



C-TPAT for OFFICERS

Anti-Terrorism Standards



Creating Alternatives



SECURITY AWARENESS





Security Awareness



Security Awareness Objectives

- Recognize Threats
- Evaluate Situations
- Respond Effectively





Security Awareness



Be Prepared – Be Aware

If you are going to effectively recognize suspicious activity in your area, you must:

Know your environment

- The people
- Normal patterns of movement
- Typical attire
- Common activities



*Become familiar with the usual,
so you will know the unusual.*





Security Awareness



Be Prepared – Be Aware

What are the categories of people who might be entering your facility?



Client Employees



Visitors



Vendors/ Deliveries



Contractors





Security Awareness



Be Prepared – Be Aware

Be aware of known methods used to slip through security, which include:

- Slipping in behind an authorized person (“piggybacking”)
- Entering the property at a remote or unobserved location
- Using doors or gates that were earlier left intentionally unlocked
- Use of false identification or credentials
- Hiding or hiding someone in a vehicle or cargo compartment
- Use of counterfeit or stolen uniforms (delivery, government, etc.)
- Use of vehicles that have been marked to appear to be official
- Use of stolen official vehicles



Counterfeit Texas DOT truck pulled over in 2007. The misapplied striping alerted the Trooper.





Security Awareness



Use Systematic Observation:

- What you SEE
- What you HEAR
- What you SMELL

Look for:

- The Unusual
- The Suspicious
- The Potentially Dangerous

Become familiar with the usual so you will know the unusual.





Security Awareness



Patrols

Security patrols enhance our security awareness of an area. The patrol officer moves through an area in order to **observe, gather knowledge**, and in some cases **take corrective action**, especially where security and safety risks are detected. The patrol is required to **report** all such activity and actions taken.

The presence of highly visible, professionally conducted security patrols also help to **deter unauthorized activity** by making it known that security is present in the area, as well as **convey a sense of security** to people working in the area.





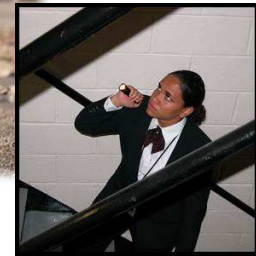
Security Awareness



Patrol Methods

Foot Patrol

- Can more closely and methodically inspect different areas
- May pick up sights, sounds, smells that a person in a vehicle would miss
- *Less visible - less deterrent effect; May become "lost in the crowd"*
- *Slower to respond to emergencies or remote locations*



Vehicle Patrol (golf cart, bicycle, truck, etc.)

- Covers more territory
- Highly visible – greater deterrent effect
- Quicker response to emergencies or remote locations
- *May miss sights, sounds, smells that a person on foot would detect*
- *Limited by size or facility policy to specific routes*

Each method has its strengths and weaknesses. When both methods can be used together, the overall patrol presence is very effective.





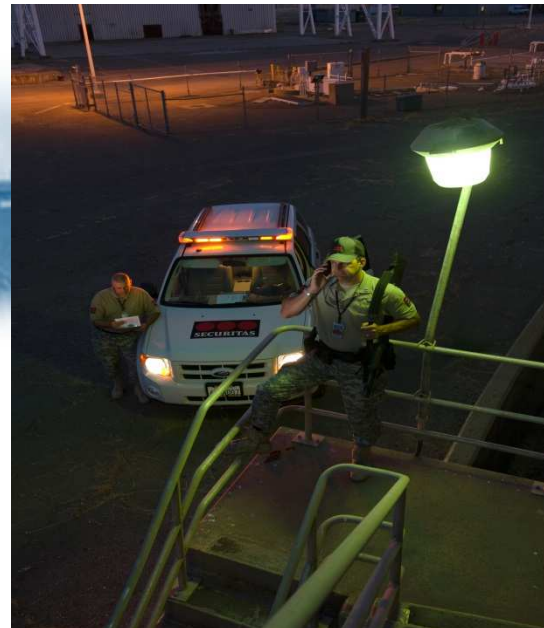
Security Awareness



Types of Patrols

Patrols can be tailored to suit a specific mission or situation. The different types of patrols are:

- Conspicuous Patrol
- Inconspicuous Patrol
- Regular Patrol
- Random Patrol
- Selective Patrol
- Stationary Patrol
- Virtual Patrols (Cameras)





Security Awareness



Preparing for a Safe and Effective Patrol

In order for your patrols to be effective and successful, you must:

- **Know your Patrol Environment**
- **Use the Proper Equipment**
- **Be Aware of Site Activities**





Security Awareness



Preparing for a Safe and Effective Patrol

Know your Patrol Environment

- Read and understand your Post Orders
- Understand your patrol route and responsibilities

Know the location of all:

- Entries and exits
- Shortcuts and alternate routes
- Places where people might hide
- Phone locations
- Routine sights, smells, and sounds (so you know when something is different)
- People (and their normal work areas)
- Fire alarms and fire suppression systems (to include fire extinguishers)
- Emergency power source
- Utility shutoffs





Security Awareness



Preparing for a Safe and Effective Patrol

Use the Proper Equipment

- Pen, field notebook, and some method of telling time
- Clipboard with Shift Activity Report
- Flashlight (even during daylight hours)
- Properly inspected and maintained vehicle, if applicable
- Communications gear (ex: radio or mobile device)
- Personal Protective Equipment (ex: hard hat, respirator, ear plugs, etc.)
- Tour recording equipment, if applicable (ex: H2 Tablet, Android)
- Keys or access cards
- Important phone numbers and special instructions
- Rain or weather gear as appropriate





Security Awareness



Preparing for a Safe and Effective Patrol

Be Aware of Site Activities

- Increased traffic due to special event
- Normal routes restricted due to construction or damage
- Site where suspicious person has been sighted
- Area where suspected employee theft is occurring
- Area where suspected external theft is occurring
- Employee shift change times
- Any special instructions in effect
- Criminal or other activity in the areas neighboring your facility





Security Awareness



Recognizing Suspicious Behavior

- Suspicious behavior and activity may signal terrorist planning. It is a CTPAT requirement that all suspicious activity at your facility must be investigated and reported.
- You must be able to spot suspicious behavior and activity in and around your post. Remember: the key is:

***Become familiar with the usual,
so you will know the unusual.***





Security Awareness



Suspicious persons are those who:

- You don't recognize
- Do not appear to belong
- Behave strangely

Behaviors that give them away:

- Sketching or taking photos of the facility
- Blank or nervous facial expressions
- Clothing inappropriate for the setting
- Unusual carried or dropped items
- Loitering or repeated short visits
- Asking suspicious questions



*Terrorists may potentially be of any national origin, ethnic background, or gender. They may have been specifically selected to blend in with their targets. Concentrate on identifying **behaviors**, not stereotypes.*





Security Awareness



Suspicious Questioning

Can occur in person, by phone, e-mail or mail.

Attempts to gain *Security Sensitive Information*, especially at a key facility:

- Site logistics/ transport methods
- Shipment routes/ dates
- Security patrols and procedures
- Number of security personnel on site
- Critical product or storage location
- Business operations or shift changes





Security Awareness



Suspicious Vehicle Activity

Like suspicious persons, suspicious vehicles are those that:

- You don't recognize
- Do not appear to belong
- Are being operated strangely

Features that give them away:

- Parked with their engines running
- Operating at night with no lights
- Left unattended for extended periods of time
- Parked in a remote or secluded area
- Continually "cruising", passing by available parking spaces
- Delivery vehicles outside of their normal areas
- Delivery vehicles arriving at unusual times





Security Awareness



Suspicious Vehicle Activity

When patrolling parking lots or around parked vehicles, look for:

- Windows left down
- Engine left running
- Keys left inside
- Headlights left on
- Leaking fuel, oil, or other fluids
- Flat tires
- Appears to sit very low to the ground, as if something heavy is inside

Record the license plate number and state of any vehicle you think is suspicious.





Security Awareness



Responding to Suspicious Activity

Detect

- ***Do not approach if you do not feel it is safe to do so!***
- Keep the person, vehicle or activity under observation. Note complete description.
- Immediately alert your notification chain, in accordance with your Post Orders.

Deter

- If you feel it is safe to do so, approach and ask to offer assistance.
- Ask for identification and purpose of the activity or presence.
- If unauthorized, direct the person or vehicle off of the property.



Report

- Ensure your entire notification chain has been notified – Supervisor, Client, Manager.
- Note the time of activity on your Shift Activity Report or Logbook.
- Complete and submit a formal Incident Report before the end of your shift.





Contractor/Vendor Sign-In Log

[illegible]

² Note: Have the individual returning the badge/keys initial this box before returning his property to him.





Access Control



Access Control: Monitoring and controlling the flow of people and/or vehicles past a specific point.

Common Access Control responsibilities include:

- Checking ID (proper identification or credentials to verify a person's identity)
- Obtaining or verifying authorization for entry
- Monitoring pedestrian traffic flow
- Monitoring vehicle traffic flow
- Recording the entrance and exit of all visitors and deliveries
- Arranging or providing Escort to sensitive locations

The goal of Access Control is to let authorized people and products in and keep intruders and unwanted materials out.





Access Control



Access to a facility can be controlled in several successive **layers**:

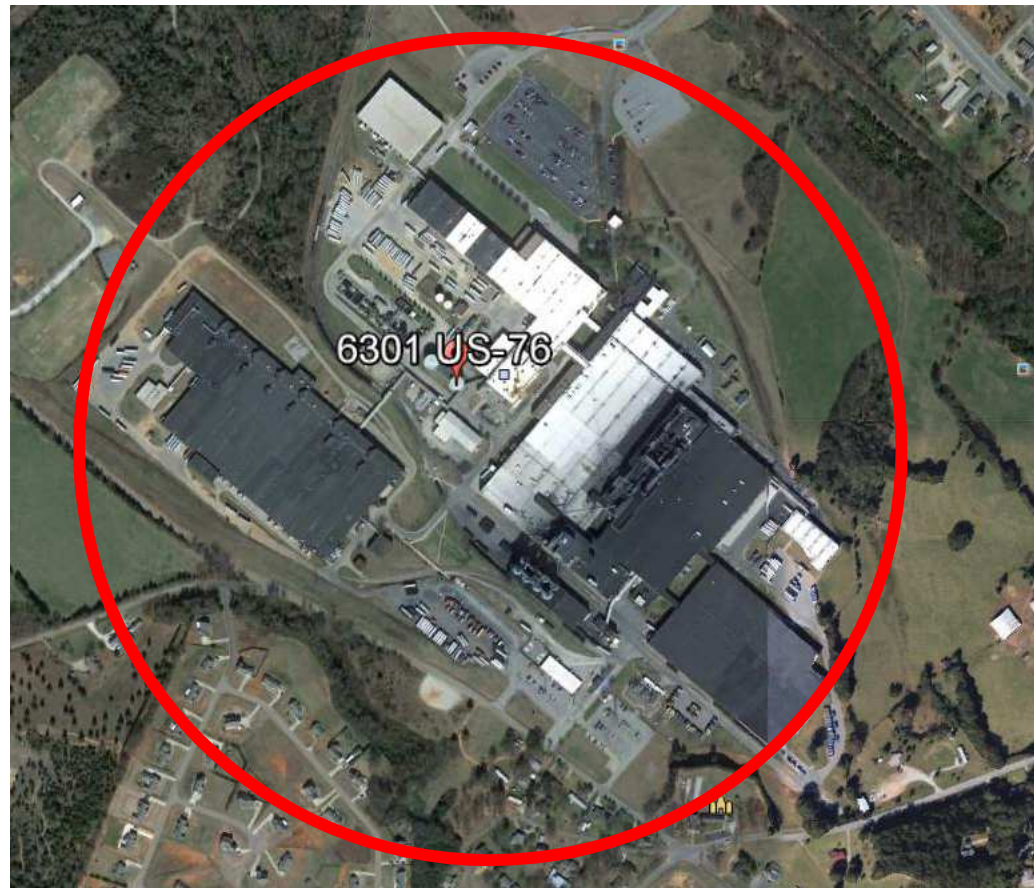




Access Control



From the outer property line or “perimeter”...





Access Control



With access restricted to specific control points...





Access Control



To internal buildings with their own access control points...





Access Control



To access control points to areas within those buildings.





Access Control



Your Post Orders help you determine:

- Who can enter a facility or building
- How other people might receive authorization to enter
- Who may give that authorization
- When they can enter (business hours)
- Where they are allowed to go in a facility or building
- How their movement is tracked (badges, entry logs)





Access Control



As mentioned earlier, you must know the categories of people who will enter your facility...



Client Employees



Vendors/ Deliveries



Visitors



Contractors





Access Control



...as well as the categories of vehicles...



Employee or Company Vehicle



Visitor Vehicles



Vendors/ Deliveries/Product



Emergency Response





Access Control



...and you must verify that everyone attempting to enter through your control point fits into one of those categories.

Those who do not are potentially UNAUTHORIZED.

When faced with a potentially unauthorized person or vehicle at your control point, you must immediately take control of the situation and determine why they are there.

Unauthorized people or vehicles may simply be lost. It is your job to stop them, ask questions, and redirect them to where they need to go.





Access Control



Handling Unauthorized Persons at your Control Point

A courteous and polite but firm approach yields better cooperation.

- Ask questions (to determine why they are there).
- Follow your Post Orders.
- Be polite, but firm in enforcement of the entrance policies.
- Be courteous and in control – your job is to *control* access; not simply allow it.
- Explain the client's security and entrance policy.
- Try to help, consistent with your Post Orders.
- Direct the person to leave the area.
- Ensure that they do!
- Report and record the event on your Shift Activity Report.

Call your supervisor for assistance as necessary.





Access Control



Sometimes, people who are authorized to enter the facility do not want to follow procedure or your instructions.

- Maintain a courteous and professional demeanor. Be friendly.
- Do not let your emotional response escalate the situation.
- Be polite but firm. Explain the security policy.
- Don't make exceptions. Allow entry only when the person has complied with the policies.
- If necessary, ask the person to wait while you call for assistance.



Afterwards, document the incident on an Incident Report.





Access Control



Several **security safeguards** exist to help keep intruders out. These include:

- Fences, Bollards and Grab Nets
- Alarms
- Hedges or other terrain features, whether man-made or natural
- Motion Detectors
- Locks
- Gates and Gate Arms
- Closed-circuit television (CCTV)
- Doors
- ID Badge Readers

These safeguards, along with your Access Control Post Orders procedures, assist you – the security officer - in controlling access to the facility. The key is these features cannot keep someone out on their own; they are only aids.

YOU MAKE THE DIFFERENCE!





Access Control



Locks and Keys

Locks are the primary element of virtually every security system. Their purpose is to:

- **Delay unauthorized access to a facility, area or item.**
- **Provide evidence of intrusion.**

Why only delay – not “prevent”?

Because given enough time and no disturbance, virtually every lock can be defeated.



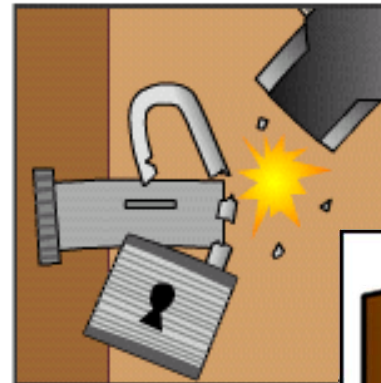


Access Control



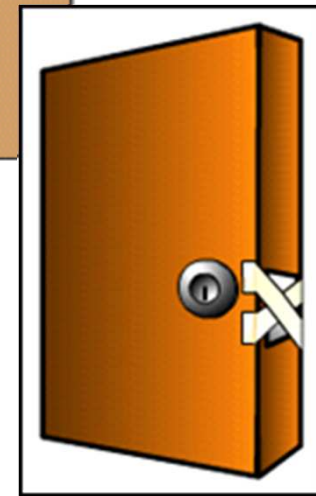
Four Basic Ways to Defeat Locks:

- Breaking
- Picking
- Taping or Jamming
- Using a Counterfeit Key



Always maintain proper key control procedures:

The easiest way to defeat a lock is to get its key!

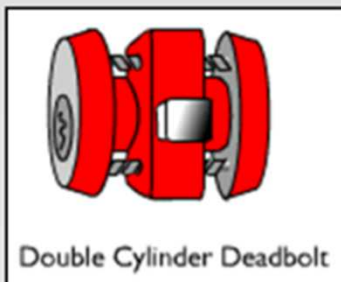
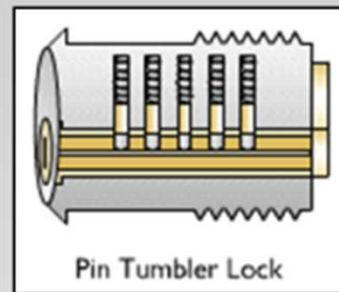
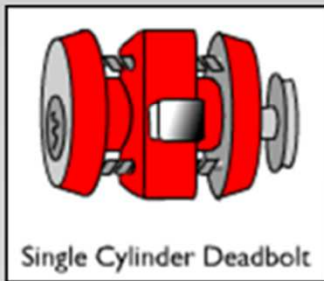




Access Control



What you'll encounter...





Access Control



Maximize the value of locks at your site in four steps:

Check

- Physically twist or pull gates and doors that are supposed to be locked. Never just walk or drive by, assuming that “it looks locked”.
- Be aware of any alarms and be careful not to set them off.

Inspect

- Look for evidence of tampering, damage, or maintenance. Report and document your findings.

Know

- Know the areas that must be locked, why they are locked, what they protect, and what type of lock is used.
- Who has access to the keys or combination codes, and where are they kept?

Schedule

- Know when doors and gates should be locked or unlocked, and make sure that schedule is followed. Correct, document and report any violations of the schedule.





Access Control

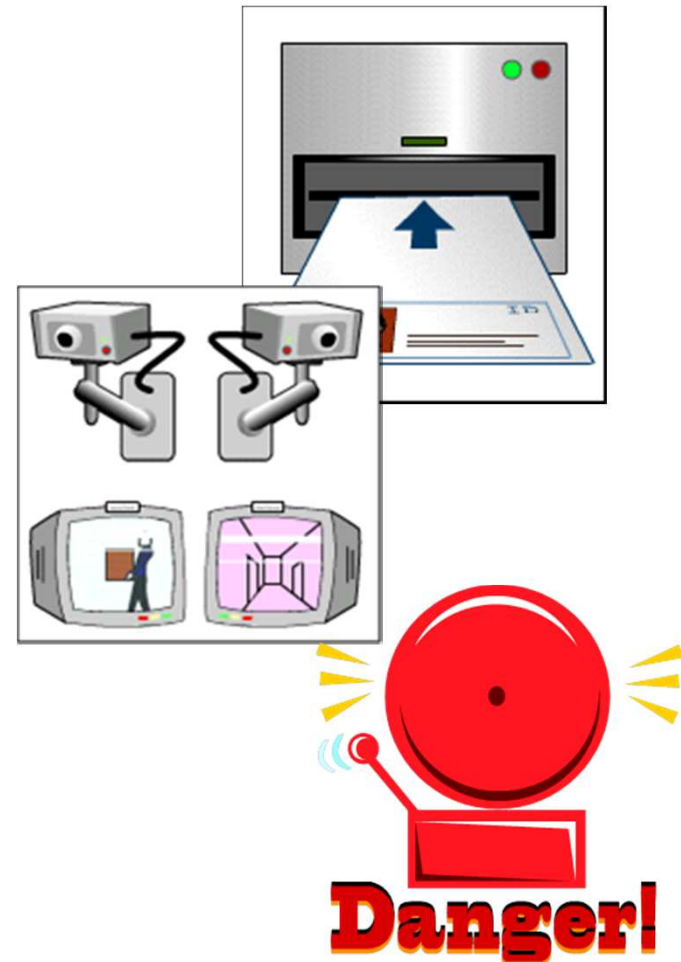


Access Control Equipment

More complex access control equipment may be used to further guard against unauthorized entry and security threats.

A complex access control system might include:

- ***Electronic Access Card Readers***
- ***Closed Circuit Television (CCTV)***
- ***Alarms***





Access Control

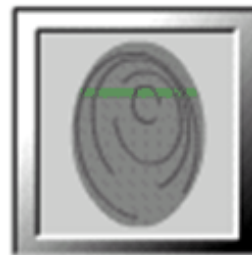
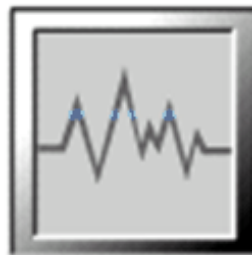


Some sophisticated access controls systems scan physical body features of the person requesting entrance, and compare them to a known database of the features of authorized personnel.

These “**biometric**” systems are sometimes less effective in high-traffic or weather-exposed areas, but they are very useful for entry to specific, low-traffic areas where a very high level of security is desirable.

Biometric access control systems might scan or read:

- **Voice**
- **Fingerprints**
- **Hand prints**
- **Retina patterns (eye)**





Access Control



Closed-circuit television (CCTV)

enhances sight by allowing the officer to monitor large or remote areas, or several areas at once.

It may provide a **deterrent** to theft or intrusion if the cameras are visible.

The cameras may employ sophisticated features such as night vision or heat-sensing technology to further enhance their **detection** capability.

It **records** immediate, permanent and detailed information with accuracy.



Some CCTV limitations:

- *Equipment may break down or malfunction.*
- *Cameras may be bumped, jarred, destroyed, or moved on purpose to no longer show the correct picture.*





Access Control



During training to use a CCTV system, it's important to take a **tour** of all camera locations so that each camera view is fully understood:

- *“What area of the facility am I looking at?”*
- *“If a person leaves this camera, which camera will pick him up next?”*



Keep your observation skills sharp!

- ***Avoid “visual fatigue”***
- ***Observe actively – not passively***
- ***Notice movement***





Access Control



You may be required to respond to **alarms** of various types. Alarms may be linked to other access control systems such as CCTV or card readers.

Alarm systems will vary among sites, but all systems have **three common elements**:

- **Sensor** (detection device)
- **Circuit** (sending device)
- **Enunciator** (sound device)



Alarms function to:

- Signal the presence of an intruder
- Warn of a hazardous condition or danger
- Monitor and detect physical changes in an area





Access Control



There are different types of alarm systems. It's important to know what types you are monitoring and how they function.

Central Station

- Monitored from off-site
- Personnel dispatched

Proprietary System

- Inside facility
- Monitored locally (you are dispatched)

Local Alarm System

- Sets off a signal
- Only those within sight or hearing distance respond





Access Control



Be aware of all of the security safeguards in use in your area of responsibility (duty stations or patrol routes).

You should understand how they work and how you need to respond to them. Detailed discussions of these access control systems and more can be found in the Securitas courses:

- **Fundamentals of Access Control**
- **Access Control Equipment**
- **Perimeter and Vehicle Access Control**

As a Securitas officer you have a requirement to complete these courses! Your supervisor or manager will ensure that you have the online access or necessary materials.





Access Control



“**100% ID Checks**” mean that you verify every person’s identification each and every time they enter your control point.

- You don’t accept IDs “flashed” you from a distance.
- You never “wave through” people you know.
- You use the “face-to-ID” method each time to ensure the ID belongs to that person.
- You verify the expiration date and physical security features of the card.

Even a person you checked that morning and you know has a valid credential may have left it in the car after lunch. Check every time!



Face-to-ID method:

1. *Physically take the card in hand.*
2. *Look at the photo.*
3. *Look at the person’s face.*
4. *Look back at the photo to verify it is the same person.*





Access Control



Container Inspection

7-Point Container Inspection Process:

1. Outside/ Undercarriage (before entering facility)
2. Inside/ Outside doors
3. Right side
4. Left Side
5. Front Wall
6. Ceiling/Roof
7. Floor (Inside)



7-Point Container Inspection





Access Control



17-Point Tractor & Trailer Inspection

- | | |
|------------------------------|-------------------------------|
| 1. Bumper | 10. Outside/
Undercarriage |
| 2. Engine | 11. Floor |
| 3. Tires (truck & trailer) | 12. Inside/ Outside Doors |
| 4. Floor | 13. Side Walls |
| 5. Fuel Tanks | 14. Ceiling/ Roof |
| 6. Cab/ Storage Compartments | 15. Front Wall |
| 7. Air Tanks | 16. Refrigerated Unit |
| 8. Drive Shafts | 17. Exhaust |
| 9. Fifth Wheel | |





Access Control



17-Point Tractor & Trailer Inspection





Access Control



Importance of Container Inspections



Step up to get inside! Why?





Access Control



Importance of Container Inspections



1,300 lbs. of cocaine !





Access Control



Importance of Container Inspections



Normal block and air vent





Access Control



Importance of Container Inspections



Short distance between block and vent. Wall colors are different!





Access Control



Importance of Container Inspections



1,290 lbs. Marijuana. False wall.





Access Control



Importance of Container Inspections





Access Control



Seal Inspection and Seal Controls

VVTT Seal Inspection Process

V – View seal & container locking mechanisms.





Access Control



V – Verify seal number for accuracy.





Access Control



T – Tug on seal to make sure it is affixed properly.





Access Control



T – Twist & Turn seal to make sure it does not unscrew.





EMERGENCY RESPONSE





Emergency Response



In emergency situations, specific security duties are highly dependent on the ***Emergency Response Plan*** in effect at your facility.

It is crucial for you to know and understand that Emergency Response Plan, and to be aware of the procedures outlined in your ***Post Orders*** when responding to any emergency.

In general, security has these basic responsibilities during emergencies:

- *Know and follow your Post Orders.*
- *Help with the evacuation of site personnel.*
- *If trained to do so, provide medical assistance.*
- *Provide clear and accurate information to Fire, Police, and EMS crews under stressful conditions.*
- *Take part in restoring daily routines following the emergency.*





Emergency Response



You can expect your site's ***Emergency Response Plan*** to contain the following information:

- *Emergency escape procedures*
- *Duties of critical personnel who will remain on site*
- *Procedures to account for personnel*
- *Rescue and medical duties of various personnel*
- *Procedures for fire and other emergencies*
- *Reporting procedures*
- *Chain of command/ designated Incident Commander*
- *Important telephone numbers*





Emergency Response



Due to security's role in interacting with the public on behalf of the facility, security officers will often be the ones to receive or discover ***bomb threats*** to the facility.

If you receive such a threat over the phone, your role is to:

- *Remain calm.*
- *Gather and fully document as much information from the caller that you can.*
- *Report your information immediately following the call. Be discreet.*
- *Be prepared to assist in emergency procedures as directed.*





Emergency Response



Bomb Threat Facts

There is an upward trend of bomb threat incidents. Statistics show that only one out of a hundred bomb threats are real. However:

Rule #1: NO bomb threat should be dismissed as a hoax.

The person who commits this type of threat

- Aims to spread fear
- Wants to create confusion
- May be seeking publicity, extortion, or revenge

*Usually, **terrorists** will not warn of a bomb they have planted, as they want to cause as much damage and inflict as many casualties as possible. In fact, they may plant a second device meant to go off when the first responders arrive.*





Emergency Response




A **Bomb Threat Checklist** should always be kept beside any phone with an outside line.

Upon receiving a bomb threat, go down the list, asking each of the questions and writing down the response. Note any accent or background sounds, as indicated on the checklist.

Once the caller has hung up, report the call immediately. document the call on your SAR and on a separate Incident Report.

Review your Post Orders for the precise Bomb Threat procedure.



Post Orders

Emergency Response

Bomb Threat Questionnaire			
When is the bomb going to explode?			
Time the call was made and phone number that threat was received on:			
Exact words of the caller:			
Are you sure you called the right building?			
What number did you call?			
Where is the bomb right now?		What floor?	
What side of the building?			
What kind of bomb is it?			
How powerful is it?			
What does it look like?			
Why did you place the bomb?			
How did you get it into the building?			
Where are you calling?			
What's your name?			
Description of the caller's voice/characteristics:			
1) Male	2) Young	3) Old	4) Voice Tone:
5) Female	6) Middle Aged	7) Accent	Type of Accent
1) Slow	Angry	2) Loud	Slurred/Drunken
3) Normal	Scared	4) Sincere	
5) Rapid	Laughing	6) Disguised	Soft
7) Broken	Stutter	8) Excited	
Background noises:			
Is the voice familiar?		Who does it sound like?	
Time caller hung up:			
Remarks:			
Person who received the call:			
Address/Telephone:			

Note: Immediately report this information to the police and any other appropriate authority.

Issue Date: February 2011

Revision Date: November 5, 2012





MICHELIN

SECURITY COMMUNICATIONS





Security Communications



As a security officer, ***communication is central to your job***. In the conduct of your duties, you may be called upon to communicate:

- *Verbally*
- *In writing*
- *In electronic communications (e-mails)*
- *By hand signal*
- *By telephone*
- *By radio*

Your ability to communicate effectively will largely determine your success as a security professional.



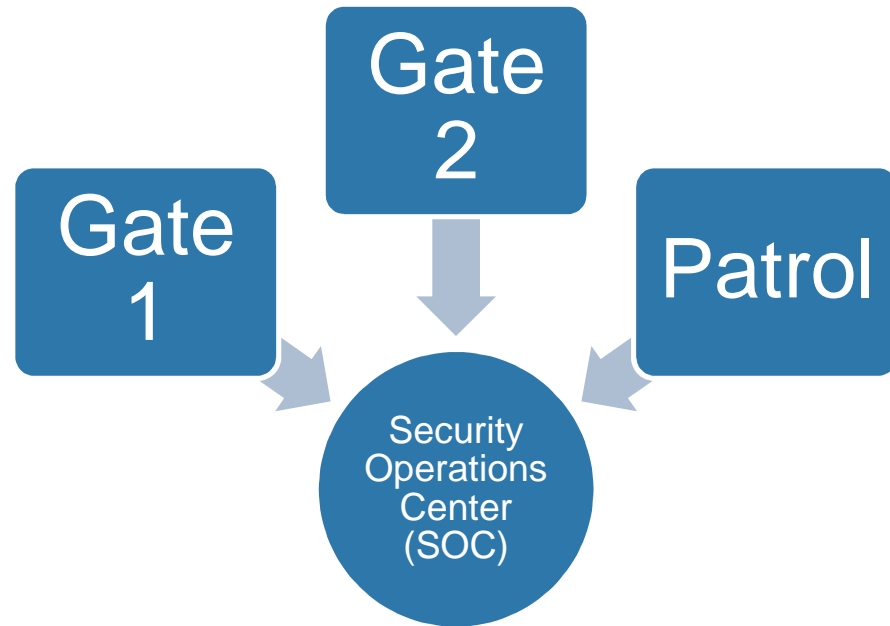


Security Communications



At any assignment, one of the first things you need to be made aware of are the forms of communication equipment available to you and how to operate it.

Understand who you must report information to and when. Is there an SOC that receives and redirects all security communications, or do you call in directly to a Securitas manager or client contact? Who gets any Incident Reports you write? Who do you call for assistance?



At no time should you be on any post, no matter how small, without some form of communication – even if it is just line of sight to another security officer!





Security Communications



One of the most common forms of security communication equipment is the two-way radio. You should become an expert in its use. Some basics of radio operation:

- *Radios are limited in range.*
- *Each person on the channel or “net” has a unique identifier*
- *Only one person can transmit at a time.*
- *Radios are NOT private; any number of people may be using the same channel, or someone may be standing next to the person you are talking to, and overhear your transmission.*

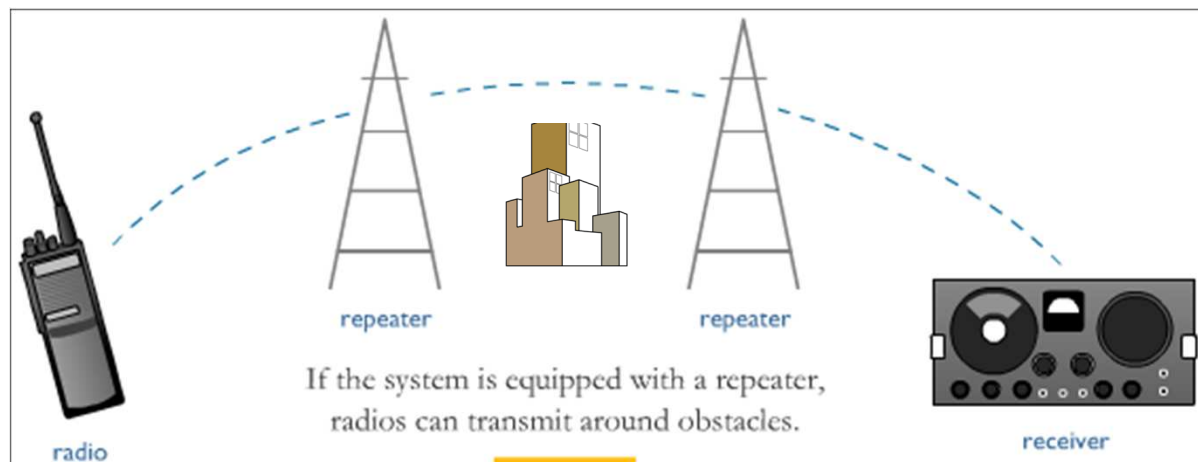




Security Communications



Radios work best on ***flat, open terrain*** with direct “line-of-sight” to their receiver. Intervening terrain, buildings or other obstacles can block or degrade radio transmissions, but ***repeating stations*** can help transmit around those obstacles, as well as increase transmission range.





Security Communications



Radio Functions

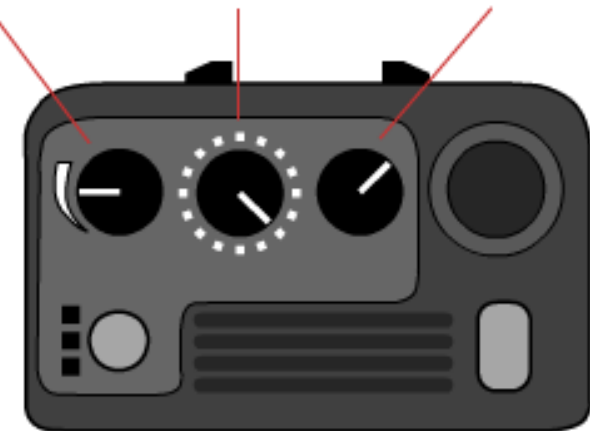
- On/Off, volume switch
- Channel selector
- Squelch control
- Battery operated (nickel-cadmium)



Battery Maintenance Notes:

- Charge new batteries for a full 24 hrs before using.
- Completely discharge before recharging.
- Maintain a set recharge schedule (for example: change batteries at each shift change)
- Turn radios OFF while recharging. Do not leave operating radios sitting on their charging stand!
- Use a pencil eraser to clean battery, charger, and antenna connections.

On/Off Switch Channel Selector Squelch Control



Radio (top view)

Security will often operate on its own dedicated radio channel, or share one with another Dept., such as Safety. SOC's may operate on additional channels to communicate with trucks or maritime traffic. See your Post Orders for authorized Security radio channels.





Security Communications



Professionalism and Radio Etiquette

- **Identify yourself.** Speak clearly.
- **Identify who you want to speak with.** Instead of names, use station designations and 10-codes, if they are available and in use at your site.
(example: "Patrol to Gate 1, 10-10.")
(example: "Gate 1 to Patrol, 10-4".)

*Keep all radio transmissions **brief and to the point.***

Do not key your mike unnecessarily. Always carry your radio in a manner that ensures you are not accidentally pressing or sitting on the transmit button.

Never allow or engage in non-work related radio conversations, or use slang, laughter, jargon, or unprofessional terms over the air.

10-1	Receiving poorly	10-19	Return to base
10-2	Receiving well	10-20	Location
10-4	All right. Yes. Agreed.	10-24	Completed assignment
10-7	Out of service	10-33	Emergency
10-8	In service	10-42	Traffic accident
10-9	Repeat	10-62	Unable to copy
10-10	Available for a call	10-112	Bomb threat
10-14	Restroom break		

10-codes keep your radio transmissions short and discreet.



Remember: Radio transmissions are NOT private!





Closing Note



This completes the course “CTPAT for Officers”.

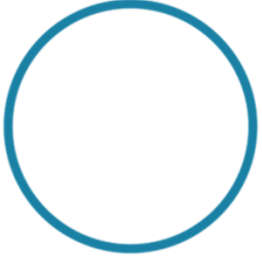
Two additional Securitas training courses are designed to further enhance your knowledge of the unique conditions and potential threats at CFATS-regulated facilities. Your supervisor or manager will ensure that you also have the opportunity to complete the following :

- ***Terrorism Threat Awareness and WMD Training for Security Officers***

Additional Course:

- ***Fundamentals of Access Control***
- ***Access Control Equipment***
- ***Perimeter and Vehicle Access Control***
- ***Emergency Response***
- ***Patrolling Tips and Techniques***
- ***Bomb Threat***
- ***Radio Communications***





Creating Alternatives