# MODULE 8: SURVEILLANCE AWARENESS: WHAT YOU CAN DO

**Day**: 3 **Time:** 1.0 Hour **Level of Understanding:** Comprehension

Instructional Strategies:
- Lecture
- TeachBack Moment

Module Equipment/Facilities:
- Standard Classroom Setup

Participant Materials/Handouts:
- Workbook 8.1: Critical Infrastructure as Targets
- Workbook 8.2: Indicators of Hostile Surveillance Activities

## Terminal Learning Objective

By the end of this module, you will be able to explain the actions necessary to detect and report suspicious activities associated with hostile surveillance.

## Introduction

Terrorist organizations make it very clear through both their rhetoric and actions that they will continue to strike out against entities that are contrary to their beliefs and intentions. Terrorist organizations are extremely dedicated to their respective causes, patient and thorough in their preparation, well trained in their techniques, and increasingly sophisticated in their tactics. Their attack planning involves extensive advance surveillance of target facilities or personnel in order to gather the necessary information to formulate and execute an attack plan. If you detect and report suspected hostile surveillance during an early phase of attack planning, prevention or deterrence of a potential attack may be possible.

By becoming aware of the surveillance indicators and using the reporting processes covered in this module, you will reduce your vulnerability to a terrorist or other criminal attack. Additionally, your chances of identifying hostile surveillance behavior and activities in and around your critical infrastructure facilities and personnel during the pre-attack planning stage will increase. This proactive approach to security observation and reporting will allow your agency or organization to take preventive measures that might discourage or preclude a possible terrorist attack.

## Module Topics

An outline of key topics and an approximate time plan are shown below.

| Topic | Enabling Learning Objectives | Approximate Time |
|---|---|---|
| Module Introduction | ▪ Not Applicable | 5 minutes |
| Understanding | ▪ Describe the information obtained by surveillance that is of interest to | 5 minutes |

| Topic | Enabling Learning Objectives | Approximate Time |
|---|---|---|
| Surveillance | hostile surveillants. | |
| Potential Targets of Surveillance | ▪ Identify potential targets of hostile surveillance. | 5 minutes |
| Hostile Surveillance | ▪ Describe indicators of surveillance within the everyday environment. | 10 minutes |
| Detecting Surveillance | ▪ Identify actions that you can take to detect potential hostile surveillance incidents. | 20 minutes |
| Reporting Suspicious Activities | ▪ Describe the importance of identifying and reporting suspicious activities associated with hostile surveillance.<br>▪ Specify actions you can take to report potential incidents of hostile surveillance. | 10 minutes |
| Module Summary | ▪ Not Applicable | 5 minutes |

The module times are guidelines only. The actual time required may vary based on the experience level and interest of the participants or other factors encountered during the training session.

**Key Terms**

| Key Term | Description |
|---|---|
| Countersurveillance | A reactive and offensive security measure used to confirm whether hostile surveillance is occurring |
| Hostile surveillance | The discreet monitoring of a person, facility, or area with the intent of gathering information to formulate a plan that will enhance the likelihood of a successful terrorist operation or attack |
| Surveillance | The monitoring of a person, facility, or area with the intent of gathering information, generally through discreet observation |
| Surveillance detection | A defensive security operation used to determine whether a person or persons are conducting hostile surveillance; conducted temporarily or (for some critical infrastructures) permanently by an individual or full-time by a trained team to observe, recognize, and confirm suspicious activities |
| Surveillant | A person conducting surveillance |

| **Topic: Module Introduction** | **5 Minutes** |
|---|---|

| **Slide 1 Surveillance Detection Overview** |
|---|
| ▪ Title Slide |
| *Graphic Description: US Flag and Seal* |

## Module Preparation

- **Timing and Methods:** Use the suggested time plan at the beginning of the module. As with all modules in this course, read all the content (Facilitator Guide and PowerPoint slides) and familiarize yourself with each facilitator note before class.
- Be thoroughly prepared for exercises, discussions, or other activities required for the module. Follow all facilitator notes. Use a combination of lecture, large-group discussion, small-group activities, and TeachBack moments.

## Orientation to Participant Guide

- When beginning this module:
  - Refer participants to the beginning of this module in the Participant Guide.
  - Note the list of workbook sections the participants will use during this module.
  - Explain that instructions for all exercises are included in the addendums.
  - Review the key terms before beginning the module.

| **Slide 2 Module Objective** |
|---|
| ▪ By the end of this module, you will be able to explain the actions necessary to detect and report suspicious activities associated with hostile surveillance |
| *Graphic Description: No Graphic* |

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Understanding Surveillance
  - Potential Targets of Surveillance
  - Hostile Surveillance
  - Detecting Surveillance
  - Reporting Suspicious Activities
- Explain that this module will help law enforcement officers, security personnel, critical infrastructure employees, service providers, and the community become more aware of actions they can take to detect and report suspicious activities associated with hostile surveillance.

## Topic: Understanding Surveillance — 5 Minutes

Enabling Learning Objective:

- Describe the information obtained by surveillance that is of interest to hostile surveillants.

### Slide 3 What Is Surveillance?

- The monitoring of a person, facility, or area with the intent of gathering information, generally through discreet observation
- Law enforcement and security personnel actions

*Graphic Description: Man with camera hiding behind plant*

- Define **surveillance:** the monitoring of a person, facility, or area with the intent of gathering information, generally through discreet observation.
- Tell participants that the word surveillance comes from the French word for "watching over."
- Explain that law enforcement and security personnel use surveillance to identify behaviors, activities, and other changing information.

### Slide 4 Important Surveillance-Related Terms

- Surveillant
- Hostile surveillance
- Surveillance detection
- Countersurveillance

*Graphic Description: Man sitting outside with laptop open but looking out over screen*

- Define the following terms:
  - **Surveillant:** a person conducting surveillance
  - **Hostile surveillance:** the discreet monitoring of a person, facility, or area with the intent of gathering information to formulate a plan that will enhance the likelihood of a successful terrorist operation or attack
    - Distinguished by its criminal purposes, which may include domestic and international terrorism, crimes against individuals or particular groups, espionage, theft, or stalking
    - May also include destruction of property and life
  - **Surveillance detection:** a defensive security operation used to determine whether a person or persons are conducting hostile surveillance; conducted temporarily or (for some critical infrastructures) permanently by an individual or full-time by a trained team to observe, recognize, and confirm suspicious activities

- **Countersurveillance:** a reactive and offensive security measure used to confirm whether hostile surveillance is occurring
  - Has the same initial purpose as surveillance detection but includes an additional reaction component
  - Conducted by law enforcement when hostile surveillance has been established or is greatly suspected

| **Slide 5 Who Can Detect Hostile Surveillance?** |
|---|
| ▪ Everyone working together serves as a force multiplier in protecting critical infrastructure and the community as a whole<br>• Members of the community<br>• Critical infrastructure employees<br>• Critical infrastructure security personnel<br>• Law enforcement |
| *Graphic Description: No Graphic* |

- Explain that surveillance detection is not limited to law enforcement personnel.
- Explain that everyone working together serves as a force multiplier in protecting critical infrastructure and the community as a whole.
- Tell participants how the following groups may be part of surveillance detection:
  - Members of the community
    - Using community awareness programs such as "See Something, Say Something"
    - Knowing what is usual and unusual in their community
    - Reporting unusual behavior or suspicious activities to law enforcement
  - Critical infrastructure employees
    - Participating in employee awareness training
    - Knowing what is usual and unusual in their areas of responsibilities
    - Reporting unusual behavior or suspicious activities to security personnel
  - Critical infrastructure security personnel
    - Providing and participating in employee awareness training
    - Observing what is usual and unusual in their areas of responsibilities
    - Reporting unusual behavior or suspicious activities to law enforcement personnel
    - Maintaining an incident log or database of all suspected and confirmed incidents in or near the critical infrastructure
    - Analyzing suspected and confirmed incidents that occur in or near the critical infrastructure
  - Law enforcement
    - Conducting a surveillance detection operation on high-threat assets — Note: inform participants that ATA has a nine-day course on Surveillance Detection
    - Countersurveillance on reports of surveillance
    - Maintaining incident database
    - Identifying hostile operatives
    - Analyzing data from all sources
    - Gathering intelligence

- Sharing information

| **Slide 6 Information Collected through Hostile Surveillance** |
|---|
| ▪ Depends on type of target and attack<br>▪ Information about facilities, personnel, and procedures<br>▪ Information about special events |
| *Graphic Description: No Graphic* |

- Explain that there is an unlimited amount of information that can be collected by hostile surveillance — the information collected depends upon the target and type of attack that is being planned.
- Tell participants that some common types of information are:
  - Information about facilities and personnel
    - Locations and numbers of security personnel and cameras
    - Facility layout, including access and egress routes
    - Security and visitor processes and procedures
    - Crowd data (determine when will the site be most crowded)
    - Timing of routine procedures or occurrences
    - Security equipment, including badges and uniforms
    - Maintenance and cleaning personnel and procedures
    - Access requirements for restricted or employee-only areas
    - Parking facility access and operations
  - Information about special events
    - Event-specific information
    - Event timing
    - Arrivals and departures of notable guests
    - Crowd data (when the event or venue might be the most crowded during the event)
    - Access requirements for those attending the event
    - Parking facility access and operations

## Topic: Potential Targets of Hostile Surveillance — 5 Minutes

Enabling Learning Objective:
- Identify potential targets of hostile surveillance.

**Slide 7 Categories of Critical Infrastructure as Targets (1 of 2) (Workbook 8.1)**

- Banking and finance
- Chemical sector
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services

*Graphic Description: No Graphic*

**Slide 8 Categories of Critical Infrastructure as Targets (2 of 2) (Workbook 8.1)**

- Energy
- Food and agriculture
- Government facilities and national monuments
- Health care and public health facilities
- Information technology
- Nuclear reactors, materials, and waste
- Transportation, postal, and shipping systems
- Water

*Graphic Description: No Graphic*

- Remind participants of the categories of critical infrastructure discussed in *Module 2: Introduction to Critical Infrastructure Security and Resilience*.
- Refer participants to **Workbook 8.1: Critical Infrastructure as Targets of Attack**.
- Use the addendum to discuss the two or three categories that are most relevant to the participants' nation and how those categories are vulnerable to terrorist attacks.

**Slide 9 Target Selection Surveillance**

- Location and surroundings
- Access, egress, or vulnerabilities
- Usual activities
- Security systems
- Other relevant information

*Graphic Description: Security officer sitting in front of a bank of security system monitors*

- Explain that when planning their attack, terrorists may conduct surveillance at multiple sites to learn all they can about potential targets to help them select the target that offers the most likelihood of a successful attack:
  - The location and the surrounding area
  - Building or structure access, egress, or vulnerabilities
  - Usual or routine activities of employees, suppliers, customers, and visitors
  - Security protocols, equipment, monitoring systems, or any other elements of a physical or electronic security system
  - Other relevant information that will help plan a successful attack

| **Slide 10 Pre-Attack Preparation** |
| --- |
| ▪ Scope determines length of preparation<br>▪ Hostile surveillance<br>▪ Security system tests<br>▪ Repeated visits — most vulnerability for operative<br>▪ Acquisition of supplies and materials<br>▪ Practice or rehearsals<br>▪ Detection and halting attack most likely |
| *Graphic Description: No Graphic* |

- Explain that the scope of the planned attack will determine whether terrorists conduct pre-attack preparations such as those listed below over a period of months or even years.
  - Surveillance of physical and activity elements of the site
  - Security system tests of the physical barriers, electronic monitoring, or security personnel at access and egress points
  - Repeated visits to the location to collect needed information about the potential target may take place over several days, weeks, or months — this repetition places the terrorist in a very vulnerable position to be detected
  - Acquisition and assembly of supplies and materials to make explosives, places of concealment, or necessary elements of a cover story
  - Practice or rehearsals at the selected or similar site of the planned attack
- Explain that terrorist activities are most likely to be detected during pre-attack preparation, so the likelihood of halting an attack is highest at this time.

## Topic: Hostile Surveillance — 10 Minutes

Enabling Learning Objective:
- Describe indicators of surveillance within the everyday environment.

**Slide 11 Indicators of Hostile Surveillance Activities (1 of 2) (Workbook 8.2)**

- Making observations with vision-enhancing devices
- Drawing maps or diagrams
- Asking for more than routine information
- Taking notes about observable security

*Graphic Description: No Graphic*

**Slide 12 Indicators of Hostile Surveillance Activities (2 of 2) (Workbook 8.2)**

- Charting crowd patterns
- Putting documents in a pocket
- Photographing anything related to security
- Observing or taking notes about responses to a security breach
- May include both people and vehicles

*Graphic Description: Man photographing building in downtown area*

- Refer participants to **Workbook 8.2: Indicators of Hostile Surveillance Activities**.
- Explain that many innocent activities — when observed in the area of critical infrastructure — may be considered indicators of hostile surveillance activities:
  - Drawing maps or diagrams
  - Observing employees and facilities using vision-enhancing devices (for example, binoculars, still and video cameras, and night vision goggles)
  - Asking employees for information that goes beyond the usual routine questions, especially about regular routines, security procedures, or delivery schedules
  - Taking notes about security and routines
  - Charting crowd patterns at access and egress points and through mechanical chokepoints such as elevators or gates
  - Pocketing documents — even a seemingly innocent page of notepaper may be significant if it has a company logo or an executive's name printed on it
  - Photographing any sort of security equipment, badges, or apparel
  - Observing or taking notes about the response of security personnel after attempting unauthorized access or witnessing a security breach
  - Discuss the information in the addendum about both people and vehicle surveillance.

**Slide 13 Unusual Hostile Surveillant Behavior (1 of 2)**

- Attempting to hide when observed
- Reacting visibly to security events of interest
- Making sudden turns or stops
- Making visible hand or other signals
- Running immediately when detected
- Hiding, averting the face, or bending down to avoid detection

*Graphic Description: No Graphic*

**Slide 14 Unusual Hostile Surveillant Behavior (2 of 2)**

- Failing to have a valid reason to be in a location
- Engaging in activities not normally conducted in a location
- Dressing inappropriately for the environment

*Graphic Description: Man covering face near large machinery*

- Explain that obvious unusual behavior can indicate hostile surveillance.
- Examples of obvious unusual behavior can be a hostile surveillant who:
  - Attempts to hide as soon as you observe him or her
  - Reacts visibly to events of interest such as security guard movements by moving, communicating, or taking notes
  - Makes sudden turns or stops, such as turning around abruptly and entering a doorway
  - Makes visible hand or other signals to communicate with others on the team
  - Runs away immediately to quickly flee the area when detected
  - Hides and averts his or her face, or bends down behind a barrier to avoid detection
  - Fails to have a valid reason to be in a particular location
  - Engages in activities not normally conducted in a particular location
  - Dresses inappropriately for the environment:
    - Wearing overly casual clothing in a professional environment
    - Wearing business or formal attire while claiming to be a maintenance or other type of custodial employee
    - Wearing accessories that hide or disguise his or her appearance

**Topic: Detecting Surveillance** **20 Minutes**

Enabling Learning Objective:

- Identify actions that you can take to detect potential hostile surveillance incidents.

**Slide 15 Surveillance Can Be Detected**

- Weak link in the preparations for an attack
- Surveillants are vulnerable due to:
  - The time needed for surveillance
  - The likelihood of repeated visits to the same site

*Graphic Description: Man on cell phone in urban area*

- Explain that, as terrorists or criminal organizations prepare to launch an attack against a critical infrastructure site, surveillance can be the weak link in the preparation process.
- Explain that surveillants conducting surveillance are vulnerable due to the time needed for the surveillance to gain all of the needed information:
  - Surveillance may take place over several days, weeks, or longer
  - The need to make repeated visits to the same site to continue information gathering or updating

**Slide 16 Trained and Untrained Surveillants**

- Highly trained individuals or teams may use:
  - Sophisticated observation equipment
  - Multiple forms of transportation
  - The cover of posing as families or tourists
- Untrained surveillants are:
  - Not well equipped
  - Vulnerable to detection due to their inexperience

*Graphic Description: No Graphic*

- Explain that surveillance conducted by highly trained individuals or teams may employ:
  - A variety of sophisticated surveillance equipment
  - Multiple forms of transportation
  - Cover stories by acting like families or tourists to gain access to and probe selected targets
- Explain that untrained surveillants involved in planning terrorism are:
  - Not always well equipped
  - More vulnerable to detection by employees, passersby, and others because of their inexperience

**Slide 17 How to Detect Hostile Surveillance**

- Know what is normal in order to detect what is abnormal
  - Notice the indicators of surveillance
  - Evaluate surveillance-related activities
- Determine whether they seem unusual or out of place

*Graphic Description: Hands holding cell phone taking photo of national monument*

- Explain that knowing what is normal in a law enforcement officer's area of responsibility helps the officer know what is abnormal.
- Explain that, to detect surveillance by a hostile surveillant, an officer:

  - Should take note of observed activities that are typically associated with indicators of surveillance, such as watching a location or recording information about it over time
  - Evaluate any observed surveillance-related activities to determine whether they seem unusual or noteworthy
- Explain that surveillance activities will appear unusual and out of place.

| **Slide 18 Look for Unusual Activities — Examples 1 and 2** |
|---|
| 1. An individual is observed one time with a tripod-mounted camera and is openly taking photographs of a critical infrastructure<br>2. A person is observed on repeated occasions taking several quick secretive photos of a critical infrastructure with a cell phone from several locations |
| *Graphic Description: No Graphic* |

- Ask one participant to read each example on the slide.
- Ask another participant to describe what is unusual about the surveillance example.
- Ask the class what surveillance indicators they see in the example — they can use Addendum 8.2 to provide responses.
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Attempting to hide position, location, or photo-taking activity*
  - *Returning several times to take photos of the same location*

| **Slide 19 Look for Unusual Activities — Examples 3 and 4** |
|---|
| 3. An individual is taking photographs of everything notable in a popular tourist area and includes companions in the photographs<br>4. An individual is photographing building entrances, windows, or security personnel or features and does not include companions in the photos or video |
| *Graphic Description: No Graphic* |

- Ask one participant to read each example on the slide.
- Ask another participant to describe what is unusual about the surveillance example.
- Ask the class what surveillance indicators they see in the example — they can use Addendum 8.2 to provide responses.
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Focusing on security-related areas*
  - *Not including companions*

| **Slide 20 Evaluating Unusual Activities (1 of 2)** |
|---|
| ▪ Isolated unusual activity may not necessarily indicate hostile surveillance<br>▪ Evaluate all observed actions and behaviors in context |
| *Graphic Description: Man taking photo of high-rise structure with cell phone* |

- Tell participants that unusual surveillance-related activity by itself may not necessarily be an indicator of adversarial surveillance.
- Explain that an officer must assess and evaluate the totality of observed actions and behaviors as well as other relevant circumstances in the environment — for example, a person may be interested in building doors or entrances for a variety of innocent reasons, and the officer may observe him or her taking photos of many ornate doors in a tourist area.

**Slide 21 Evaluating Unusual Activities (2 of 2)**

- Consider behaviors to be suspicious if there are additional unusual behaviors observed:
  - Repeated visits to same location
  - Disguised interest in location
  - Focused interest in alarms, security features or personnel, or restricted areas

*Graphic Description: No Graphic*

- Clarify that participants should consider the person's behavior to be suspicious and should report the situation if the person displays additional unusual behaviors, such as:
  - Making repeated visits to the same location to record or document something about the doors or entrances
  - Attempting to disguise an interest in the doors or entrances
  - Displaying more of an interest in alarms, security features and personnel, or in restricted or employee-only entrances

**Slide 22 Discussion — Scenario 1**

- Ray is crossing the street toward the Law Enforcement Training Academy and sees someone taking photos of the building entrance with a camera
- The person taking the photos is sitting inside a car parked across the street from the building
- The car window is closed and the person is hunched over inside the car

*Graphic Description: No Graphic*

- Explain that in each of the following scenarios, an employee or passerby has observed an unusual activity that could involve hostile surveillance at the location.
- Ask one participant to read the scenario on the slide.
- Instruct participants to identify any aspects of the situation that seem unusual.
- Tell participants they may use Addendum 8.2 to assist with their responses.
- Ask participants: **In Scenario 1, what is unusual about this person's activities?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Taking photos from a car rather than out in the open*
  - *Taking photos with the window closed*
  - *Attempting to hide in the car*

**Slide 23 Discussion — Scenario 2 (1 of 3)**

- People gather across the street from Law Enforcement Headquarters near a bus stop every day
  - The bus comes at the same time every hour
  - People who are waiting check often for an approaching bus and look at their watches or cell phones frequently
  - They typically wait less than 20 minutes

*Graphic Description: No Graphic*

**Slide 24 Discussion — Scenario 2 (2 of 3)**

- One day, you notice a man sitting at the bus stop and writing in a notebook
  - When you look up again almost an hour later, the man is in the same location
  - He does not look up as a bus approaches

*Graphic Description: No Graphic*

- Ask one participant to read the scenario on the slides.
- Instruct participants to identify any aspects of the situation that seem unusual.
- Ask participants: **In Scenario 2, what is unusual about this person's activities?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *The man does not get on the bus*
  - *Writing in a notebook at the bus stop*
  - *Does not look up as a bus approaches*
  - *Waiting, writing, but not taking the bus*
  - *Not looking at the bus but at the building*

**Slide 25 Discussion — Scenario 2 (3 of 3)**

- You see him several more times in the following week at different times of the day
  - He waits for an hour or more each time, writing in his notebook
  - He looks up often, but only toward the building

*Graphic Description: No Graphic*

- Conduct further discussion to determine whether participants' opinions have changed.

**Slide 26 Discussion — Scenario 3 (1 of 2)**

- Ella is walking from her car in the employee parking lot of the Water Department
  - There is a young man in front of her taking long strides
  - When he reaches the parking lot gate, he stops and writes something in a small notebook

*Graphic Description: No Graphic*

- Ask one participant to read the scenario on the slides.
- Instruct participants to identify any aspects of the situation that seem unusual.

- Ask participants: **In Scenario 3, what is unusual about this person's activities?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Pacing the distances then writing in the notebook*
  - *Stopping when he realizes he is being observed*

| **Slide 27 Discussion — Scenario 3 (2 of 2)** |
|---|
| • The young man walks alongside the parking lot fence from one end to the other, stopping again at the end to write in his notebook<br>▪ When he turns around and sees Ella watching, he quickly puts the notebook in his pocket and rapidly walks away |
| *Graphic Description: No Graphic* |

| **Topic: Reporting Suspicious Activities** | **10 Minutes** |
|---|---|

Enabling Learning Objectives:
- Describe the importance of identifying and reporting suspicious activities associated with hostile surveillance.
- Specify actions you can take to report potential incidents of hostile surveillance.

| **Slide 28 Reporting Observed Activities (1 of 2)** |
|---|
| ▪ Reporting suspicious activities is invaluable to protecting critical infrastructure<br>▪ Law enforcement, employees, and the community are in the best position to observe and report unusual activities in the area of critical infrastructure |
| *Graphic Description: No Graphic* |

| **Slide 29 Reporting Observed Activities (2 of 2)** |
|---|
| ▪ Reports may be the significant factor in disrupting a terrorist attack<br>▪ Business, public, and private organizations should encourage employees to report suspicious activities |
| *Graphic Description: No Graphic* |

- Explain that reporting suspicious activities is invaluable to protecting critical infrastructure and securing their nation.
- Explain that as the participants, employees, and the communities around critical infrastructure go about their daily work, they are in the best position to observe and report unusual activities related to surveillance — their reporting may be the significant factor needed to disrupt a planned terrorist attack.
- Tell participants that business, public, and private organizations in their communities should encourage employees to report suspicious activity when they observe it.
- Remind participants that everyone working together serves as a force multiplier in protecting critical infrastructure and the community as a whole.

| **Slide 30 What Should You Report?** |
|---|
| ▪ Immediately write down as much detailed information about the person or vehicle as you remember, including:<br>• Actions, behaviors, and descriptions of people and vehicles<br>• Descriptions of what made the actions or behaviors suspicious or unusual<br>▪ Report using form or worksheet if available |
| *Graphic Description: No Graphic* |

- Explain that an observer should immediately write down as much detailed information about the person or vehicle he or she observed as possible, and any other information about the incident, in case a law enforcement officer is not immediately available to come out and take a report.
  - Writing down the details is important
  - Memories only stay fresh for a short time
- Tell participants to include:
  - Information about observed actions or behaviors and descriptions of persons and vehicles that were involved
  - Descriptions about what actions or behaviors in the situation made it seem unusual or suspicious — knowing what is normal helps describe what is unusual
- Explain that using the report forms or worksheets helps law enforcement more easily compare information from other reports or crimes.

| **Slide 31 To Whom Do You Report?** |
|---|
| ▪ Community relationships help establish reporting procedures with local law enforcement<br>▪ Employers establish reporting procedures<br>▪ Local law enforcement may supply reporting forms or worksheets |
| *Graphic Description: Three law enforcement officers* |

- Explain that as local law enforcement, participants' agencies should establish relationships with areas businesses and organizations to provide a means of reporting suspicious activity.
- Explain that this community relationship can encourage the good practice of every place of employment establishing and communicating procedures for reporting suspicious activities to management and law enforcement.
  - The procedures should identify who to contact and when, and include all relevant phone numbers
  - Employees of larger organizations may need to inform a supervisor, manager, or security personnel so that they can call local law enforcement
  - Employees of small or sole-employee companies may need to call local law enforcement contacts themselves
- Explain that law enforcement agencies or some employers may already have a reporting form or worksheet that they can supply to anyone who wants to report something he or she has observed.

| **Slide 32 Community Awareness and Reporting Programs**  |
|---|
| ▪ If You See Something, Say Something<br>▪ Txt-a-Tip Campaign<br>▪ Programs in your own countries |
| *Graphic Description: No Graphic* |

- Remind participants of the community awareness programs discussed in *Module 4: Building Community Partnerships*.
  - If You See Something, Say Something
  - Txt-a-Tip Campaign
  - Programs in their own countries
- Explain that reporting may be done through all of these programs.

| **Slide 33 TeachBack Moment**  |
|---|
| ▪ What actions can you take to detect potential hostile surveillance incidents?<br>▪ Why is it important to identify and report suspicious activities associated with hostile surveillance? |
| *Graphic Description: No Graphic* |

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Ask participants the following questions:
  - **What actions you can take to detect potential hostile surveillance incidents?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Know what is normal to detect what is abnormal*
    - *Notice the indicators of surveillance*
    - *Evaluate surveillance-related activities*
    - *Determine whether they seem unusual or out of place*
  - **Why is it important to identify and report suspicious activities associated with hostile surveillance?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Reporting suspicious activities is invaluable to the work of law enforcement*
    - *Reports may be the significant factor in disrupting a terrorist or criminal event*
- Ask participants whether they have any questions over anything covered thus far in the course.

| **Topic: Module Summary** | **5 Minutes** |
|---|---|

| **Slide 34 Module Summary** |
|---|
| ▪ Understanding surveillance<br>▪ Potential targets of surveillance<br>▪ Hostile surveillance<br>▪ Detecting surveillance<br>▪ Reporting suspicious activities |
| *Graphic Description: No Graphic* |

- Summarize the module by reviewing the following main points:
  - **Understanding surveillance**
    - Surveillance-related definitions
    - Hostile surveillance detection
    - Information collected through hostile surveillance
  - **Potential targets of surveillance**
    - Categories of critical infrastructure as targets
    - Target selection surveillance
    - Pre-attack preparation
  - **Hostile surveillance**
    - Indicators of hostile surveillance activities
  - **Detecting surveillance**
    - Surveillant vulnerabilities
    - Surveillant tactics
    - How to detect hostile surveillance
  - **Reporting suspicious activities**
    - Reporting suspicious activities is invaluable to the work of law enforcement
    - Reports may be the significant factor in disrupting a terrorist attack
    - Business, public, and private organizations should encourage employees to report suspicious activities
    - Reporting actions
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 9: Explosives and Critical Infrastructure* will explain the effects of explosives on critical infrastructure.