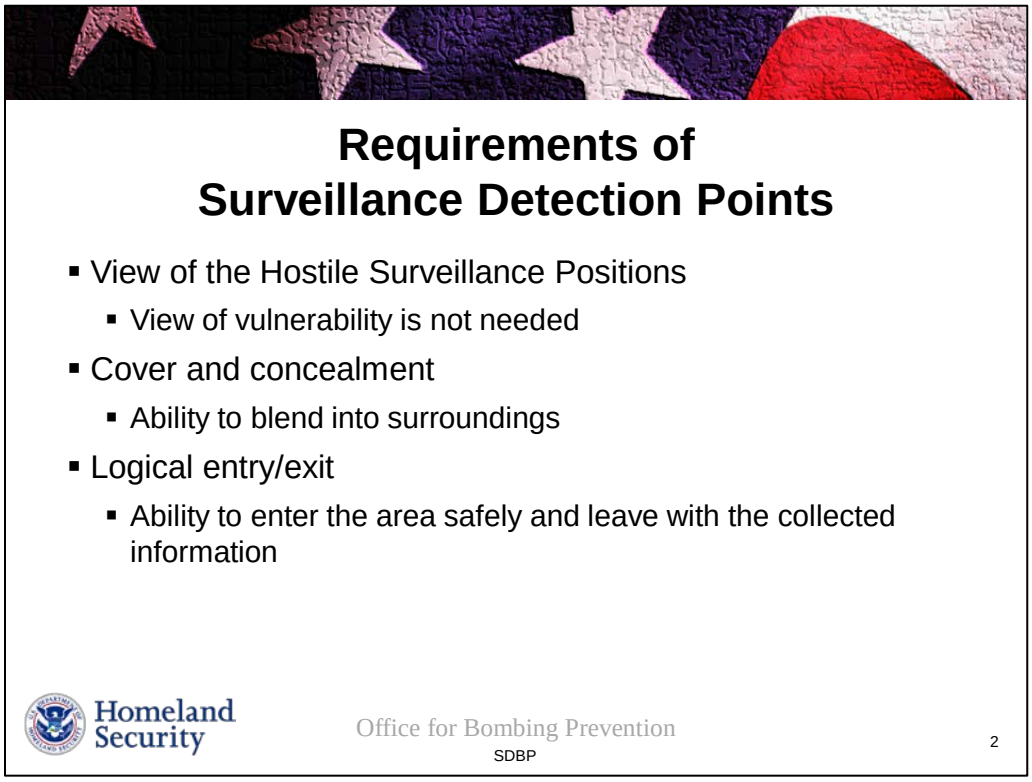


3. **Surveillance Detection Points.** Previous modules covered the vulnerability assessment and identification of hostile surveillance positions (HSPs), the first two elements of a surveillance detection plan. Surveillance detection points are the third element of the surveillance detection plan and the focus of this module.

   Surveillance detection points are where you need to be to observe and detect hostile surveillance indicators.

   They provide cover and concealment to look for abnormalities.

Media 2



a. Requirements of Surveillance Detection Points. Surveillance detection points are determined by standing in the HSPs. For the surveillance detection point to be effective, it must provide:

(1) A maintainable unobstructed line of sight **view of the HSP**.

(a) Do not need to see the vulnerability.

(b) Best positions are behind or to the side of the HSP.

(c) Try not to be in the red zone. If you must, you need to have good cover.

(2) **Cover and/or concealment** to allow observation of the HSP.

(a) Dress to blend in with the environment and support your cover for action.

(b) Avoid military/law enforcement mannerisms (the way you walk, where you stand, where you are facing, where you park your vehicle, etc.).

(c) Learn from other team members what works well and their lessons learned.

(3) **Logical entry and exit** (likely the same as the HSPs). They should:

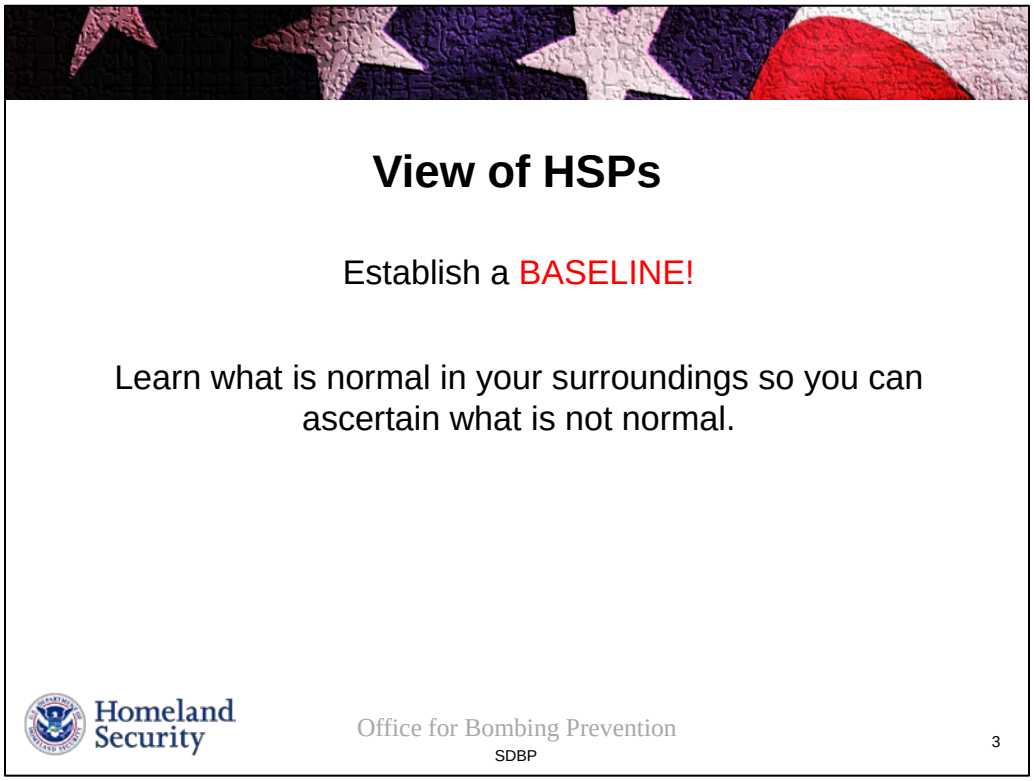
(a) Not draw attention to you being there.

(b) Never require secretive action.

(c) Be in alignment with your cover.

Surveillance detection is most effective when it is integrated into all three rings of security and you are aware of where the hostile surveillant needs to be.

Media 3

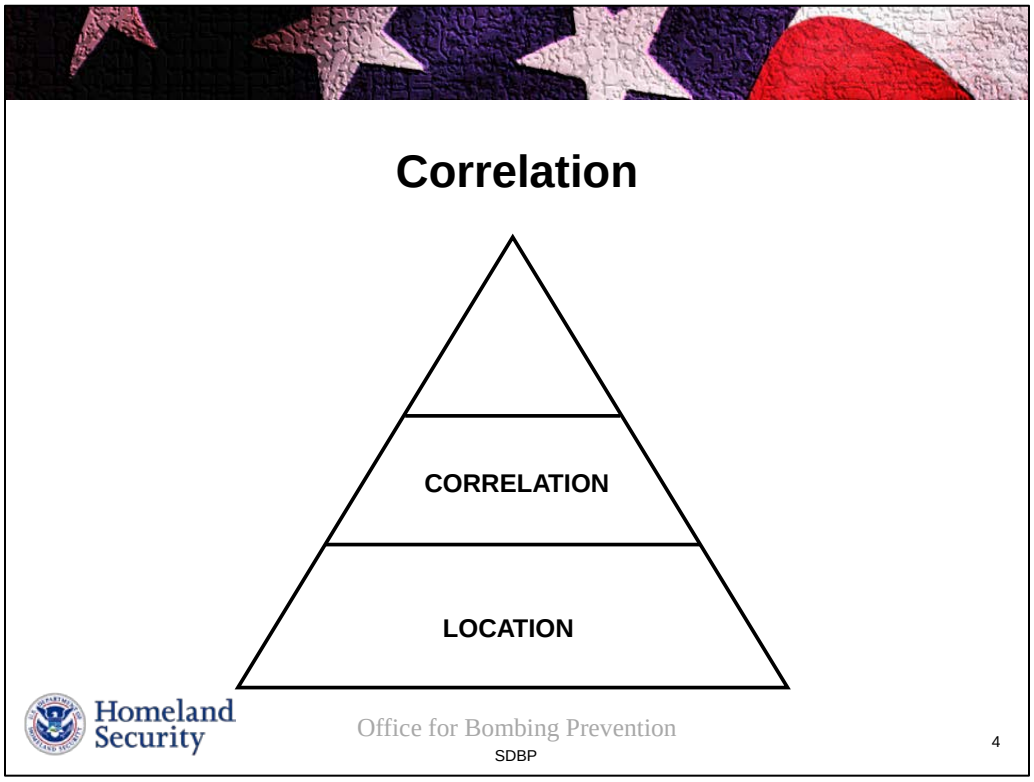


b. View of HSPs. Before you can determine what is *abnormal*, you must develop a baseline of what is *normal*. Determining a normal baseline is the basis by which all surveillance detection is conducted.

(1) Baseline is what is normal for that area.

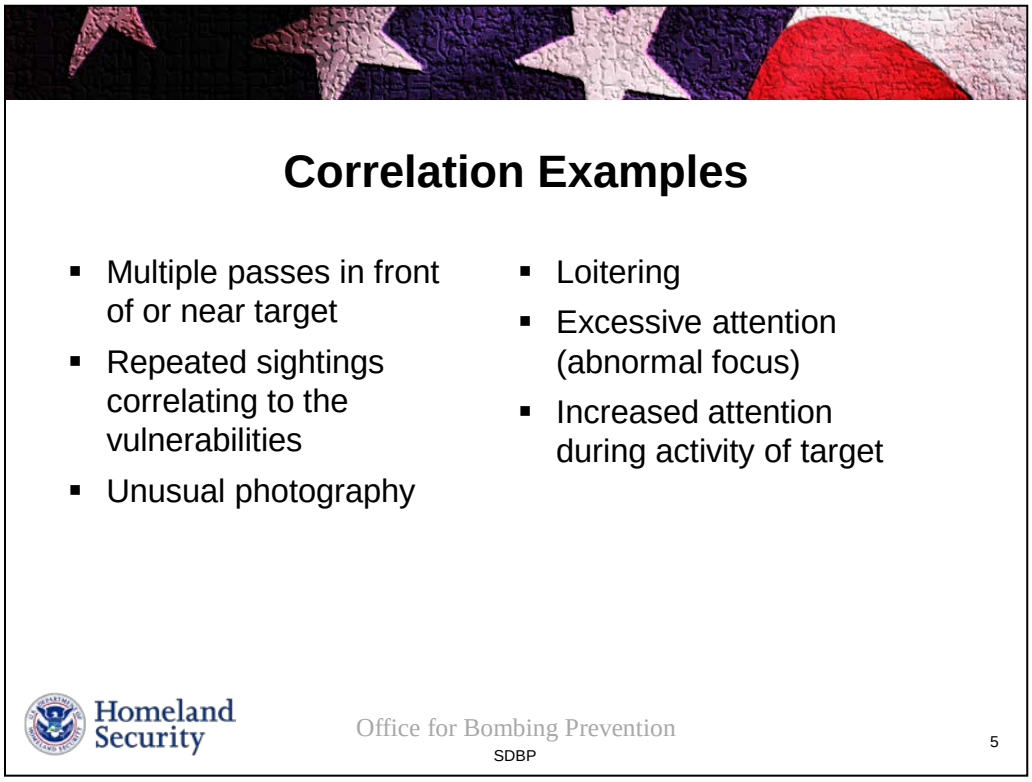
(2) Baselines are different for different areas.

Media 4



4. **Correlation.** Correlation is the middle level of the surveillance detection pyramid. Correlation is defined as the mutual relationship of two or more things. In this case, we are referencing the relationship between the hostile surveillant and the target. Using the bottom two levels of the pyramid, you can identify unusual or suspicious activity.

Media 5



a. Correlation Examples

(1) Repeated sightings of individuals correlating with the facility or vulnerability

(2) Repeated sightings of individuals correlating with different facilities/vulnerabilities

(3) Suspicious/correlative activity within the HSPs reported during heavy activity, deliveries, event preparation, VIP arrivals, or service calls

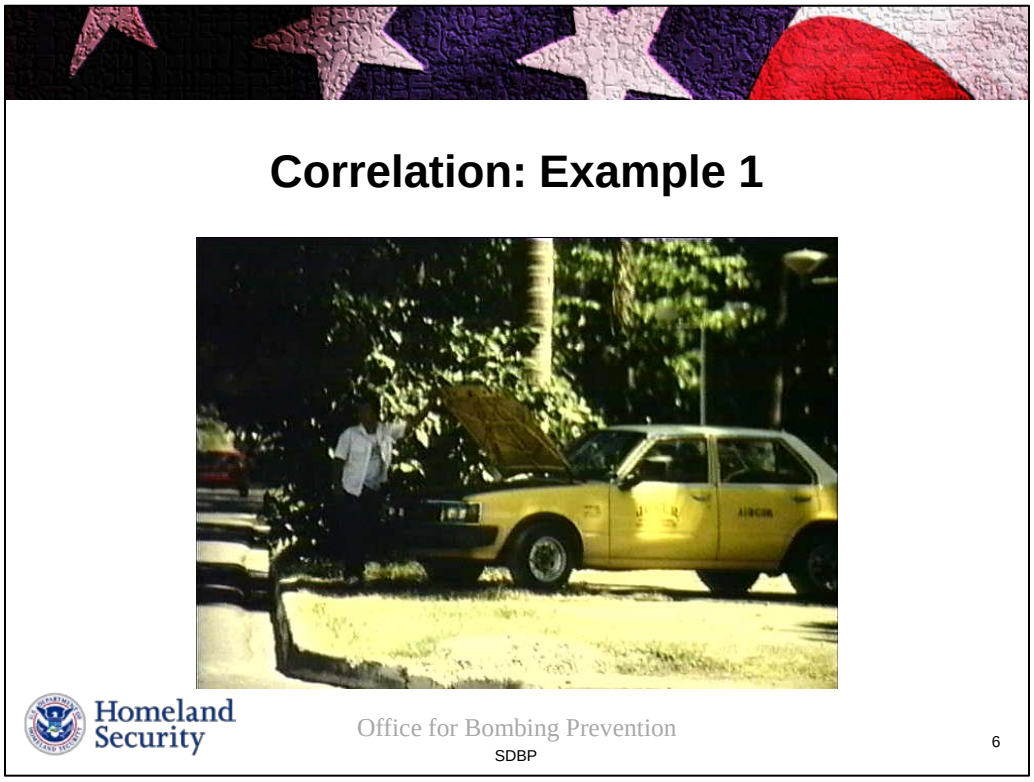
(4) Photographing things that would not normally be photographed

(5) Multiple passes in front of or near the target

(6) Loitering (particularly in the HSPs)

(7) Excessive attention to the target (abnormal focus)

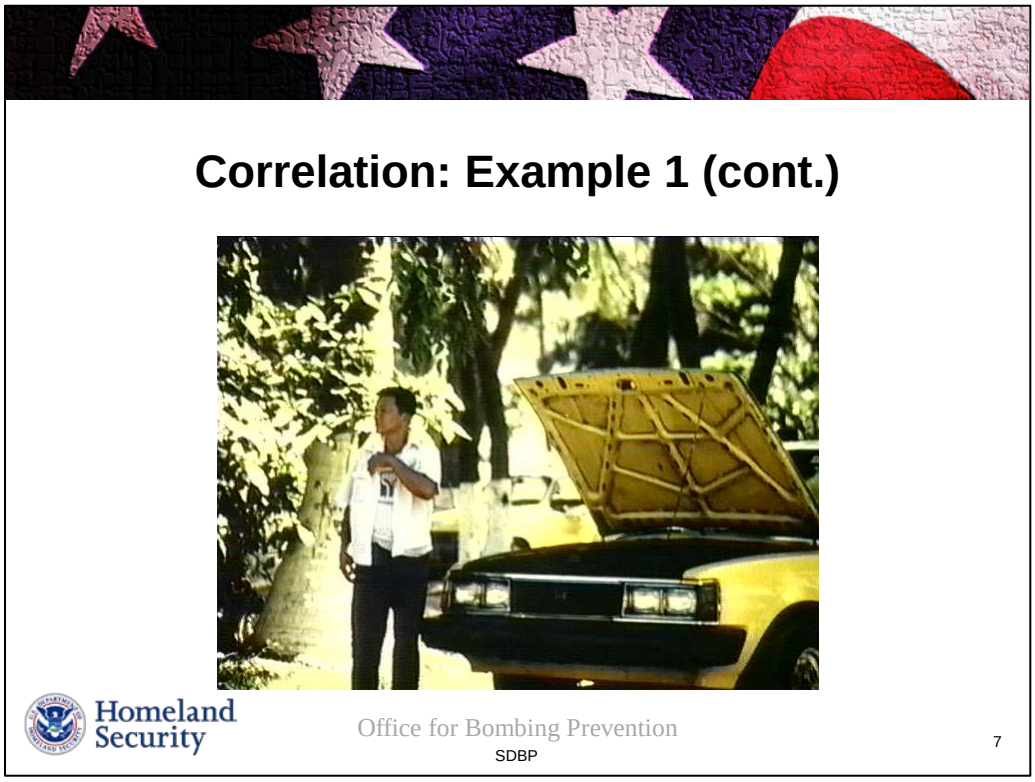
Media 6



b. Correlation: Example 1

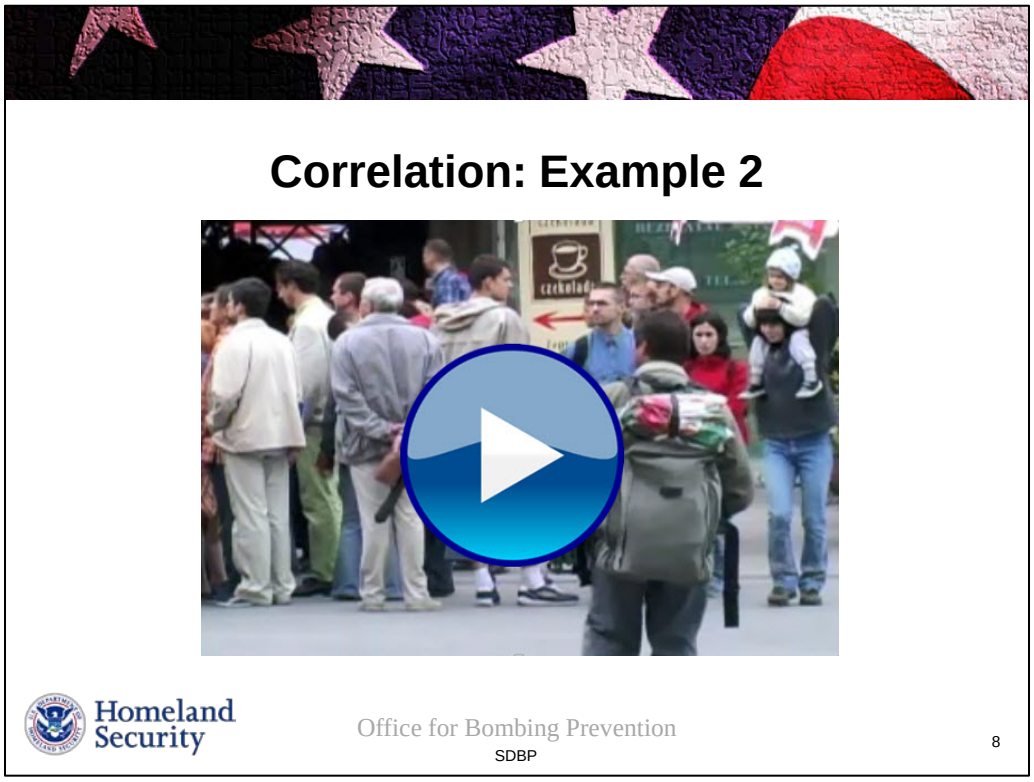
Take any notes you feel necessary below.

Media 7



Take any notes you feel necessary below.

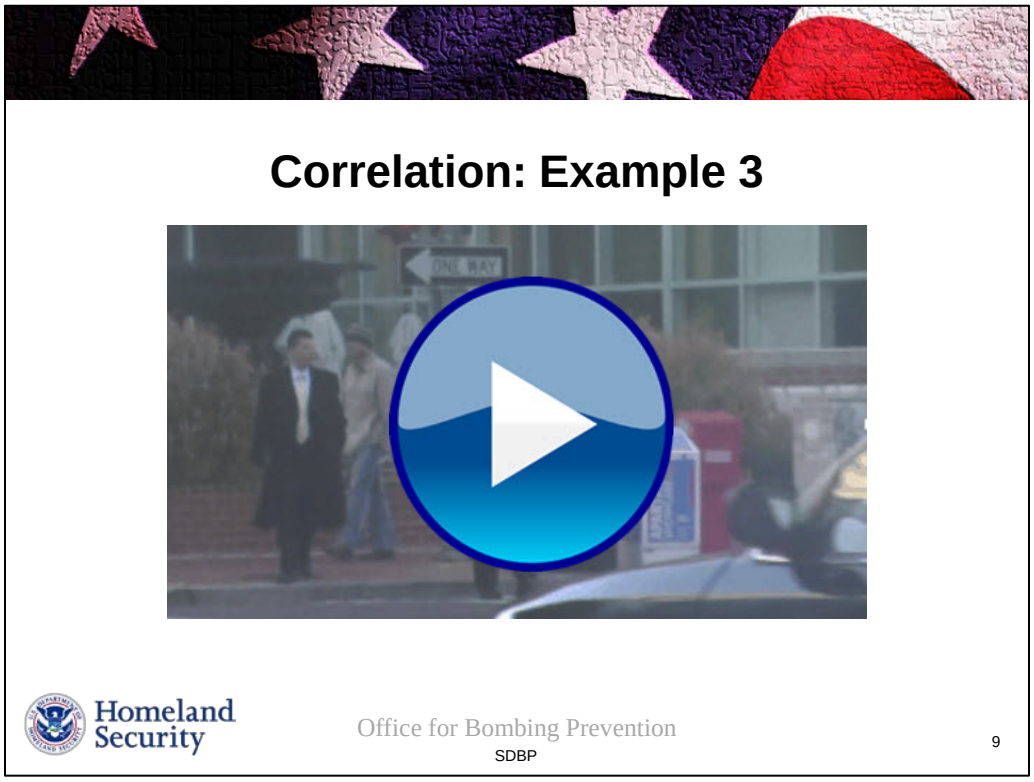
Media 8



c. Correlation: Example 2

Take any notes you feel necessary below.

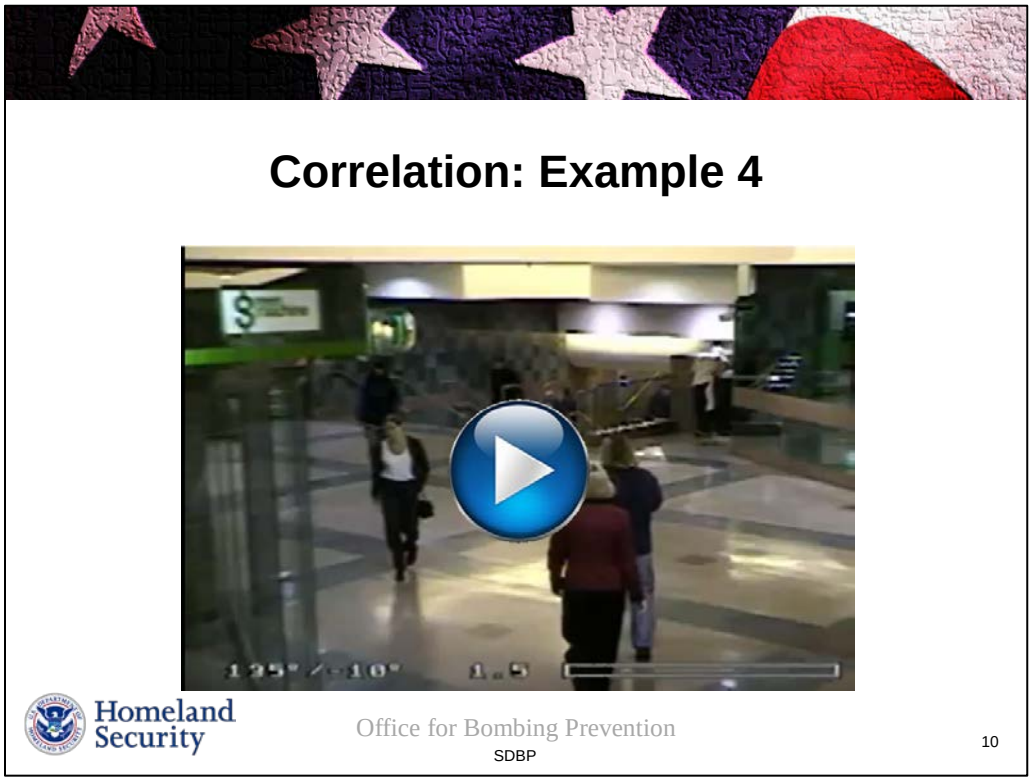
Media 9



d. Correlation: Example 3

Take any notes you feel necessary below.

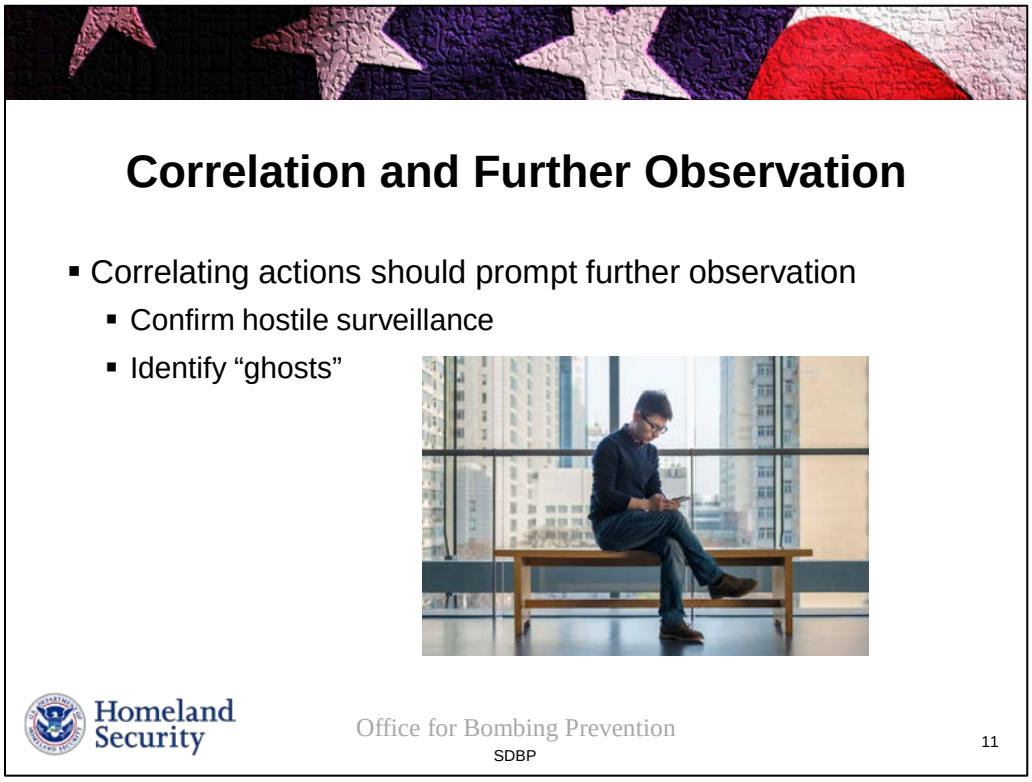
Media 10



e. Correlation: Example 4

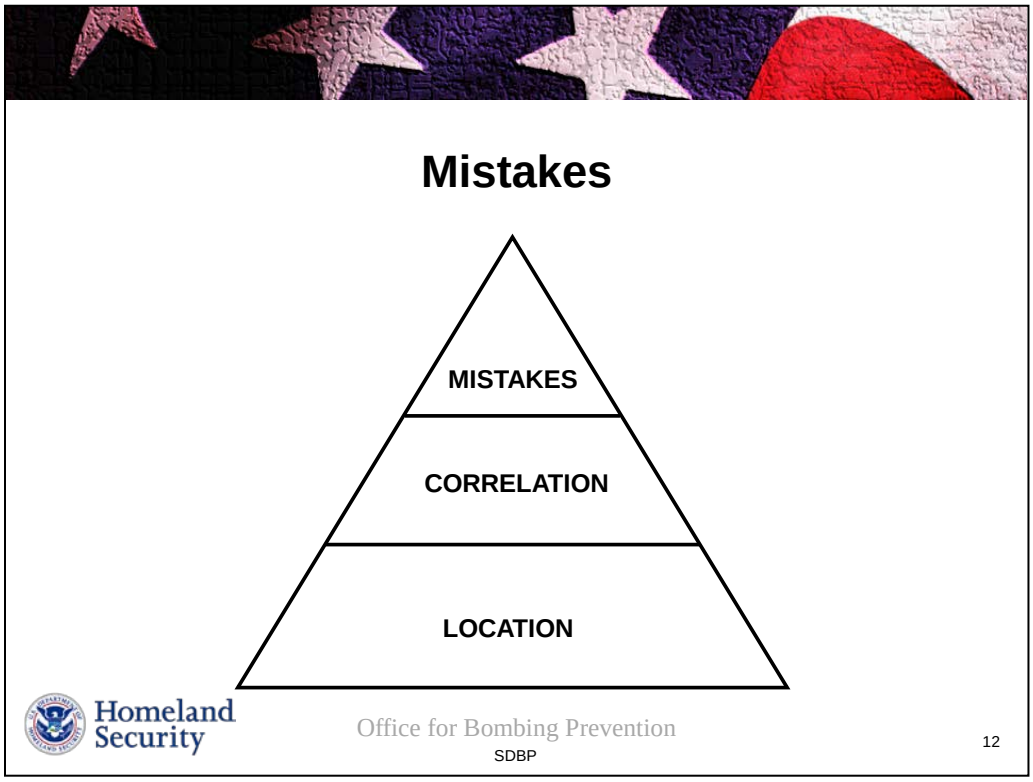
Take any notes you feel necessary below.

Media 11



f. Correlation and Further Investigation. Correlating actions should prompt further observation. Further observation will either confirm the individual is conducting hostile surveillance or the individual is innocent. Innocent people initially suspected of suspicious activity and later ruled out are known as “ghosts.”

Media 12



5. **Mistakes.** Many mistakes involve activities inconsistent with the cover. Examples:

   a. Suspicious behavior with cell phone or camera

   b. Pace of movement out of the norm for the area

   c. Appearing uncomfortable

   d. Departing the area immediately after an event

   e. Parking in a prohibited area

   f. Occupied vehicle parked in the same spot for prolonged periods

   g. Moving a vehicle to get a better view

   h. Parking and not getting out of the vehicle

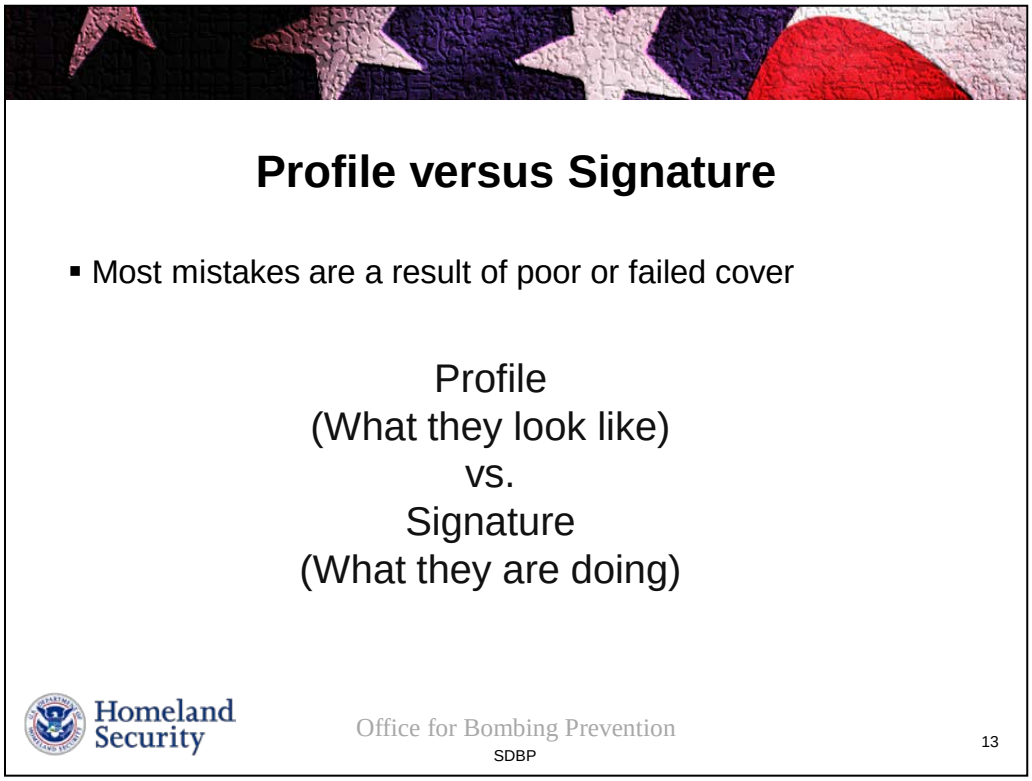
   i. Adjusting vehicle mirrors after parking

   j. Altered or obstructed license plates

   k. Broken-down vehicle in key observation points

   It takes identifying the mistake to confirm hostile surveillance.

Media 13



I. **Profile versus Signature.** Most mistakes are the result of poor or failed cover when what they look like (profile) does not match what they are doing (signature).

Media 14

Profile versus Signature (cont.)

- Examples

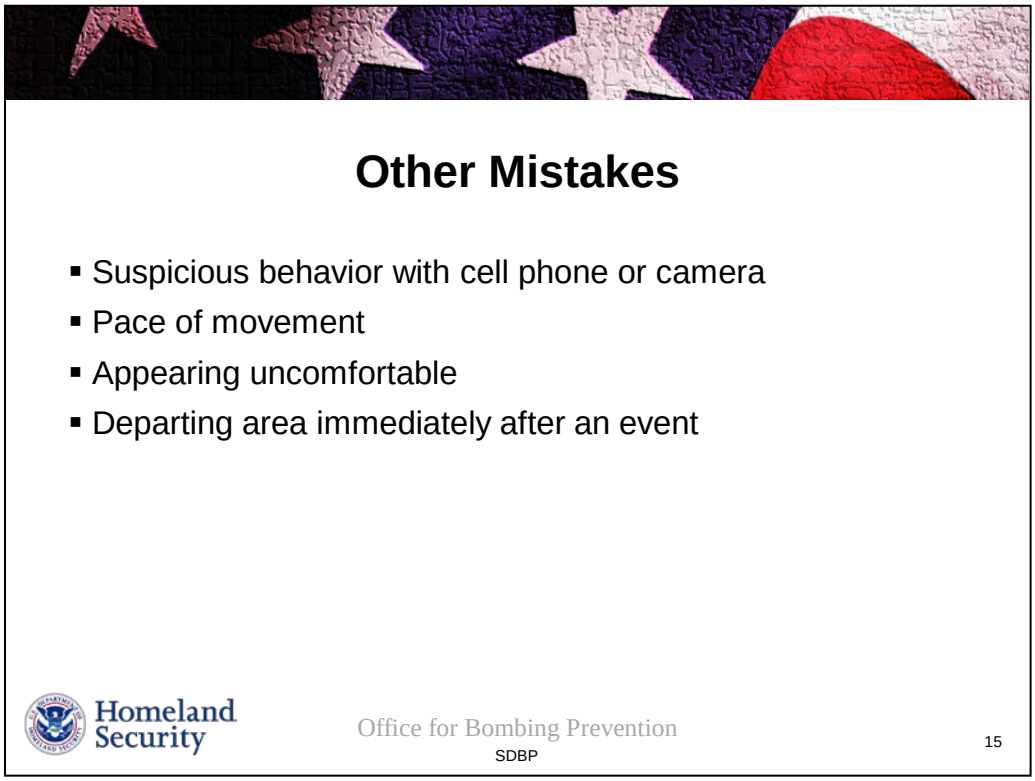
Homeland Security

Office for Bombing Prevention

SDBP

14

Media 15



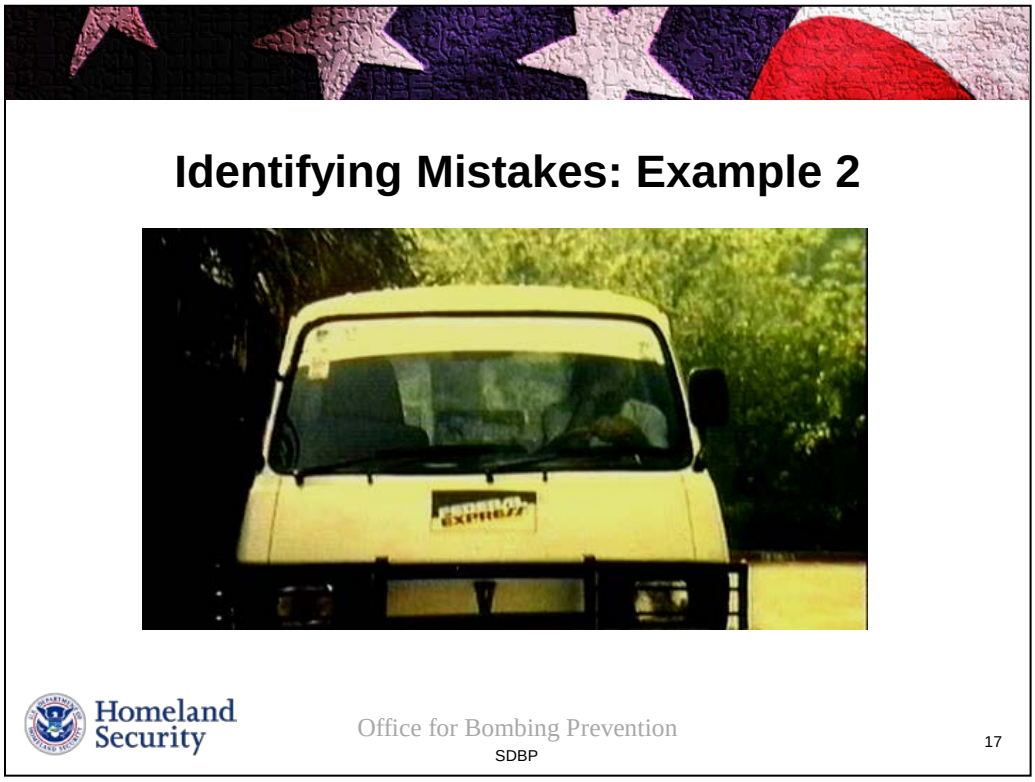
m. Other Mistakes

Media 16

n. Identifying Mistakes: Example 1

Take any notes you feel necessary below.

Media 17



o. Identifying Mistakes: Example 2

Take any notes you feel necessary below.

Media 18

Identifying Mistakes: Example 2 (cont.)

Homeland Security

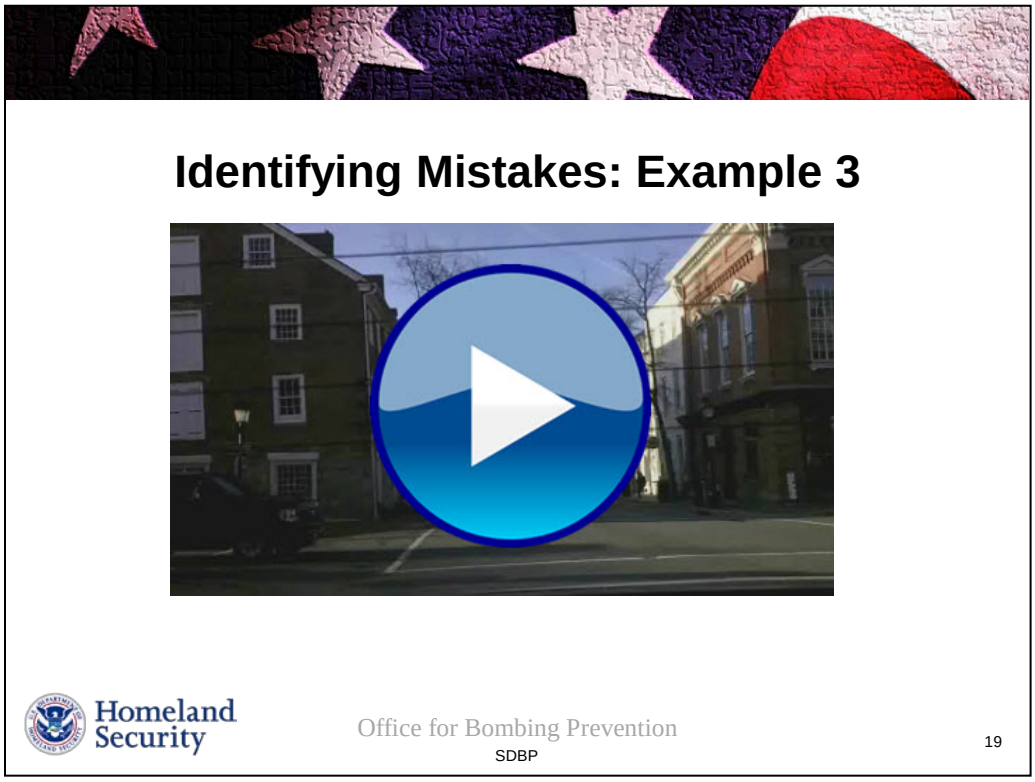
Office for Bombing Prevention

SDBP

18

Take any notes you feel necessary below.

Media 19



d. Identifying Mistakes: Example 3

Take any notes you feel necessary below.

Media 20

e. Identifying Mistakes: Example 4

Take any notes you feel necessary below.

Media 21

f. Identifying Mistakes: Fountain Place Case Study (TRIPwire n.d.)

(1) Hosam Maher Husein Smadi was a Jordanian national in the U.S. illegally overstaying his 2007 student visa. He came to the U.S. for the specific purpose of committing Jihad.

(2) In June 2009, Hosam Maher Husein Smadi met with an undercover FBI agent, telling him that he wanted to target the buildings belonging to the biggest credit card companies to shake the weak economy.

(3) He explained he intended to "…enter the building prior…to see how the security is, how they search…what type of security…so if a bomb is planted, for instance, in the car; timed or to detonate remotely…[could result in]…a very fast operation, smart, and decisive."

(4) During the same meeting, Smadi used a computer to identify possible targets. Smadi and the undercover FBI agent then conducted visual surveillance on the National Guard Armory and the airport.

(5) On May 22, 2009, Smadi was observed, photographed, and reported conducting pre-operational surveillance by participants and instructors attending a DHS Surveillance Detection Course by correlating his actions with his location. He stopped in a place where people do not normally stop (walkway), taking pictures, and did not have a good cover story.

(6) In July 2009, Smadi and the undercover FBI agent conducted physical surveillance and reconnaissance of the Fountain Place office tower in downtown Dallas. Smadi entered the building and conducted individual reconnaissance.

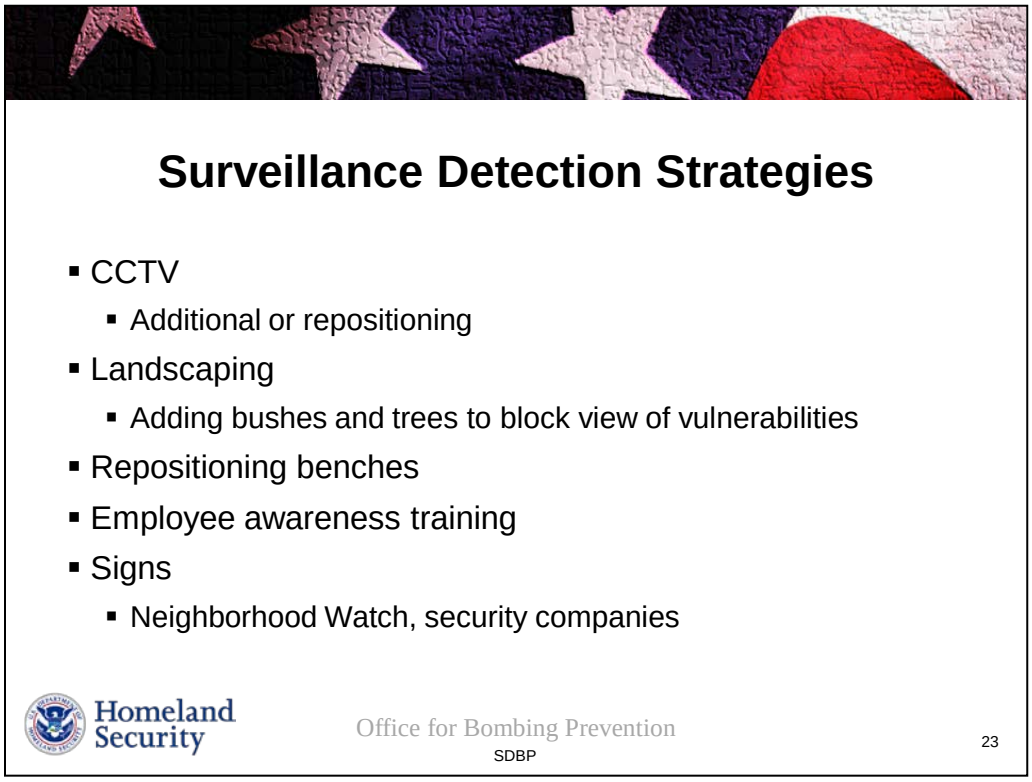
(7) When he returned, he told the undercover agent about a restroom on the basement level that had a locking door and drop ceiling, which could be accessed by standing on the toilet.

Media 22

(8) In September 2009, Smadi and the undercover agent drove to the location of the bombing. After inspecting the VBIED, Smadi conducted surveillance on the target location one last time. He then drove the VBIED through downtown Dallas and parked it in the garage directly beneath the Fountain Place building.

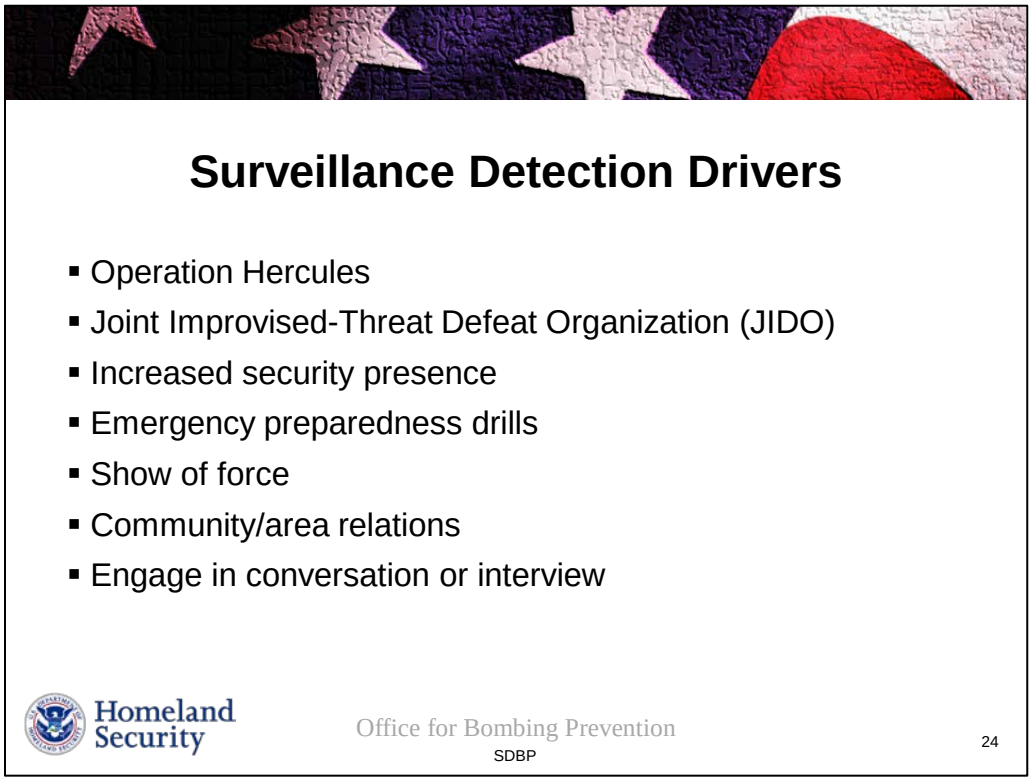
(9) He was arrested on 24 September 2009 and sentenced to 24 years in prison.

Media 23



6. **Surveillance Detection Strategies.** Surveillance detection strategies are methods employed to disable a hostile's ability to surveil from an HSP by changing the environment and adjusting security.

Media 24



7. **Surveillance Detection Drivers.** Surveillance detections drivers are methods and/or actions that can be used to drive out behaviors.

   a. **Operation Hercules.** Operation Hercules are elite, heavily armed, semi-tactical police units that appear without warning and unscheduled. There are units in London and New York City.

   b. **Joint Improvised-Threat Defeat Organization (JIDO).** JIDO teams are military combat units under the Department of Defense.

   c. **Increased security presence.** Increasing security presence may involve adding additional security, use of random anti-terrorism measures by altering schedules, and/or sending a uniformed presence if correlation is noted.

   d. **Emergency preparedness drills.** These drills prepare both response teams and civilians to respond to various emergencies.

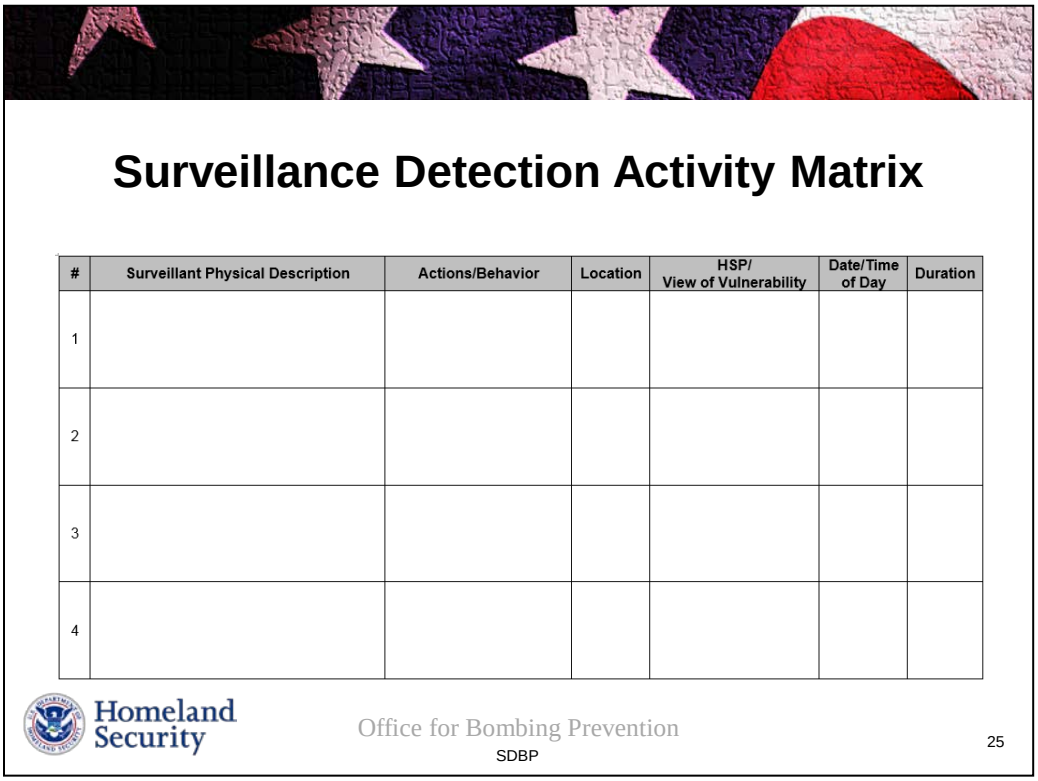
   e. **Show of force.** Show of force involves using additional armed security or law enforcement at various locations or events.

   f. **Community/area relations.** Educate the public on what to observe and what to report in terms of suspicious behavior.

   g. **Engage in conversation or interview.** Using elicitation/solicitation to determine truthfulness. Ask questions. Cover stories are typically only one or two levels deep.

When you ask more questions, it can reveal inconsistencies or missing links in the cover story.

Media 25



8. **Surveillance Detection Activity Matrix.** The surveillance detection activity matrix is a tool that should be a part of all surveillance detection plans. Its purpose is to keep all observed potential hostile surveillance in one place. This provides a summary of the history of activity at and around a vulnerability for all members of the surveillance detection team to reference and analyze.

   Each surveillance detection team should add relevant information as they note it. Each addition provides more information for analysis of ongoing potential hostile surveillance activity. This practice can help identify different surveillants, which may indicate a cell of attackers rather than a lone attacker. It may serve to identify changing potential vulnerabilities or the primary vulnerable area based on repeat visits by hostile surveillants.

   It also serves as a resource for personnel conducting surveillance detection of the area for the first time by providing a history of what has transpired in the past.

   The SD matrix should include:

   a. **Surveillant Physical Description.** Describe the physical characteristics in detail. Include how he/she was dressed.

   b. **Actions/Behavior.** Describe what the person was doing, such as eating, reading, on a computer, on the phone, and/or taking pictures.

   c. **Location.** Describe where the surveillant was located. For example, the person seated on a park bench, in a coffee shop, in a phone booth, or in a vehicle.

d. **HSP/View of Vulnerability.** Record the view of the vulnerability identified by the HSP number.

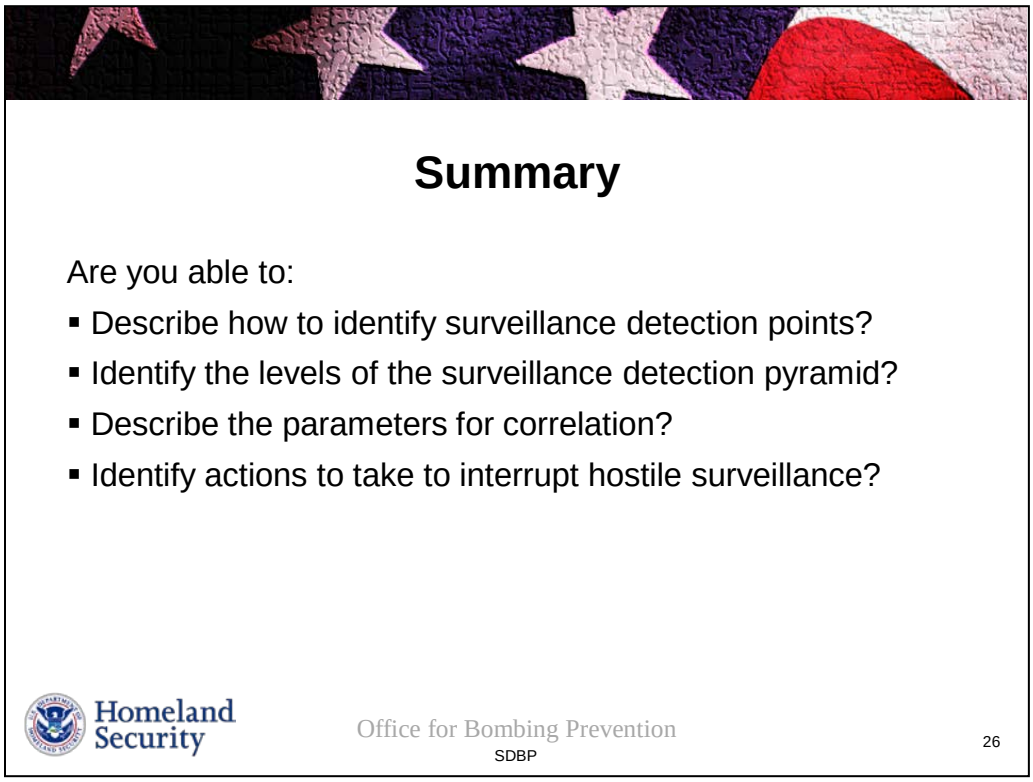
e. **Date/Time of Day.** Recording the dates and times is important for correlating future sightings.

f. **Duration.** Record how long the surveillant was in the HSP.

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 26



9. Summary. This module served to introduce you to the requirements for hostile surveillance. Are you able to:

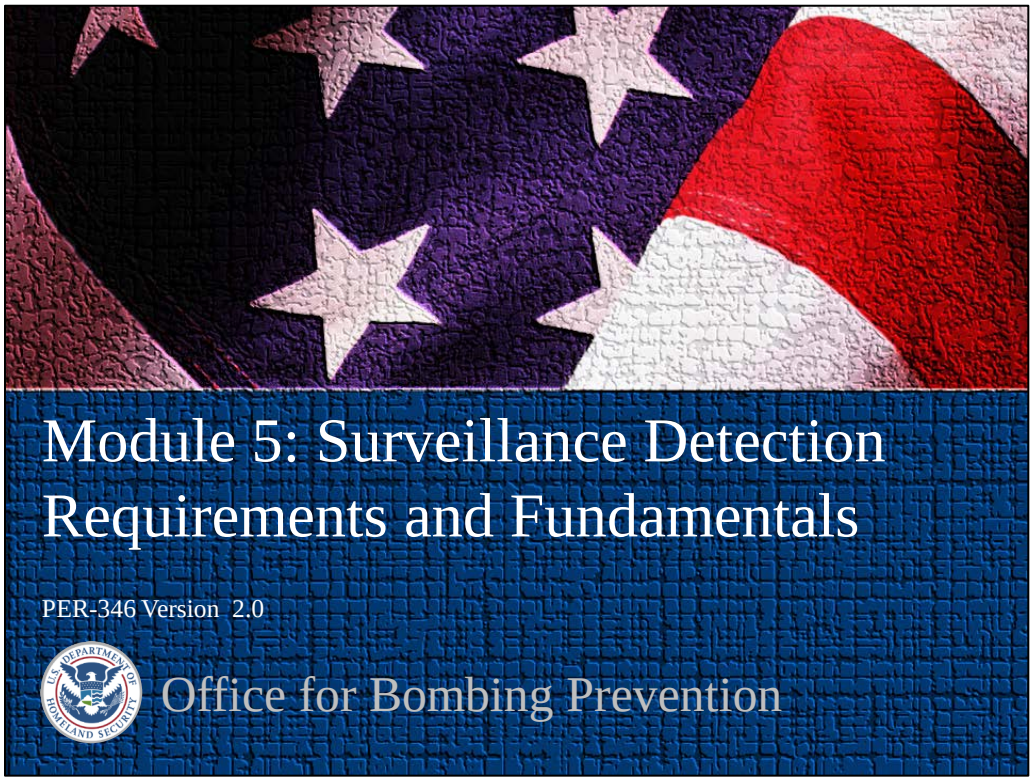
a. Describe how to identify surveillance detection points?

b. Identify the levels of the surveillance detection pyramid?

c. Describe the parameters for correlation?

d. Identify actions to take to interrupt hostile surveillance?

Media 27


Module 5: Surveillance Detection Requirements and Fundamentals
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

Kimery, Anthony L. 2008. *Suspicious Behavior Could Indicate Terror.* June 23. Accessed 1 2017, April. http://www.adjunct.diodon349.com/Attack_on_USA/suspicious_behavior_could_indicate_terror_plotiing.htm.

Sommer, Dan. 2007. "Chapter 2: Surveillance Dectection." In *How to be a Successful SD Specialist: The Surveillance Detection Manual*, by Dan Sommer, 61-69. Iceland.

Toben, Ami. 2013. *A Very Brief Introduction to Hostile Surveillance.* August 9. Accessed May 5, 2017. https://protectioncircle.org/2013/08/09/a-very-brief-introduction-to-hostile-surveillance/.

—. 2014. *A Very Brief Introduction to Surveillance Detection.* January 3. Accessed May 5, 2017. https://protectioncircle.org/2014/01/03/a-very-brief-introduction-to-surveillance-detection/.

—. 2013. *Strategies Against Hostile Surveillance.* August 16. Accessed May 5, 2017. https://protectioncircle.org/2013/08/16/111/.

—. 2015. *Surveillance Detection -- Tips & Suggestions for Field Operators.* June 19. Accessed 5 2017, May. https://protectioncircle.org/2015/06/19/surveillance-detection-tips-suggestions-for-field-operators/.

—. 2014. *Surveillance Indicators.* March 20. Accessed May 5, 2017. https://protectioncircle.org/2014/03/20/surveillance-indicators/.

—. 2013. *The Outer Circle-Disrupting and Mitigating Hostile Surveillance.* September 19. Accessed 5 2017, May. https://protectioncircle.org/2013/09/19/security-solutions-to-hostile-surveillance/.

TRIP*wire*. n.d. *Technical Resource for Incident Prevention.* Department of Homeland Security. Accessed March 1, 2017. tripwire.dhs.gov.

Module 5
Supplemental Materials

This page is intentionally left blank.

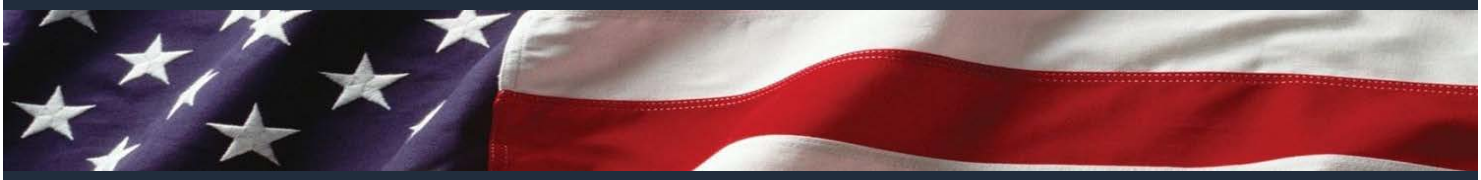
Homeland Security

Surveillance Detection Activity Matrix

Use this matrix to document descriptions and activities of suspected surveillants.

#	Surveillant Physical Description	Actions/Behavior	Location	HSP/ View of Vulnerability	Date/Time of Day	Duration
1						
2						
3						
4						

#	Surveillant Physical Description	Actions/Behavior	Location	HSP/ View of Vulnerability	Date/Time of Day	Duration
5						
6						
7						
8						
9						
10						



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Experiential Learning Guide Activity 2: Detection Fundamentals Activity

Participant Workbook

This page is intentionally left blank.

Number: Experiential Learning Activity (ELA) 2

Title: Detection Fundamentals Activity

Purpose. The purpose of this activity is to provide an opportunity to identify hostile surveillance positions (HSPs) based on determining the Red Zone of a given facility, surveillance detection points (SDPs) based on identified hostile surveillance positions, and analyze the profile versus signature of two observed individuals.

Learning Objectives

a. **Terminal Learning Objective.** Given an assigned facility, participants will identify the locations of HSPs and SDPs based on the vulnerabilities identified in Experiential Learning Activity 1: Vulnerability Assessment Activity. (SD-0220)

b. **Enabling Learning Objectives**

(1) Given a facility, participants will determine the hostile surveillance positions based on the Red Zone in accordance with the parameters presented in class. (SD-0220a)

(2) Using the identified hostile surveillance positions of a given facility, participants will determine appropriate surveillance detection points in accordance with the parameters presented in class. (SD-0220b)

(3) Participants will describe to classmates the profile and signature of two individuals observed while identifying the hostile surveillance positions and surveillance detection points. (SD-0220c)

Learning Event Description. During this learning event, your teams will return to your assigned facility and identify the HSPs and SDPs for the vulnerabilities you identified in the ELA 1: Vulnerability Assessment Activity.

Activity Instructions

a. You will remain in the same teams as the previous ELA. You can elect a new team leader or keep the same team leader from the first activity.

b. Team leaders can conduct the identification of the HSPs and SDPs however they want (e.g., assign specific tasks to each team member or assign specific areas to members to assess for both the HSPs and SDPs).

c. You are to go and sit in the identified HSPs. From these locations, you can test out location viability and the duration a hostile would stay at that location. Also from the HSP, you can identify your SDPs.

d. After you have identified your SDPs by sitting in the HSPs, you should go sit in those SDPs and again test out location viability and duration, but now from the “good guy” perspective.

e. You will need to select two random individuals to observe during the activity and determine their profile versus signature (i.e., determine if their actions support their appearance).

f. You have three hours to complete the activity. The three hours includes lunch and travel time.

g. Upon returning to the classroom, you will add the HSPs of your assigned facility in red marker and the SDPs of your assigned facility in blue marker to your schematics. Your will also complete a Module 4 Handout 1: HSP Matrix for your identified HSPs. Your will have 20 minutes to update your schematic.

h. You also need to complete the HSP matrix for each of your HSPs as well as mark them on their schematic.

(1) Select a spokesperson to report out to the class.

(2) Tell participants you will then conduct a debrief of the activity.

(3) Your responsibility for activity safety is the same as the first activity.

SAFETY BRIEF

Risk Assessment: Moderate. This activity involves controlled practical application requiring substantial exertion. Moderate risk exists for injury to personnel or damage to equipment.

Safety Precautions and Control Measures

a. Physiological stressors such as exertion, heat, cold, or hydration may have significant effects upon some individuals. If you or a fellow participant experience adverse physiological effects, inform an instructor immediately.

b. Psychological stressors may have significant effects upon some individuals. If you or a fellow participant experience adverse psychological effects, inform an instructor immediately.

Cease Training Procedures. If at any time an instructor or participant feels that an unsafe condition exists during an activity, an individual may request for training to stop by contacting the team leader who will contact the instructor. The instructor will assess the situation. The instructor will not commence training until an identified unsafe situation has been resolved and/or appropriate control measures have been implemented to mitigate the risk.

Participant Responsibility for Activity Safety. Along with the instructors and staff, each participant is also responsible for the safety of the activity.

a. Participant Responsibility for Activity Safety

(1) Be vigilant in your observance of safety precautions and associated control measures, and bring any potential concern to the attention of the nearest instructor or staff member as soon as observed.

(2) If a fellow participant or a staff member needs assistance, please aid him/her to the best of your ability without inappropriately risking your own health and/or safety until designated personnel arrive.

(3) You have the option to not participate in a training event if you feel you are physically or emotionally unable to perform the designated actions or skills. Immediately notify an instructor should you have concerns about participating in a training event.

(4) A participant may be prohibited from participating in a training event if perceived by any staff member as being physically and/or cognitively impaired by drugs, alcohol, or other substances.

b. Safety Takes Priority Over Activity Events

(1) If directed by an instructor or other designated personnel to stop training, evacuate an area, assist a staff member or participant, etc., immediately do so to the best of your ability. The safety of all personnel will take priority over the training activity.

(2) If you sense yourself or others becoming overly fatigued, dehydrated, or otherwise compromised to an unsafe extent, contact an instructor and mitigate the situation as soon as possible.

Inclement Weather. In the event of inclement weather, such as excessive heat or cold, tornadoes, thunderstorms, etc., safety protocols may determine changes in training activities and their locations. This practice is to ensure the safety of all participants and provide a safe environment to complete event objectives.

Hazards. Due to the unique training environment, there may be a wide array of walking/working surfaces and hazards. All participants must be aware of hazards that may cause slips, trips, falls, collisions, etc. within the training area. Any participant identifying a hazard requiring mitigation should notify an instructor.

Participant Behavior. Aggressive behavior will not be tolerated during the event. Examples of aggressive behavior may include hostile communications, excessive use of force, or inappropriate use of response equipment.

Additional rules for the activity are included in the Threat Portfolio Briefing. These include:

a. Never enter your assigned facility through illegal or deceptive means.

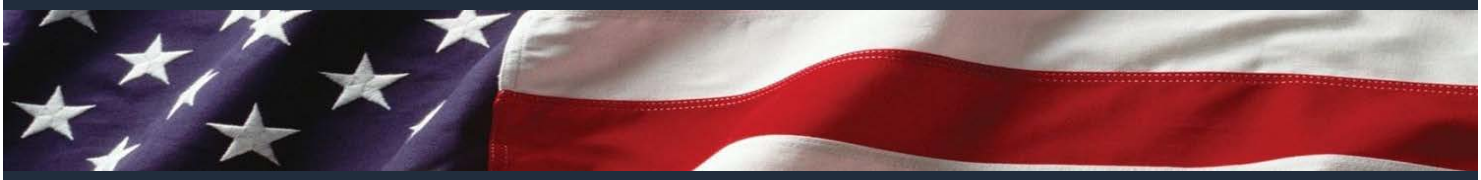
b. Conduct all activities within the public areas of the facility only, and do not disrupt operations at the facility.

c. Do not engage or otherwise alert potential hostile surveillants to surveillance detection (SD) efforts in area unless presented with exigent circumstances (disrupt an attack, prevent loss of life, etc.).

d. Do not overtly engage or otherwise communicate with contracted security personnel, employees, law enforcement officers (LEOs), or other SD team members (unless it is part of your cover).

e. If you experience any emergency (medical or criminal), contact 911, then contact the instructor.

f. Follow established agency/department policy if you encounter illegal activity.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 6: Reporting and Response

Participant Workbook

This page is intentionally left blank.

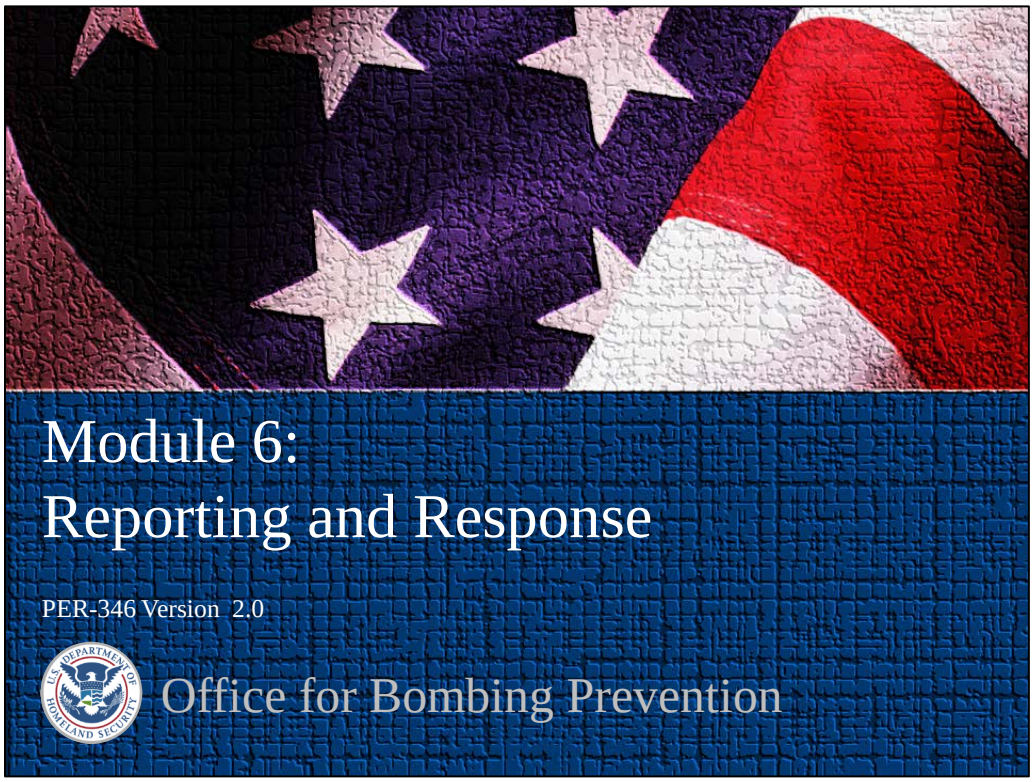
Number: Module 6

Title: Reporting and Response

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 6: Reporting and Response. The purpose of this module is to provide an overview of the final two elements of the surveillance detection plan. This module has an activity to allow you to practice your description skills.

2. **Learning Objectives**

   a. **Terminal Learning Objective.** Given a written examination, participants will describe what is included in the reporting and response elements of the surveillance detection plan. (SD-0130)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will differentiate between general and distinguishing individual physical characteristics to achieve a minimum score of 70%. (BEH-0201e)

(2) Given an image, participants will document a description of an individual so someone who did not observe the individual will be able to identify him/her out of a compilation of similar people. (SD-0130a)

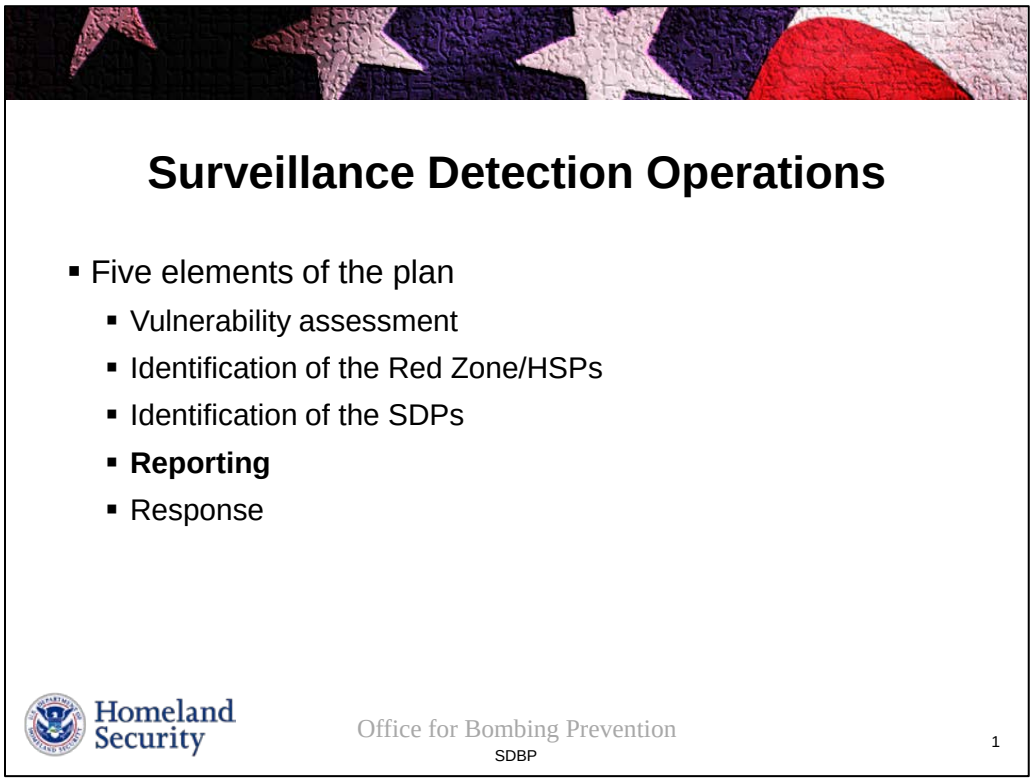
(3) Given a written examination, participants will describe the parameters to document when describing a suspicious vehicle to achieve a minimum score of 70%. (SD-0130b)

(4) Given a written examination, participants will describe the purpose of the response element of the surveillance detection plan to achieve a minimum score of 70%. (SD-0130c)

BODY

LECTURE/DISCUSSION ***10 minutes*** ***1:20***

Media 1



3. **Surveillance Detection Operations.** Surveillance detection operations are identified in the written surveillance detection plan.

   a. **Elements of the surveillance detection plan.** The five elements of the plan are noted below. Previous modules covered the first three elements of the surveillance detection plan. In this module, the focus is on reporting and response, starting with reporting.

      (1) Vulnerability assessment of the facility or site

      (2) Identification of the Red Zone and HSPs within the Red Zone

      (3) Identification of the surveillance detection points

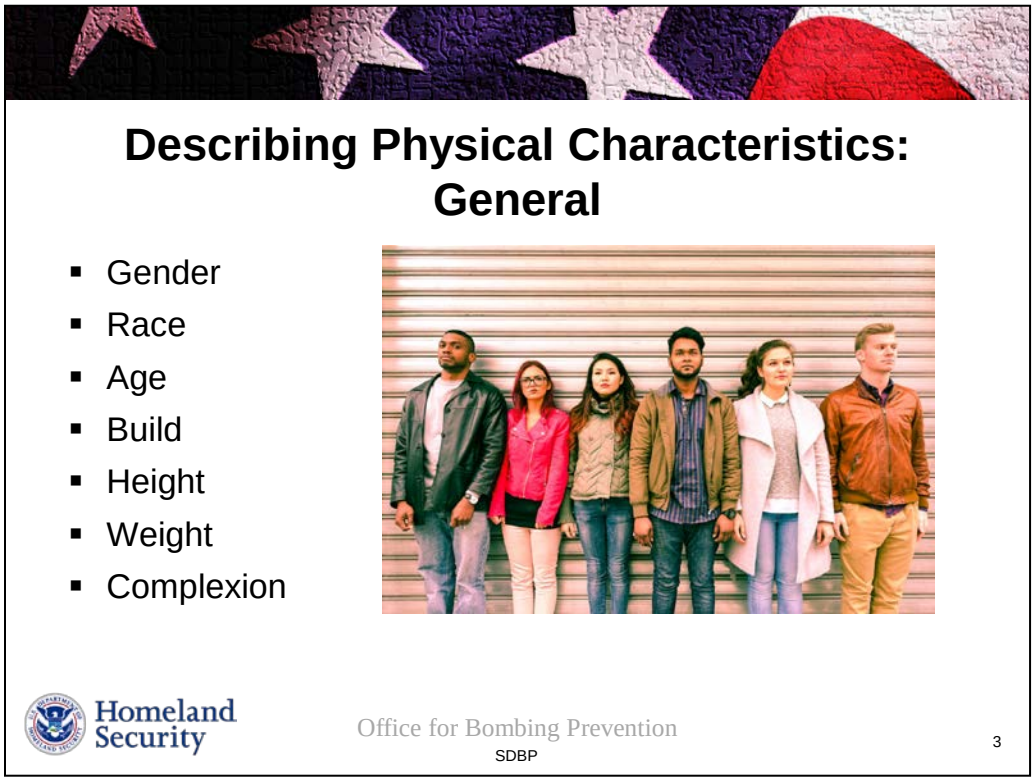
      (4) Reporting

      (5) Response

Media 2

Take any notes you feel necessary below.

Media 3



4. Describing Physical Characteristics (iluEnglish n.d.)

a. General characteristics

(1) Gender

(2) Race

(3) Age

(4) Build (i.e., body type)

(5) Height

(6) Weight

(7) Complexion

Media 4

b. Distinguishing Characteristics. Some of the characteristics noted on the slide are expanded upon below.

(1) Facial features

(a) Forehead height. This includes receding hairline or balding, which might be covered with a wig.

(b) Cheeks/chin. Dimples and/or cleft chin are not easily altered.

(c) Lip size and shape

(d) Brow. The brow, especially when a person makes certain facial expressions, is impossible to change without theater-level makeup.

(2) Teeth. Although a person's teeth cannot be easily changed, teeth can be changed using props.

(3) Ear size and shape

(4) Scars and tattoos. These can be hidden or temporary ones can be added.

(5) Body piercings. Piercings can be added or removed. However, if removed, some leave distinct holes.

(6) Skin texture. Skin texture such as pores, pockmarks, acne, birthmarks, or moles can be covered with makeup, but makeup may not cover it effectively.

(7) Race. Race cannot be changed, but skin color/tone can be altered to a degree.

(8) Age. Age appearance is not easily or effectively changed. Changing how old or young someone appears requires either theater makeup or surgery.

Media 5

c. Other Considerations

(1) Accessories

(a) Watch

(b) Wedding ring

(c) Other jewelry

(d) Bags/Briefcases

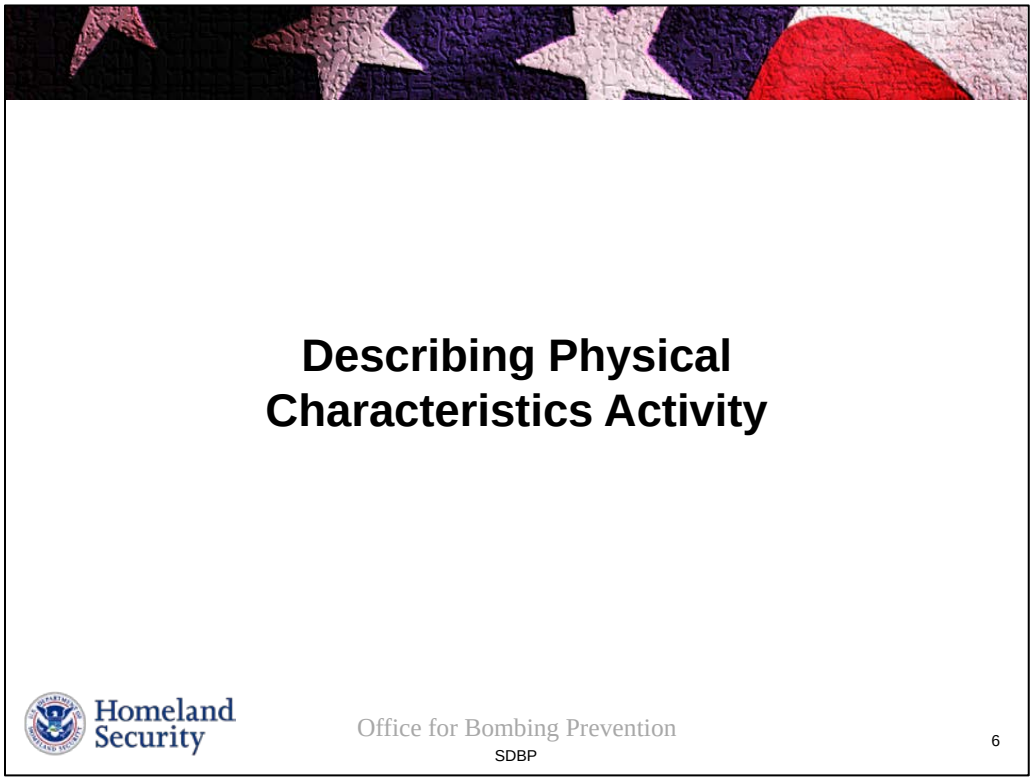
(e) Head gear

(f) Glasses/sunglasses.

(g) Canes/Seeing Eye stick, wheelchair

(2) Clothing: It is important not to use clothing in the description of an individual, since it is easily changed.

Media 6



5. Describing Physical Characteristics Activity

Media 7

This slide intentionally not included

Media 8

This slide intentionally not included

Media 9

This slide intentionally not included

Media 10

This slide intentionally not included

Media 11

This slide intentionally not included

Media 12

This slide intentionally not included

Media 13

This slide intentionally not included

Media 14

6. **Documenting Vehicle Descriptions.** Documenting vehicle characteristics helps analyze recurrent appearances for both your team and other surveillance teams. Characteristics to document include:

   a. Make and model.

   b. Year.

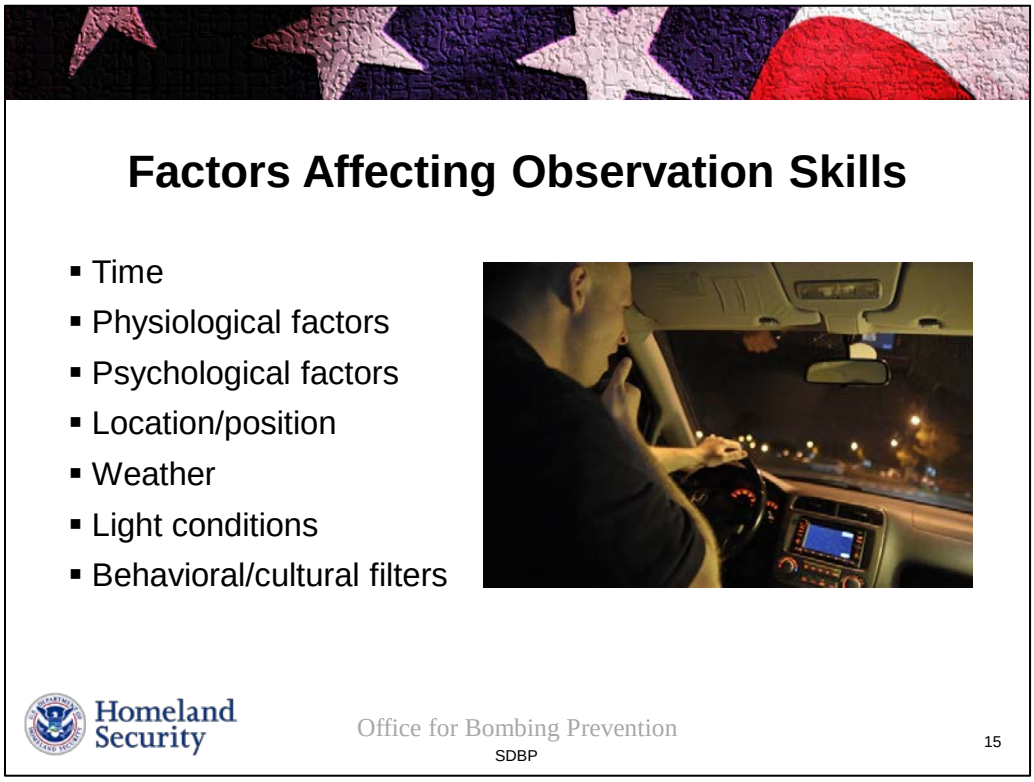
   c. Body type.

   d. Color.

   e. Marks (dents, scratches, etc.).

   f. License plate (State, number, and expiration date).

Media 15



7. **Factors Affecting Observation Skills.** Several factors can affect the accuracy of observation skills. (Sommer 2004)

   a. **Time.** Both time on shift and time of day can affect the accuracy of an observation. If you have been on shift for a prolonged period with no activity, boredom can set in. The mind can wander off the primary task. Time of day can also be a factor. Where the sun is in relationship to the HSP you are surveilling can affect the ability to see clearly.

   b. **Physiological factors.** Physiological factors include everything from vision, hearing ability, and chronic medical problems to simply being really hungry or tired. These factors can alter focus and affect the accuracy of observations.

   c. **Psychological factors.** Psychological factors include stress or worry about a personal or family matter. Prolonged periods of observation, as noted above, can result in the mind “drifting,” resulting in inaccurate observations. Intrusions from outside stimuli can also distract the observer and alter the accuracy of observations.

   d. **Location/position.** The clarity of the view of the HSP or suspicious behavior has a significant effect on how much an observer sees versus how much is inferred by what is seen.

   e. **Weather.** Rain, fog, snow, or any type of inclement weather affects the ability to see what is happening. Heat or cold can also be a physiological factor on the observer that results in distracted observations.

f. **Light conditions.** As stated above, sun position during daylight hours and the location of night lighting affect the ability to accurately see actions and movement.

g. **Behavioral/cultural filters.** Other cultures may have ingrained mannerisms that seem odd compared to your own. You need to distinguish odd/suspicious behavior from that which is culturally based.

Media 16

8. **Communication Plan.** Communication is critical. Communications are both covert and sensitive, so everyone must understand the plan before leaving on shift.

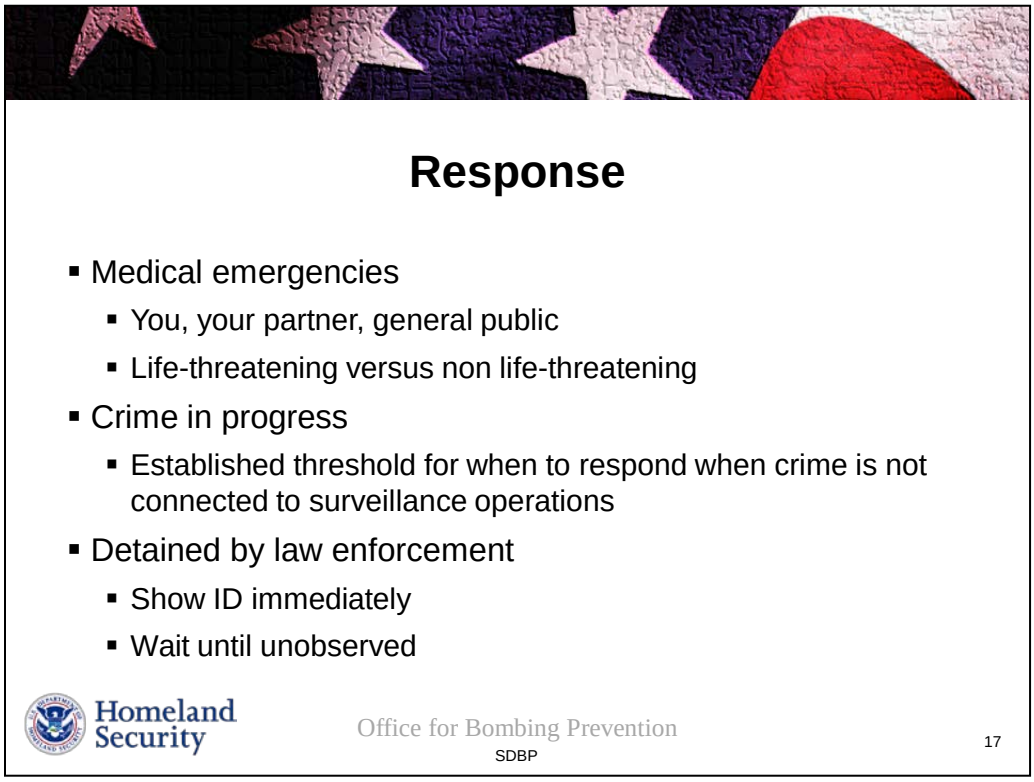
   The communication plan must be written and included in the surveillance detection plan. The communication plan should address the:

   a. Method of communication (cell phone, radio, etc.).

   b. Communication procedures, including radio discipline and the discreet use of cell phones.

   c. Communication security procedures that ensure surveillance detection activity is protected from unauthorized individuals or groups.

Media 17



9. Response. Policies and procedures related to responding to various situations are included in the response element of the surveillance detection plan. This is the fifth and final element of the plan.

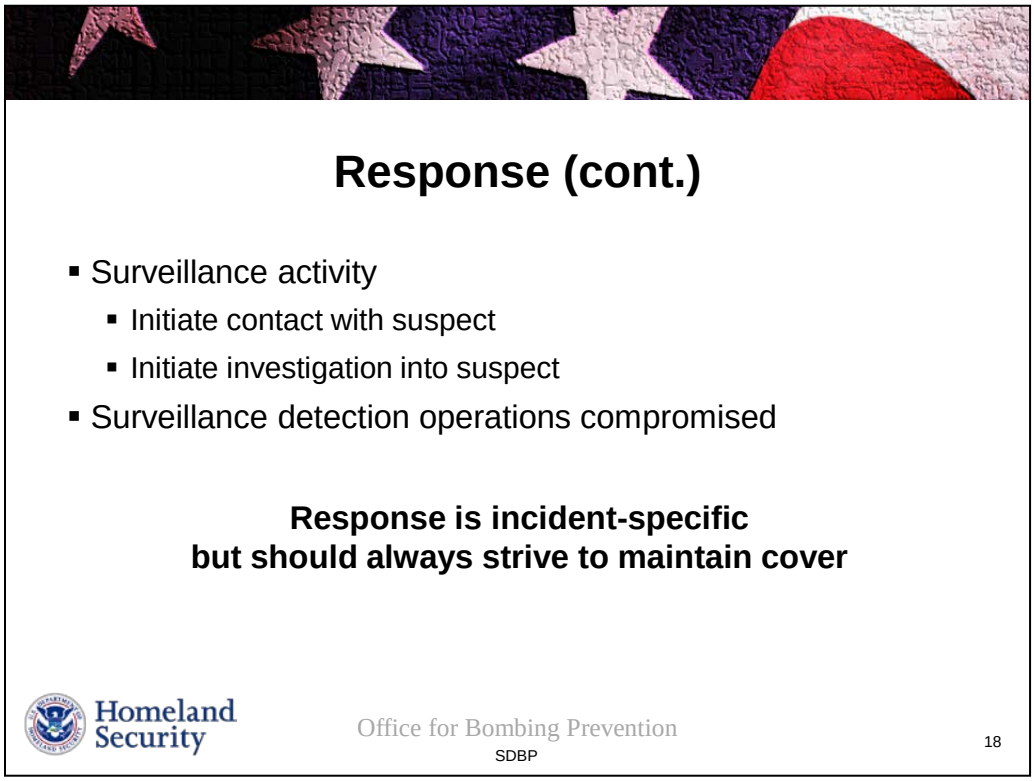
a. There are a variety of situations that should be addressed including:

(1) **Medical emergencies.** Define how to exit if you are ill; who to contact for your partner; how to respond to non-life threatening problems versus life threatening problems with you, your partner, or an innocent bystander you observe.

(2) **Crime in progress.** This includes whether to break your cover or not. Establish a threshold prior to operations for when to respond to a crime that is not connected to surveillance operations.

(3) **Detained by law enforcement.** Immediately show your identification, which might compromise you to a hostile, or have them take you and show your identification when you are alone.

Media 18



(4) **Surveillance activity:** Detain the surveillant or continue observation

(5) **Surveillance detection operations compromised**

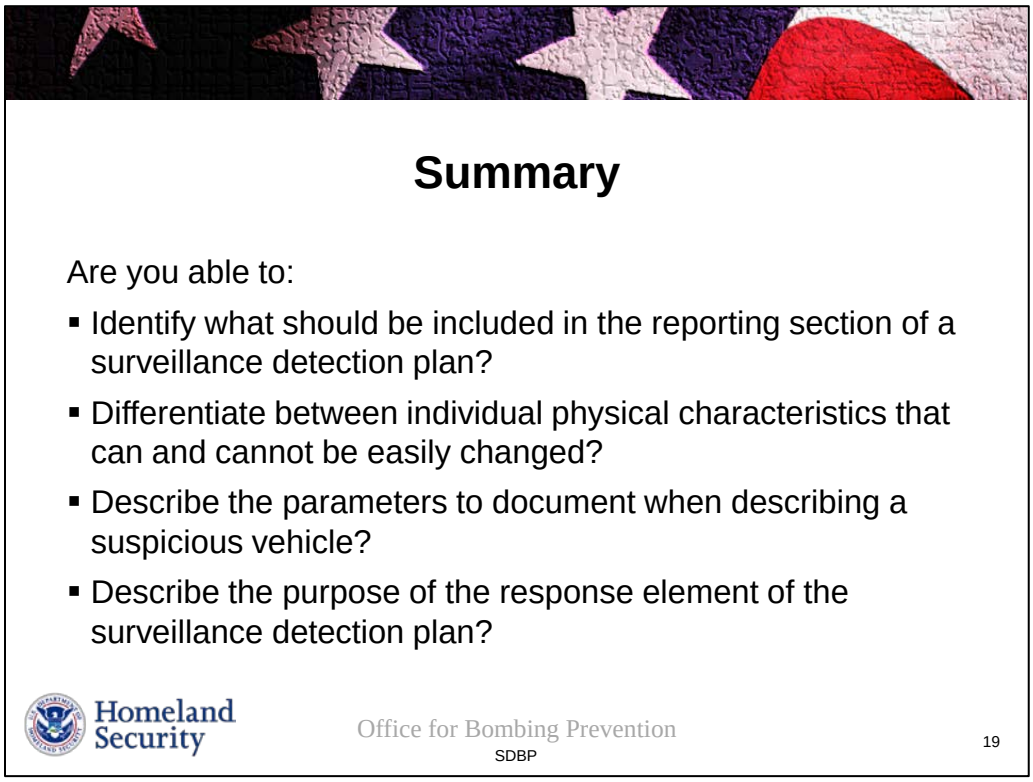
b. There is no set way to respond. Each response is incident specific and based on the agency's policies and standard operating procedures.

c. The appropriate response to an incident should always be determined from a public safety and security personnel perspective. Surveillance detection personnel should always strive to maintain their cover by not engaging with the target.

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 19



10. Summary. This module served to introduce you to the requirements for hostile surveillance. Are you able to:

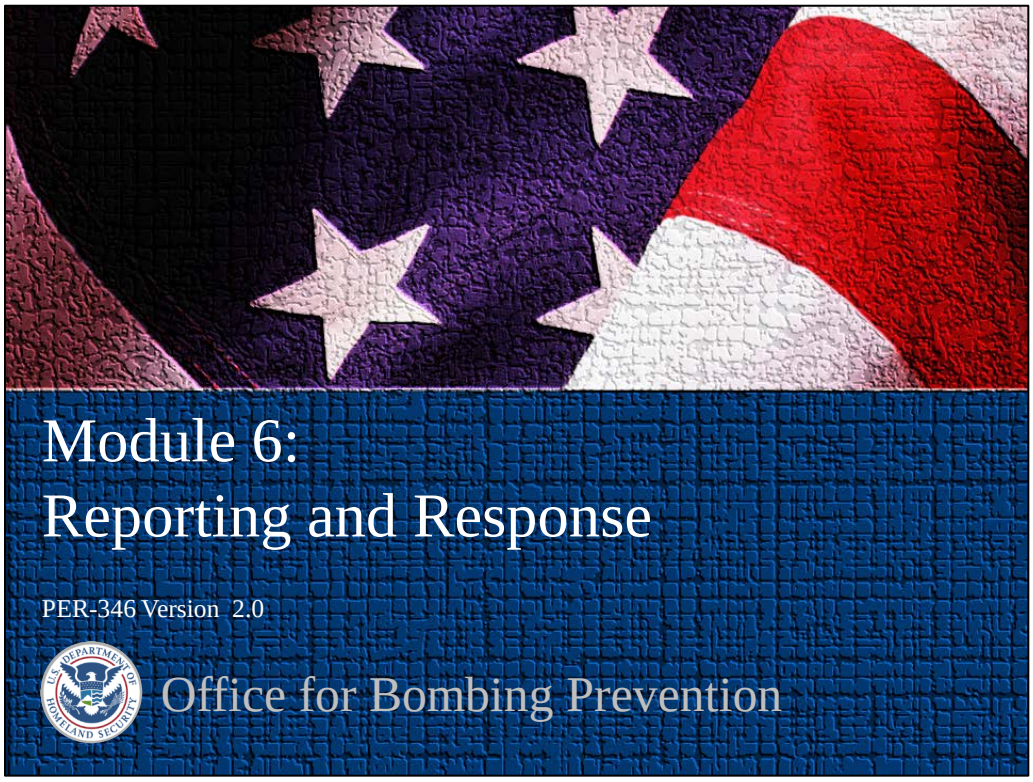
a. Identify what should be included in the reporting section of a surveillance detection plan?

b. Differentiate between individual physical characteristics that can and cannot be easily changed?

c. Describe the parameters to document when describing a suspicious vehicle?

d. Describe the purpose of the response element of the surveillance detection plan?

Media 20


Module 6:
Reporting and Response
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

iluEnglish. n.d. *Describing People: A Person's Physical Appearance.* Accessed July 31, 2017. http://www.iluenglish.com/describing-people-a-persons-physical-appearance/.

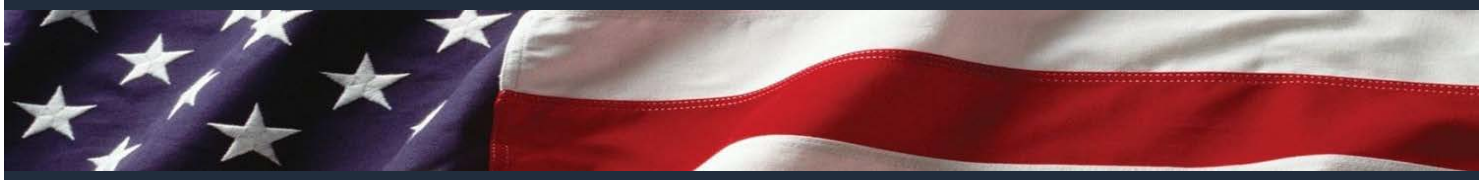
Sommer, Dan. 2004. "Surveillance Detection Skills PowerPoint Presentation."

Toben, Ami. 2016. *Inductive Observation.* February 11. Accessed April 1, 2017. https://protectioncircle.org/2016/02/11/deductive-observation.

—. 2015. *Surveillance Detection -- Tips & Suggestions for Field Operators.* June 16. Accessed April 1, 2017. https://protectioncircle.org/2015/06/19/surveillance-detection-tips-suggestions-for-field-operators/.

—. 2014. *Surveillance Indicators.* March 20. Accessed April 4, 2017. https://protectioncircle.org/2014/03/20/surveillance-indicators.

This page is intentionally left blank.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Module 7: Compromise and Deployment

Participant Workbook

This page is intentionally left blank.

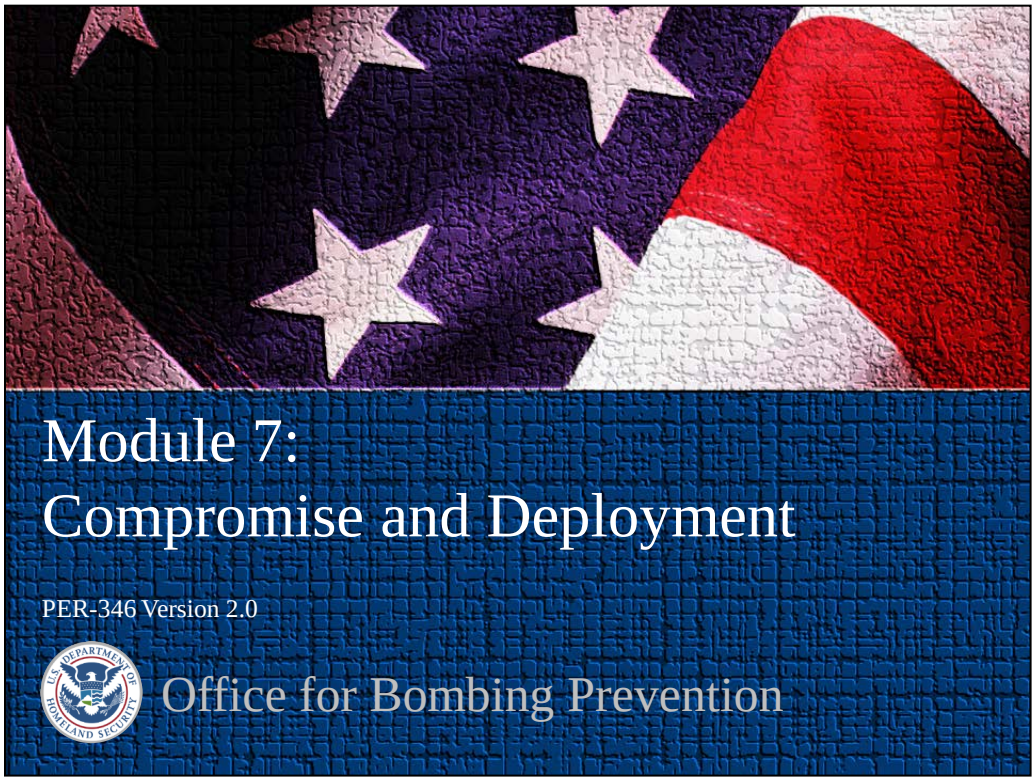
Number: Module 7

Title: Compromise and Deployment

INTRODUCTION

LECTURE ***2 minutes*** ***1:20***

Media 0



1. **Purpose.** This is Module 7: Compromise and Deployment. The purpose of this module is to provide an overview of operational security considerations and responses to being compromised during surveillance detection efforts.

2. **Learning Objective(s)**

   a. **Terminal Learning Objective.** Given a written examination, participants will explain the aspects that must be considered to maintain operational security. (SD-0140)

   b. **Enabling Learning Objectives**

      (1) Given a written examination, participants will identify the various sources of compromise to surveillance detection teams to achieve a minimum score of 70%. (SD-0140a)

(2) Given a written examination, participants will describe the appropriate response to each type of compromise to surveillance detection teams to achieve a minimum score of 70%. (SD-0140b)

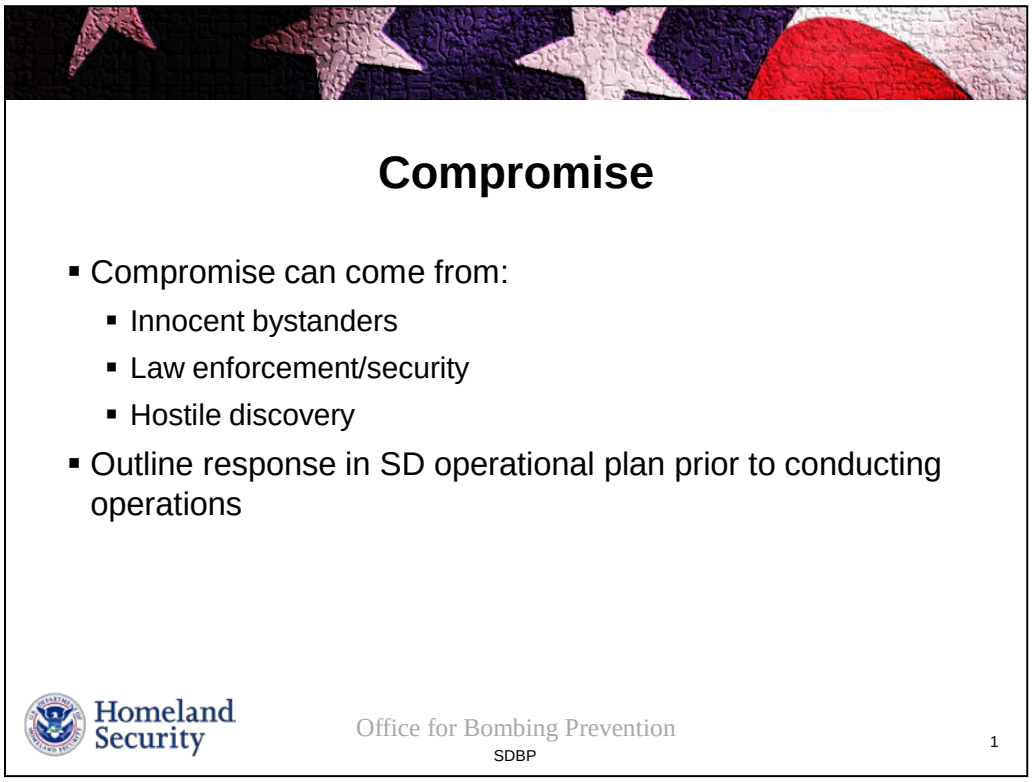
(3) Given a written examination, participants will identify the considerations that affect operational security to achieve a minimum score of 70%. (SD-0140c)

(4) Given a written examination, participants will identify the actions necessary to maintain safety during surveillance detection operations to achieve a minimum score of 70%. (SD-0140d)

BODY

LECTURE/DISCUSSION ***25 minutes*** ***1:20***

Media 1



3. Compromise. Surveillance detection operations can be compromised in a variety of ways.

Media 2

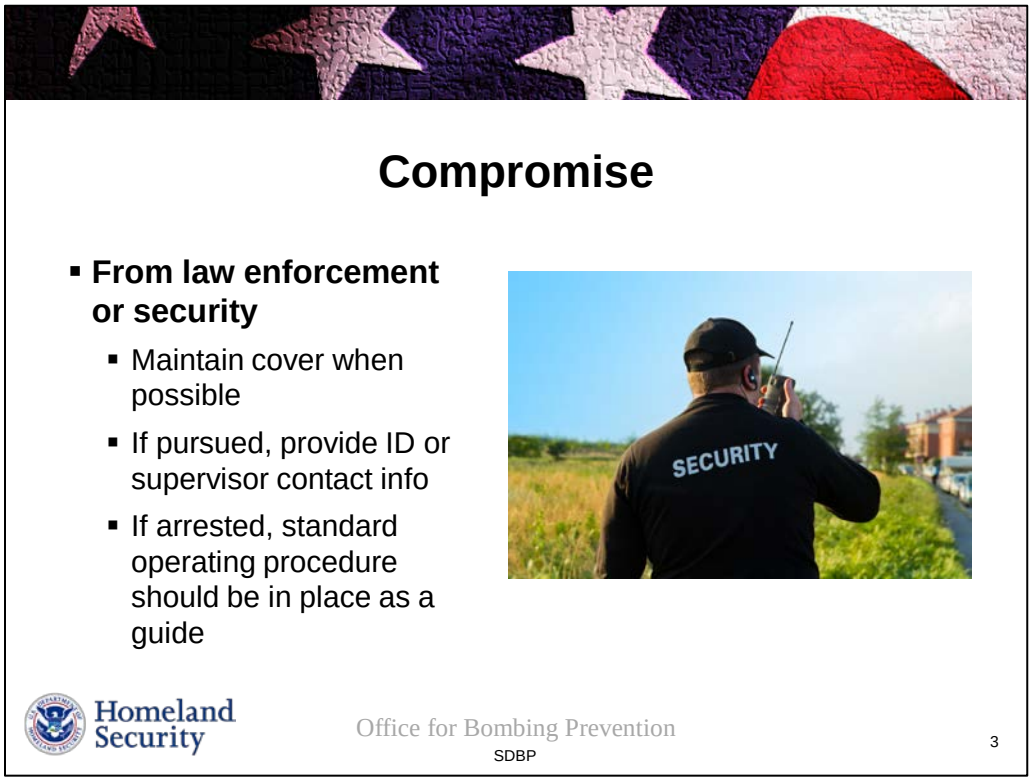
a. Innocent bystanders

(1) Bystanders who do not know you may think you look suspicious and may either confront you or call law enforcement.

(2) Bystanders who do know you, such as friends or neighbors, may call you by name or inadvertently break your cover.

(3) It is preferable to maintain your cover, but situations may arise in which you will need to identify yourself. If that occurs, you should leave the area.

Media 3



b. Law enforcement or security

(1) Maintain cover whenever possible.

(2) If pursued, provide identification or your supervisor's contact information.

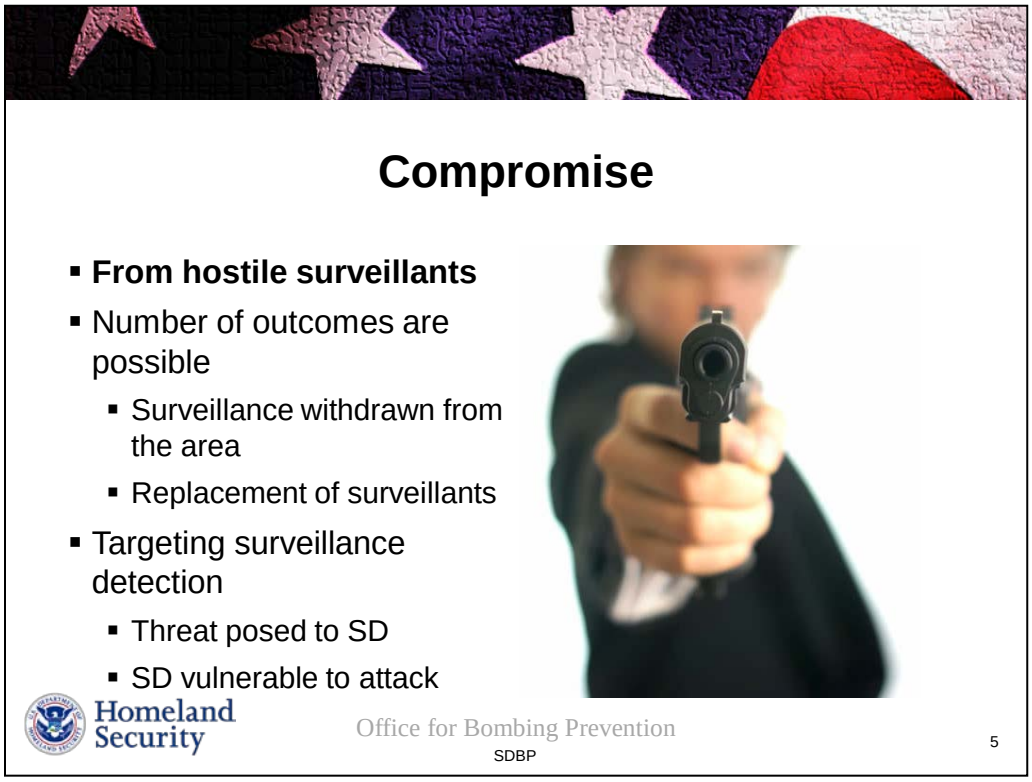
(3) The surveillance detection plan should include a policy on responding to arrest.

(4) Surveillance detection should be coordinated with local law enforcement or other agencies that may also be involved in overlapping operations.

Media 4

Take any notes you feel necessary below.

Media 5



c. Hostile surveillants

(1) There are a number of potential outcomes as the result of compromise from hostile surveillants.

(2) If compromise occurs, surveillance may be withdrawn from the area or other personnel will replace personnel conducting surveillance detection.

(3) Surveillance detection personnel may also be vulnerable to attack by hostile surveillants if they are compromised.

Media 6

4. Compromise Case Study

a. The incident occurred in August 1999 at approximately 11:30 PM. The attacker was a Latin American country-specific national, Antonio Vicenzo Viliae DeLeon.

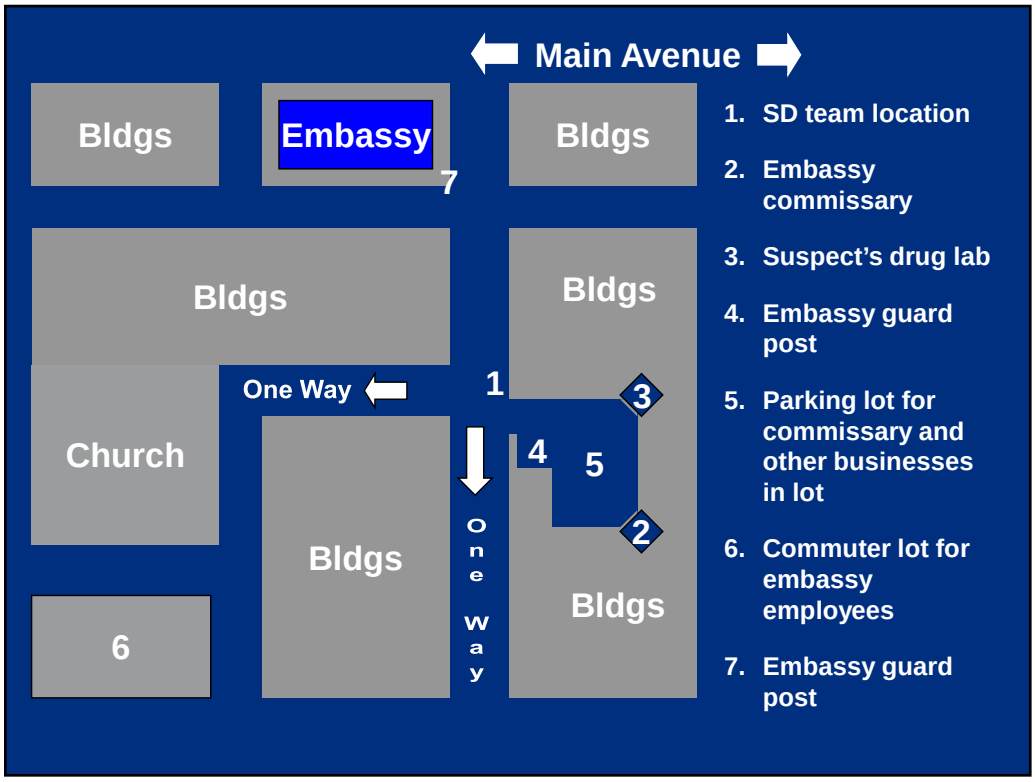
b. According to police, DeLeon was a narcotics trafficker in Latin America.

c. At the time of the attack, he was drunk and on an all-day cocaine high. He was in a rage about his wife trying to leave and divorce him. Afterward, he claimed that he did not know the surveillance detection (SD) team was an embassy security unit. He claims he thought they were either a police counter-drug unit or men hired by his wife to watch him. He said he actually liked the embassy security personnel and was very sorry he attacked them.

d. DeLeon said that at the time of the attack, he was on the way home to kill his wife. After attacking the SD team, he went home, confronted his wife, and shot up the house with a pistol. He did not harm his wife. He was captured five days later in a local Guatemala City hotel.

Take any notes you feel necessary below.

Media 7



e. The SD team was at Location 1 on the map just prior to and during the incident. This location is on a one-way street, just down from the back corner of the American Embassy compound. It is within observation distance of an embassy guard post (Location 7).

f. The guard post (Location 4) is at the junction of two one-way streets (as indicated on the map) and directly in front of a parking lot entrance (Location 5).

g. Inside the parking lot are a number of local businesses and the Embassy commissary (Location 2). Also inside the parking lot was the suspect's cover business, an office supply company (Location 3), which was actually a front for a drug lab and distribution center.

h. The parking lot is a public lot, but it had an embassy guard stationed at the entrance (Location 4) because of the location of the Embassy commissary. In addition, the U.S. Drug Enforcement Agency (DEA) office at the Embassy parked its cars in that lot.

i. Another irony here is that in a subsequent interrogation, the suspect admitted he liked having his drug business in this parking lot because of the security provided by the embassy guard posted at the lot entrance!

Take any notes you feel necessary below.

Media 8

j. Just before the incident, the SD team was parked directly where the maroon and silver SUV is visible in this photo. Note the entrance to the parking lot and the guard post directly in front of the vehicle.

k. Just before 11:30 PM, the suspect pulled out of the parking lot, going the wrong way up the one-way street toward the Embassy. He stopped his car beside the SD team's vehicle, rolled down the passenger window, and demanded to know if the SD team was watching him. The team either denied it or did not answer him. The accounts vary depending on team member. DeLeon left the area.

l. He returned about 10 minutes later, traveling up this street toward the parking lot, again going the wrong way on this one-way street. He entered the parking lot, driving in front of the SD team's vehicle. The team recognized him as the same individual who had confronted them a few minutes earlier, but they took no action.

Take any notes you feel necessary below.

Media 9

Take any notes you feel necessary below.

Media 10

Take any notes you feel necessary below.

Media 11

m. This is the area in front of the parking lot at approximately the same time of night. The Suburban was parked in the same location as the team's vehicle.

n. DeLeon came back to his business; he saw the same car sitting under the light. Therefore, he drove around and came in the wrong way so his headlights shined in their car. He stopped and looked at them, then pulled into the lot. They still did not move. He was then convinced they were after him.

Take any notes you feel necessary below.

Media 12

o. After DeLeon re-entered the parking lot, he parked the blue convertible he was driving and walked over to this Corvette, which he also owned. He extracted an M-16 from the Corvette and moved to the side of the parking lot and toward the building nearest his business. He then began to approach the SD team using the cover of the building.

Take any notes you feel necessary below.

Media 13

p. DeLeon came around the corner of the parking lot entrance near the streetlight pole. The team did not notice his approach until he was standing near the driver's door. DeLeon claimed he rapped on the window with the barrel of the gun and with his finger on the trigger, the gun fired on automatic.

Take any notes you feel necessary below.

Media 14

q. The first burst fired five rounds into the driver's window. Amazingly, the rounds hit neither the driver nor the other front seat SD team member. Bullet holes in the driver's seat and headrest show just how close the rounds came to him. The driver did get hit by some flying glass fragments as the window shattered. After the first five rounds, the M-16 jammed.

r. As DeLeon worked to clear the jammed weapon, the SD team members in the front seat jumped out of the passenger door and began running down the one-way street perpendicular to their vehicle.

Take any notes you feel necessary below.

_____
_____
_____
_____
_____
_____
_____

Media 15

q. The SD team member in the back seat remained in the vehicle.

r. After DeLeon cleared his weapon, he began firing again. At some point, probably in the first burst, or after the jam cleared, two rounds hit the SD team member in the back seat.

Take any notes you feel necessary below.

_____
_____
_____
_____
_____
_____
_____

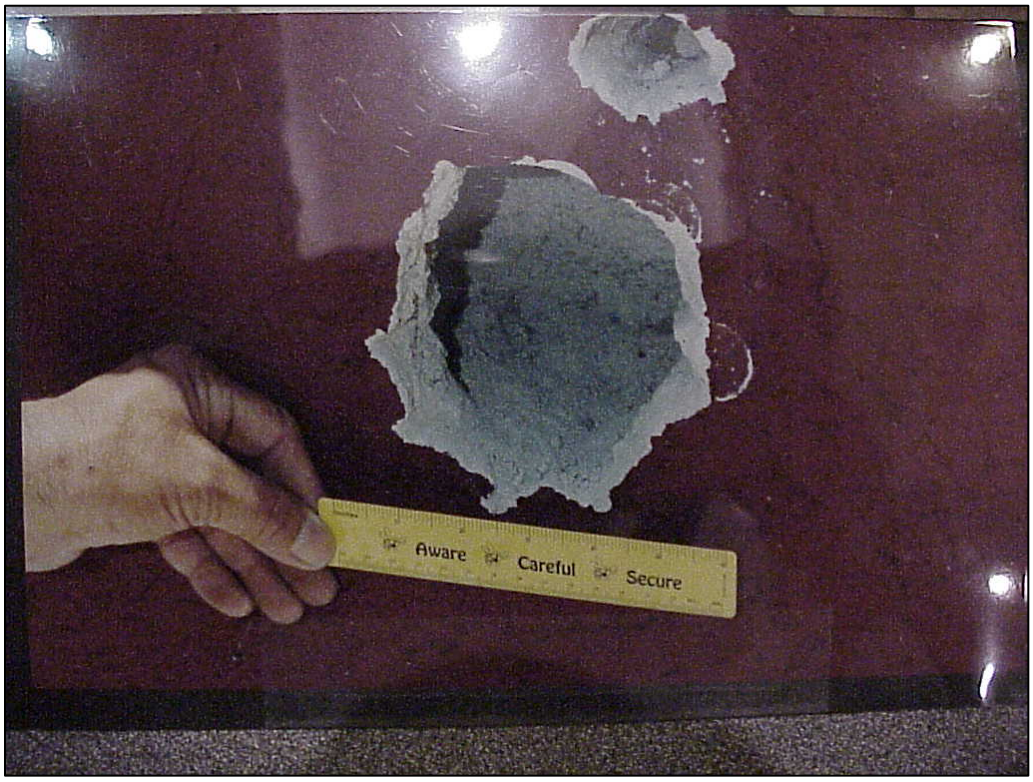
Media 16

s. The team members who fled said it was about 45 seconds between bursts. It was probably closer to 10-15 seconds, as they were still running down this street when DeLeon began firing again.

t. Rounds fired at the fleeing team members struck several buildings down the street, including the red wall halfway down the street on the right side of this picture.

Take any notes you feel necessary below.

Media 17



Take any notes you feel necessary below.

Media 18

u. After DeLeon fled the scene, he went home, took his wife hostage, and after a long standoff was arrested.

Take any notes you feel necessary below.

Media 19

Take any notes you feel necessary below.

Media 20

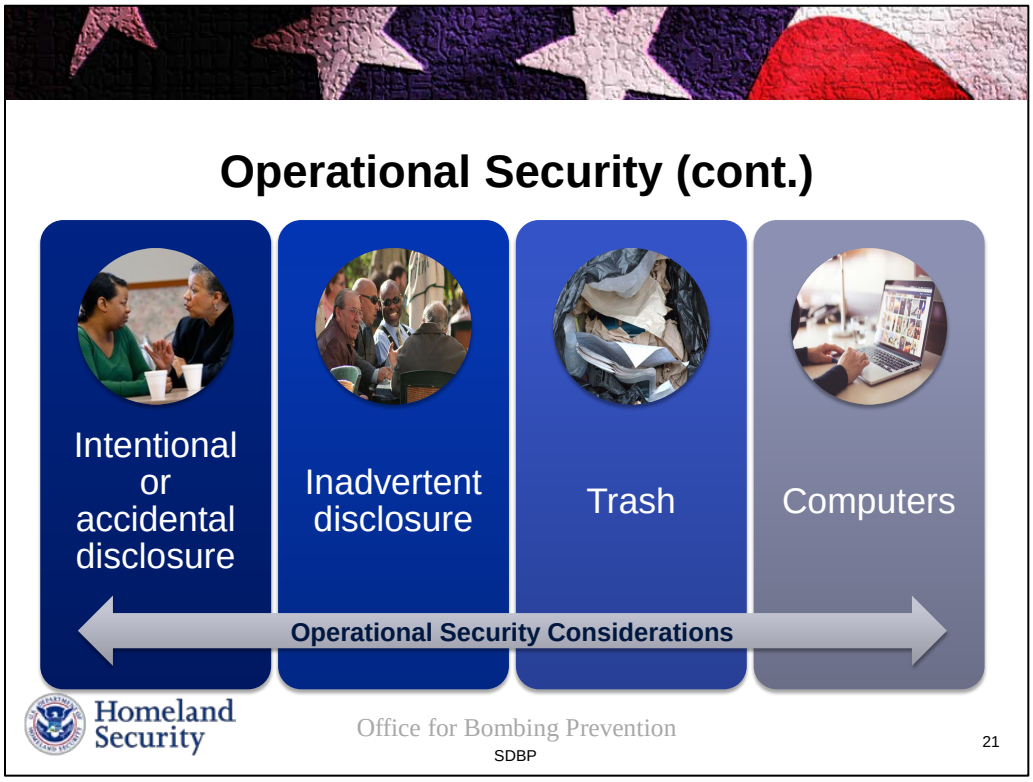
5. **Operational Security.** The safety of the operational security team and the security of surveillance detection operations rely on the ability to deny unauthorized individuals information on how surveillance detection operates. Operational security is critical to continued successful and safe operations.

   a. Operational security procedures should be incorporated into plans and routine training conducted to ensure all team members are aware of and follow those procedures.

   b. Personnel should avoid open contact with law enforcement, security, and corporate personnel.

   c. Coordination between surveillance detection teams should be controlled based on the nature of the working relationship between the program and the department/agency/security staff.

Media 21



d. Operational security considerations include:

(1) Intentionally or accidentally disclosed information.

(2) Inadvertent disclosure of information to family and/or friends during conversation.

(3) Information that is thrown in the garbage or trash.

(4) Information left accessible on open computers.

Media 22

e. Team members need to recognize the sensitivity of their duties/missions and prevent disclosure of information.

(1) Use radio discipline.

(2) Use cell phones discreetly.

(3) Use strong passwords changed regularly and do not leave files open on computers.

(4) Destroy sensitive material appropriately.

Media 23

Deployment

5 Questions

1. What are your capabilities and limitations?
2. How are your detection operational personnel deployed?
3. Where is your focus/what are you looking for?
4. Where does the information go?
5. Who acts on the information?

Homeland Security

Office for Bombing Prevention

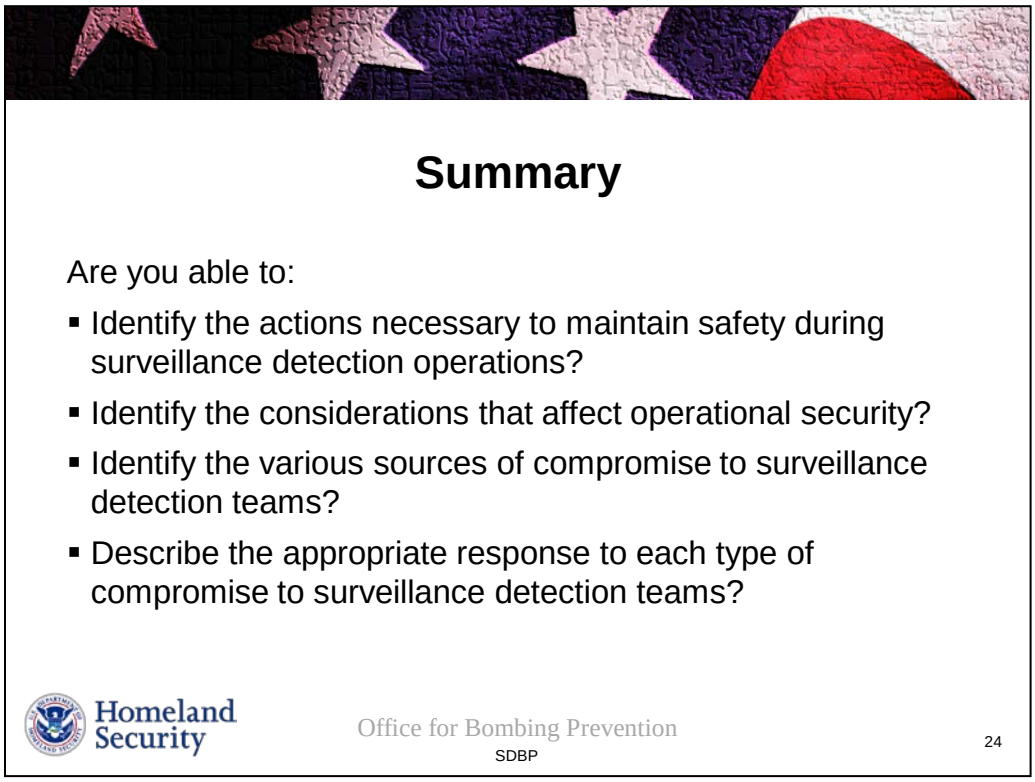
SDBP

23

SUMMARY

LECTURE ***3 minutes*** ***1:20***

Media 24



6. Summary. This module served to introduce you to the requirements for hostile surveillance. Are you able to:

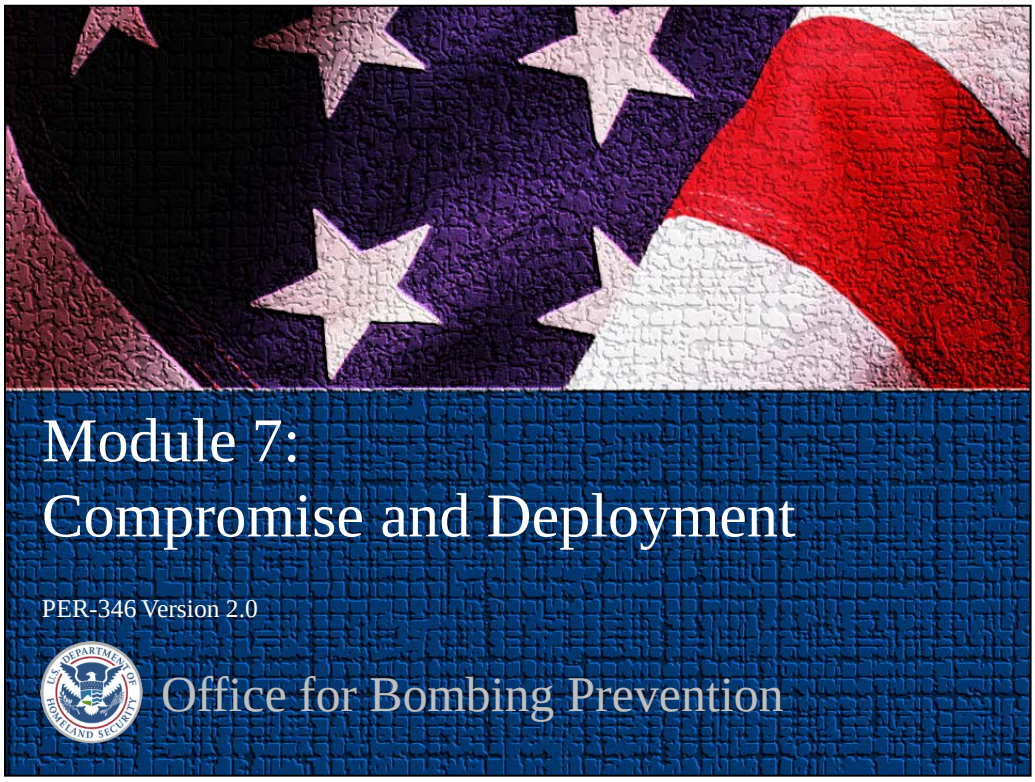
a. Identify the actions necessary to maintain safety during surveillance detection operations?

b. Identify the considerations that affect operational security?

c. Identify the various sources of compromise to surveillance detection teams?

d. Describe the appropriate response to each type of compromise to surveillance detection teams?

Media 25

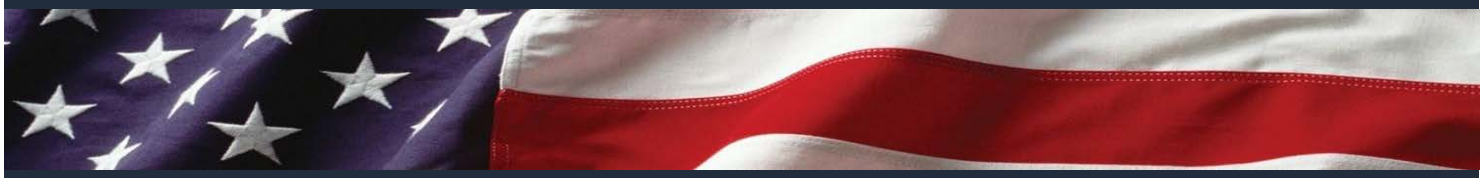

Module 7:
Compromise and Deployment
PER-346 Version 2.0
Office for Bombing Prevention

REFERENCES

Sommer, Dan. 2004. How to be a Successful SD Specialist: The Surveillance Detection Manual. Iceland.

—. 2004. "Surveillance Detection Theory PowerPoint Presentation." Dan Sommer.

Toben, Ami. 2015. Surveillance Detection -- Tips & Suggestions for Field Operators. June 19. Accessed April 4, 2017. https://protectioncircle.org/2015/06/19/surveillance-detection-tips-suggestions-for-field-operators.



Office for Bombing Prevention

Surveillance Detection for Bombing Prevention Course PER-346

v2.0

Experiential Learning Guide Activity 3: Capstone Activity

Participant Workbook

This page is intentionally left blank.

Number: Experiential Learning Activity (ELA) 3

Title: Capstone Activity

Purpose. The purpose of this activity is to provide an opportunity to apply the knowledge and skills presented in the course related to surveillance detection to identify hostile surveillant role players.

Learning Objectives

a. **Terminal Learning Objective.** Given an assigned facility, participants will detect and report hostile surveillance while working against role players as outlined in the activity directions. (SD-0230)

b. **Enabling Learning Objectives**

(1) Given an assigned facility, participants will establish discreet surveillance detection positions according to the parameters discussed in class. (SD-0230a)

(2) Given an assigned facility, participants will ensure the command/control post for communications initiates a basic “collection cycle” and disseminates information. (SD-0230b)

(3) Given actions displayed around a designated facility, participants will apply the correlation level of the SD pyramid to identify hostile surveillant role players according to the parameters discussed in class. (SD-0230c)

(4) Using observations, participants will accurately describe the characteristics of the hostile surveillant role players according to the parameters discussed in class. (SD-0230d)

Learning Event Description. During this learning event, you will return to your assigned facility and conduct surveillance detection with the goal of identifying hostile surveillant role players.

Instructions for Communication Center Team Members

a. Each team will select two team members to remain in the classroom to staff the communication center.

b. Ensure communication team members have the phone numbers of all of your team members in the field.

c. Each team will get one Module 5 Handout 1: Surveillance Detection Activity Matrix and transcribe it to a large easel pad sheet.

d. Team members in the communication center will take reports from their team members in the field and transcribe them to the Surveillance Detection Activity Matrix on the easel pad.

e. You are free and encouraged to share information on sightings and reports in order to help identify correlation behaviors.

f. Regardless of how your team members call in a description, it MUST be written in a professional manner.

Instructions for the Field Team Members

a. The remaining team members will go to the target area to conduct surveillance detection from a point identified in Experiential Learning Activity 2.

b. Team members are to report to the communication center with physical descriptions and activities of potential hostile surveillants by phone or text.

c. Texts are to be sent only to the communication center team and not to all team members.

d. You will receive a text to return to the classroom when the activity is ended. You are to include your lunch during the activity. (The activity should last approximately three hours including lunch and travel time.)

e. Your responsibility for activity safety is the same as the first two activities.

SAFETY BRIEF

Risk Assessment: Moderate. This activity involves controlled practical application requiring substantial exertion. Moderate risk exists for injury to personnel or damage to equipment.

Safety Precautions and Control Measures

a. Physiological stressors such as exertion, heat, cold, or hydration may have significant effects upon some individuals. If you or a fellow participant experience adverse physiological effects, inform an instructor immediately.

b. Psychological stressors may have significant effects upon some individuals. If you or a fellow participant experience adverse psychological effects, inform an instructor immediately.

Cease Training Procedures. If at any time an instructor or participant feels that an unsafe condition exists during an activity, an individual may request for training to stop by contacting the team leader who will contact the instructor. The instructor will assess the situation. The instructor will not commence training until an identified unsafe situation has been resolved and/or appropriate control measures have been implemented to mitigate the risk.

Participant Responsibility for Activity Safety. Along with the instructors and staff, each participant is also responsible for the safety of the activity.

a. Participant Responsibility for Activity Safety

(1) Be vigilant in your observance of safety precautions and associated control measures, and bring any potential concern to the attention of the nearest instructor or staff member as soon as observed.

(2) If a fellow participant or a staff member needs assistance, please aid him/her to the best of your ability without inappropriately risking your own health and/or safety until designated personnel arrive.

(3) You have the option to not participate in a training event if you feel you are physically or emotionally unable to perform the designated actions or skills. Immediately notify an instructor should you have concerns about participating in a training event.

(4) A participant may be prohibited from participating in a training event if perceived by any staff member as being physically and/or cognitively impaired by drugs, alcohol, or other substances.

b. Safety Takes Priority Over Activity Events

(1) If directed by an instructor or other designated personnel to stop training, evacuate an area, assist a staff member or participant, etc., immediately do so to the best of your ability. The safety of all personnel will take priority over the training activity.

(2) If you sense yourself or others becoming overly fatigued, dehydrated, or otherwise compromised to an unsafe extent, contact an instructor and mitigate the situation as soon as possible.

Inclement Weather. In the event of inclement weather, such as excessive heat or cold, tornadoes, thunderstorms, etc., safety protocols may determine changes in training activities and their locations. This practice is to ensure the safety of all participants and provide a safe environment to complete event objectives.

Hazards. Due to the unique training environment, there may be a wide array of walking/working surfaces and hazards. All participants must be aware of hazards that may cause slips, trips, falls, collisions, etc. within the training area. Any participant identifying a hazard requiring mitigation should notify an instructor.

Participant Behavior. Aggressive behavior will not be tolerated during the event. Examples of aggressive behavior may include hostile communications, excessive use of force, or inappropriate use of response equipment.

Additional rules for the activity are included in the Threat Portfolio Briefing. These include:

a. Never enter your assigned facility through illegal or deceptive means.

b. Conduct all activities within the public areas of the facility only, and do not disrupt operations at the facility.

c. Do not engage or otherwise alert potential hostile surveillants to surveillance detection (SD) efforts in area unless presented with exigent circumstances (disrupt an attack, prevent loss of life, etc.).

d. Do not overtly engage or otherwise communicate with contracted security personnel, employees, law enforcement officers (LEOs), or other SD team members (unless it is part of your cover).

e. If you experience any emergency (medical or criminal), contact 911, then contact the instructor.

f. Follow established agency/department policy if you encounter illegal activity.

This page is intentionally left blank.

Office for Bombing Prevention

Copyright and Usage Notice: Unless a copyright is indicated, information contained herein is in the public domain and may be copied and distributed without permission. Citation of the U.S. Department of Homeland Security as a source of the information is appreciated. If a copyright is indicated on a photo, graphic, or other element, then permission to copy these materials must be obtained from the original source.