All references to "PGS" used in this book refer to Pinkerton Government Services, LLC.
INTRODUCTION

■ WELCOME!

*How It Works ...*

The PGS 5 Star Security Officer Training program has been developed as a flexible learning vehicle that can be a facilitator-led course or a self-paced course. This does not mean it is a self-taught course. Your supervisor will be available as a resource person during your progress. This course is divided into five levels — Star 1, 2, 3, 4 and 5. Each module or group of modules contains either a quiz or exercise that must be completed before moving onto the next module. At the end of each Star level you will be required to take a final exam.

In the tradition of PGS, this program has been designed so that you will gain the necessary skills and knowledge needed to enhance your skills as a respected security professional. The knowledge presented in this training program will greatly enhance your ability to provide the type of security services you can truly be proud of.

Good luck in your journey to becoming a PGS 5 Star Officer.
# Table of Contents

## Chapter 1 – Basic Security Officer Responsibilities
- Security Officer Handbook ................................. 1
- Discrimination and Harrassment ............................ 2
- Professional Image ........................................... 7
- Legal Aspects .................................................. 14
- Use of Force ..................................................... 16

## Chapter 2 – Observation and Incident Reporting
- Post Orders ...................................................... 17
- Theft Prevention ............................................... 20
- Communication ................................................ 24
- Report Writing ................................................ 31

## Chapter 3 – Access Control
- Physical Security ............................................... 37
- Key Control ..................................................... 38
- Technology ..................................................... 39
- Information Security ......................................... 43

## Chapter 4 – Emergency Response
- Emergency Response ......................................... 45
- Bomb Threats .................................................. 51
- Introduction to Terrorism .................................... 57

## Chapter 5 – Life and Safety
- Assessing the client’s Safety Risk ........................... 63
- Personal Protection ............................................ 69
- Safe Housekeeping ............................................ 70
- Fire Prevention ............................................... 71
- Worksite Fire Emergencies .................................. 72
- Fire Equipment ............................................... 74

## Chapter 6 – Industrial Security
- NISPOM ......................................................... 79
- Threat Awareness Briefing ................................... 82
- Defensive Security Briefing ................................. 92
- Security Classification System .............................. 93
- Reporting Obligations and Requirements .................. 94
Introduction Summary
This Pinkerton Government Services Introduction is a four and one-half hour introductory training course for new security officers. The program welcomes security officers who are new to the company. It introduces them to the Pinkerton Government Services culture and to the fundamental responsibilities of a professional Pinkerton Government Services security officer.

The program also includes OSHA-required training and notification on Bloodborne Pathogens and Hazard Communication.

Program Prerequisite
New security officers enrolled in the PGS Introduction Program must have successfully completed all company interviews, forms and background checks as outlined in the "Hiring Process" section of the Pinkerton Government Services Human Resources Manual. Employee eligibility can be confirmed with the Region Human Resources Manager. All hiring procedures must be successfully completed for each employee.

Program Materials
Pinkerton Government Services and Securitas Training Videos

#1: Introduction of Pinkerton (Running time: 11:53)

#2: Basic Security Officer Responsibilities (Running time: 11:49)

#3: Client Service Skills (Running time: 17:55)

#4: Loss Prevention Techniques (Running time: 17:58)

#5: Responding to Emergencies (Running time: 10:15)
**Hazard Communication Materials**

Hazard Communication: Signs of Safety Video (Running time: 13:00)

Hazard Communication Examination

Answer Sheet (for student use)

Answer Key and Review Sheets (for instructor use)

Acknowledgment Form

**Bloodborne Pathogens Materials**

Bloodborne Pathogens-CFR 1910.1030 Handout

Acknowledgment Form

**Drive of Life** (Optional) - (Running Time 30 Minutes)

Drive For Life Manual and Answer Key

Answer Sheet (for student use)

Road Test Tally Sheet
Welcome PGS. The purpose of this introduction is to provide a clear understanding of the role of the security officer and our requirements. Provide the basic knowledge and skills necessary to meet client requirements and to create awareness of career opportunities.

Lesson Objectives
When you have completed this chapter you should know:

- the components of the PGS Security Officer Handbook.
- PGSs’ harassment and discrimination policy.
- how to maintain a professional Image.
- the legal aspects of contract security.

Introduction to PGS

Pinkerton Government Services (PGS) was formed in 1988 to support Department of Energy contracts with both physical security and consulting and Investigative services. In 1999, PGS was reorganized and combined with the Pinkerton Aerospace Division resulting in contracts for cleared services being consolidated into Pinkerton Government Services, a subsidiary of Securitas Security Services U.S.A. Inc.

Security Officer Handbook

The security officer handbook is pocket-sized resource that is the key guide to company policies and procedures. The handbook is a reference document for the new security officer to use on the job. Review your Security Officers Handbook.
The Company

Productive Work Environment

Professional Development

Standards of Conduct

Your Employment

Benefits

Employee Assistance Program (EAP)

Discipline and Termination

Local Office Organization and Telephone Numbers

**PGS Policy 4.1**

**PGSs’ Policy Against Discrimination and Harassment**

PGS promotes a productive work environment, and does not tolerate conduct by any employee who harasses, disrupts or interferes with another’s work performance, or who creates an intimidating, offensive or hostile environment. Harassment based on race, age, sex, national origin, religion, disability, pregnancy, sexual orientation, religion or any other protected characteristic is a violation of state and federal law. Any individual who commits such a violation may be subject to personal liability action, as well as discipline by the company.

Each supervisor and manager has a responsibility to keep the work place free from any form of harassment, particularly of a sexual nature. No supervisor or manager is to threaten or insinuate, either explicitly or implicitly, that an employee’s refusal or willingness to submit to sexual advances will affect the employee’s terms or conditions of employment.

Other sexually harassing or offensive conduct in the work place, whether committed by any PGS employee, client employee or agent of the company, is also prohibited. This conduct includes

- unwanted physical contact or conduct of any kind, including sexual
flirtations, touching, advances or propositions.
• verbal harassment of a sexual nature, such as lewd comments, sexual jokes or references and offensive personal references.
• demeaning, insulting, intimidating or sexually suggestive comments about an individual’s personal appearance.
• the display in the work place of demeaning, insulting, intimidating, or sexually suggestive objects, pictures or photographs.
• demeaning, insulting, intimidating, or sexually suggestive written, recorded, or electronically transmitted messages.

Any of the above conduct, or other offensive conduct, directed at individuals because of their race, sex, national origin, religion, disability, pregnancy, age or military status is also prohibited.

Any employee who believes that any PGS employee or client employee’s actions or words constitute unwelcome harassment has a responsibility to report or complain about the situation as soon as possible.

All supervisors and managers will immediately report any complaints of discrimination or harassment to the next level of management.

All complaints of harassment are to be investigated promptly and in as impartial and confidential a manner as possible. Employees are required to cooperate in any investigation. A timely resolution of each complaint should be reached and communicated to the parties involved. Retaliation against any employee for filing a complaint or participating in an investigation is strictly prohibited.

Any employee, supervisor or manager who is found to have violated the harassment policy will be subject to appropriate disciplinary action, up to and including termination. PGS prohibits any form of retaliation against employees for communicating bonafide complaints or providing information about harassment. However, if an investigation of a complaint shows that the information was false, the individual who provided the false information will be subject to disciplinary action, up to and including termination.

PGSs’ policy is formulated to protect employees from unsolicited and
unwelcome overtures or conduct, as well as to provide guidelines for responding to harassment issues when security officers are victims of or witness to such conduct. The policy prohibits any employee misconduct that may adversely impact employee morale, be personally offensive, or interfere with an employee’s work and efficiency. There are two components to ensure that PGSs’ commitment to this policy is carried out: Responding and Reporting.

**Responding**

Any employee who believes he/she has been subjected to discrimination or harassed by a co-worker, supervisor or agent of PGS should promptly report the facts of the incident and the names of the individuals involved to his/her supervisor, Branch Manager, Area Vice President, Regional Manager of Human Resources or the AlertLine® at 800-932-5378.

**Reporting**

All supervisors and/or managers will immediately report any complaints of discrimination or harassment to the Branch Manager, Area Vice President, Regional Manager of Human Resources or the AlertLine® at 800-932-5378. All claims will be thoroughly investigated. Any employee found to have unlawfully harassed another employee will be subject to disciplinary action up to and including termination.

If you have any questions regarding this policy, contact your supervisor.

**Recognizing and Reacting to Sexual Harassment**

- Preventing sexual harassment is everyone’s responsibility.

**The Four Rs for Victims of Sexual Harassment**

There are four Rs to keep in mind if you are being harassed, or providing assistance to someone who is: Remember, Respond, Record and Report.

*Remember*… sexual harassment is not a shameful secret that must be faced in solitude and fear. There are steps and procedures to assist you in stopping sexual harassment. It is an illegal act and will not be condoned or tolerated by PGS.
Respond ... firmly and negatively to any advances. Let the harasser know that you disapprove. When you are approached, speak up. Tell the individual you do not appreciate his/her advances. Inform him/her that you feel uncomfortable as a result of their behavior. Tell him/her to “STOP!”

Record ... the incident. Your report should be a detailed record of the event(s), and include the date(s), time, location and any witness to the incident. If observed, you may want to inform the harassed person of your report, and inform him/her of your plan to report the incident to your manager or supervisor.

Report ... the incident(s) to your manager or supervisor.

The best course of action is to avoid all sexually related conduct in the work place. Employees should be aware that their conduct might be offensive to a co-worker. If you’re not absolutely sure that your conduct may constitute sexual harassment, DON’T DO IT.

How Sexual Harassment Affects Security

There are two ways in which sexual harassment affects security:

• security officers as individuals
• PGS as an organization

Good security is enhanced by people who demonstrate an attitude of caring about the organization’s goals and having a work place free from the costly, debilitating aspects of discrimination, harassment and unfairness.

Harassment’s Influence on You as a Security Officer, and as an Individual

Your job is to help protect our clients’ employees, visitors and property. Security first needs to provide safe environment free from threats and hazards for themselves. In adopting the adage of “practice what you preach,” security officers are the models. All actions should demonstrate commitment to an environment that fosters integrity, dignity, teamwork, safety and stability.

Harassment also affects security because it prevents you, as a security officer, from doing your job. If distracted by your own environmental threats, it is
difficult to focus on the task at hand — providing a safe environment for others. Your performance is increased if your energy and thoughts are focused on your immediate surroundings.

**Effect on PGS as an Organization**

If an employee feels that he or she is being harassed or treated unfairly, resentment may be displayed in more costly ways than just grumbling. Theft, carelessness and other destructive behaviors are far more likely to be found in a work place in which harassment or unfair treatment is tolerated. Morale, positive or negative, is highly contagious. Slower productivity in your work place and unfair treatment become costly with investigators, lawyers, fines and adverse publicity. Furthermore, the costs do not stop there.

Harassment and discrimination can hurt PGS as an organization by affecting our pool of applicants. Stories of harassment, via “word of mouth,” could influence any potential applicants. Employees who are harassed will share their misfortune with their friends, creating a negative effect on our applicant resources. As an organization, we are only as effective as our employees.

PGS stands by its harassment and discrimination policy. It is part of your job to enforce the policy. Remember that actions speak louder than words. If an employee sees a demeaning or harassing act occur without consequence, they may feel it is permitted or even condoned.

It becomes increasingly clear that there are many reasons for preventing, identifying and ending harassment of any kind. The responsibility to protect yourself and fellow employees falls upon each security officer. By completing this module you have taken the first step in preventing, identifying, and ending harassment and discrimination.
Professional Image

In many instances, the casual observer may overlook the important work carried out by Security Personnel. Although it may be difficult for the average person to understand the value and worth of our services, it is easy for them to recognize and detect the failure in these services, hindering our future contracts/business. This presents a substantial challenge for our organization. In an effort to gain the confidence and recognition of the persons we serve, every member of the PGS security organization must strive to maintain and improve our services and professional image.

Why Is Professionalism Important?

The extent to which we view ourselves and are viewed by others as professionals influences not only our immediate performance, but our future performance as well. If Pinkerton employees do not view themselves as professionals, they will not conduct themselves in a professional manner. This could lead to a lowering of the quality of our services, as well as costing PGS valued customers. It is for this reason that Pinkerton strives to set the high standards of our profession, as well as conducting ourselves in a professional manner. In an effort to maintain the confidence and recognition of our clients, every member of the PGS team must strive to improve the quality of our services. Every Pinkerton Security Officer, Supervisor, Coordinator and/or Manager must take pride in the organization. Any action or conduct exhibited by one person on our security team is a reflection on Pinkerton as a whole. Understanding the perceptions that others hold about our organization and the quality of work we provide is critical to our success. Thus, we all play an equally important role in providing world-class service. We must all take pride in our work, the services we provide and the reputation of Pinkerton Government Services.

A professional image is an image put forth by an employee that demonstrates high ethical standards in both conduct and those qualities that characterize one’s profession.
What Steps Do We Take to Promote a Professional Image?

We have all heard the phrase, “A picture is worth a thousand words.” We have also heard, “The first impression is a lasting one.” Contrary to common belief, first impressions are based on more than just looks. The impression we give to others is based on three things: appearance, attitude and personal interactions with customers. It is for this reason PGS incorporates these into your training and your job description.

Realizing these facts, we must do as much as we can to manage perceptions. Our future survival depends upon how each of us improves our approach, attitude and personal interactions with our customers. Our clients perceive us as experts and security professionals. (It is our challenge to demonstrate the value we create for our customers.) It is said actors/actresses are only as good as their last performance. They are the same person as before that performance, but they are only remembered by their last scene. If we are to be remembered by our last contact with our customers, we must promote ourselves in a professional manner at all times.

Appearance — First Impressions

First impressions are important. Pride in your personal appearance sends a message to your customers that you care about both your job and your customer. It is also important to understand that there is a direct connection between how you view yourself and the attitude that you portray. The higher your self-image the better impression you will make on others.

Physical appearance applies to your personal appearance (e.g., clothing), your body language and mannerisms (approachability), and your security post (e.g., neatness). All of these aspects are taken in by a customer when they form their first impression.

Appearance — Professionalism

Professional demeanor encompasses items such as the personal conduct and courtesy exhibited toward a customer by a member of the Pinkerton Security Team.
Items of personal attention relative to proper appearance and demeanor of PGS officers include the following:

- clean uniforms — neatly pressed
- ties, jackets, hats, badges worn appropriately
- speaking in a courteous manner
- not talking excessively on the telephone
- physically getting out of one’s seat to address a customer
- giving clear and concise directions
- not talking in slang
- not reading a newspaper, magazine, book, etc.
- not putting one’s feet on desks, chairs, etc.
- not sleeping
- portraying a “Customer Friendly” attitude.

Your uniform helps set your customer at ease by indicating you are part of Pinkerton Government Services. This uniform makes a powerful statement. Customers gain a sense of confidence when they realize that they can count on the person in that uniform for their security and safety needs.

**Appearance — Uniforms**

As a security officer for PGS you will be issued and required to wear a uniform. How you wear your uniform has a direct impact on your image and the image of the company. You must dress to reflect the image of yourself and Pinkerton as being a professional security provider.

There are several reasons why you must wear a uniform. The uniform allows you to

- be highly visible.
- be recognized as a person with authority.
- patrol freely on the client’s premises.
- enforce policy and procedures under your jurisdiction.
- be identified by police and fire personnel.
Properly wearing your uniform and good personal grooming projects a positive attitude. People respect spotless grooming because it reflects attention to detail, high standards and self respect. Spotless grooming also creates an impression of reliability and dependability. How you wear your uniform itself must be viewed in two ways.

1. The crispness of the uniform itself.
2. The pride you take in wearing it.

**Appearance — Uniform Articles**

**Shirts and Trousers**

Security Officers will wear prescribed company uniforms. No fancy belt buckles may be worn. Unauthorized pins, patches or devices may not be worn. Absolutely no political, religious or other organizational symbols of any kind may be worn while on duty or in uniform. Company uniforms should be clean and properly maintained at all times. Trousers should be to the length that covers the shoe laces. A belt that matches the color of your trousers with a simple buckle should be worn, with the belt buckle centered. Shirts must be tucked in at all times. If wearing long sleeve shirts the sleeves must be down and the cuffs must be buttoned. A clean white tee-shirt should be worn under all shirts.

**Tie**

Clean clip-on ties must be worn at all times. Clip-on ties are required for your safety. PGS tie bars are available through your branch office.

**Shoes and Socks**

Shoes and socks should be all black in color. The type of shoe you wear should be one required by the environment in which you work. Always shine your shoes and replace worn heels when needed.

**Coats or Jackets**

Only jackets, coats or rain coats issued and/or approved by PGS are to be worn over the uniform. When jackets are worn the breast badge will be on the outer garment and visible.
Clothing Accessories
For female employees, one earring per ear is acceptable and should be small in size and conservative in style and color. Over-sized earrings are not acceptable. For male employees, earrings may not be worn while working. Excessive jewelry may not be worn unless previously authorized by your branch management. Visible body piercing accessories or tattoos are not permitted.

Breast Badge
Your breast badge should always be visible. Normally you wear it on the left side of your shirt. When you wear a jacket be sure that you place your badge on the jacket. You must wear your badge so that it is visible for four reasons:

1. The badge is a symbol of authority.
2. The badge shows the company logo.
3. The badge shows your rank.
4. In certain jurisdictions, it’s a legal requirement.

Your cap can be a great aid when you are on patrol. It is highly visible and recognizable. Always wear your cap “square,” that is level on your head with the bill shading your eyes.

Hair
Your hair must be neat and combed in a natural style that is appropriate in the work environment. Unconventional or extreme colors of hair and/or hairstyles are not acceptable. For men, sideburns should not extend below the middle of the ear. Facial hair is limited to neatly trimmed mustaches above the lower lip. Handlebar mustaches are not authorized.

Hands and Nails
Clean hands are a requirement at all times. Fingernails are to be clean, neat and not extreme in length or color.
Hygiene
The way we appear to others is very important, the way we smell can also have a lasting impression on many customers. Take care not to use to much perfume or after shave. Always use under-arm deodorants and mouth wash. That way you will be confident that you are leaving a good lasting impression.

Officer in uniform may not enter bars, cocktail lounges, taverns or other places where alcoholic beverages are being served unless assigned to such a place while on duty. Uniforms will not be worn when off-duty, except in travel to and from your assigned post. There can be exceptions to this such as wearing your uniform to a funeral of a fellow officer. Supervisors should use their best judgment in those cases.

Personal Contact and Professionalism

In most instances, when customers arrive at one of our facilities, the first person they come in contact with is a member of PGS. First impressions are lasting impressions. It is essential that each initial contact a customer has with an officer be one that portrays a neat appearance and professional demeanor.

Physical appearance, such as neatness and cleanliness of clothing, hair, etc., are important aspects to remember when dealing with customers. Equally important when you are in direct contact with customers are such things as alertness, body language and personal mannerisms.

Speak with and treat each customer in the same manner in which you would like to be spoken to and treated if you were to reverse roles with that customer.

The key aspect to the over-all effectiveness of your personal job performance is to remember the word “perform.” Every time you, or one of your co-workers, comes in contact with a customer, you are placed in a role of a “Performer.” Think of your favorite musical performer or favorite song. Every time the performer sings and performs that song, the audience at that one particular performance expects it to be good, regardless of how many times he or she has performed the same song.
What Are Our Customers’ Needs?

Our customers have hired PGS not only to protect their physical assets but to provide psychological security for their employees, vendors, customers and visitors. These psychological needs may be met directly by you in face-to-face contact. Our customers have very specific and basic needs when they approach us.

1. The need to be understood.
2. The need to feel welcome.
3. The need to feel important.
4. The need for comfort.
5. The need to feel secure.

The need to be understood
Those who select your services need to feel they are communicating effectively. This means the messages they send should be interpreted correctly. Emotions or language barriers can get in the way of proper understanding.

The need to feel welcome
Anyone doing business with you who feels like an outsider will not feel welcome. People need to feel that you are happy to see them and that they are important to you.

The need to feel important
Ego and self-esteem are powerful human needs. We all like to feel important. Anything you can do to make a customer feel special is a step in the right direction.

The need for comfort
Customers need a place to wait, rest, talk or do business that provides physical comfort. They also need psychological comfort provided by the assurance they will be taken care of properly and that their needs will be met.
The need to feel secure

Customers need physical security — a safe and secure work environment. Just as they need physical comfort, they need to feel safe and secure psychologically; the confidence that in the event of an emergency they will be taken care of properly puts a person at ease.

Your success on the job will depend on how well you and PGS provide for these basic needs. Keep these needs in mind when you find yourself in a face-to-face interaction.

■ Legal Aspects

For most accounts, security officers are not law enforcement personnel. For some clients you may have special police powers granted by the state or city in which you work. In this segment of our program we will discuss some of the legal aspects involved in your work.

■ Felonies and Misdemeanors

For our purposes a felony is a criminal offense that is so serious the offender can be imprisoned for one year or more. Usually this means damage of property or theft of items valued at $100 dollars or more. For example, the theft of a computer would be considered a felony. A misdemeanor is considered to be a crime for which the offender may be sentenced up to one year in jail. Citizen’s arrests are only made for felonies which are witnessed by the citizen. PGS and client policy will determine if you will be required to make an arrest, however, most security professionals will not be asked or required to make an arrest. You will find that your authority to make an arrest for a felony will vary from state to state.

To make a citizen’s arrest you are required to follow the guidelines listed below:

- You must have observed the offense committed by the individual you are arresting.
- Always attempt to have a witness.
- Do not physically or verbally abuse the offender.
• Use only the amount of force necessary for your protection — have assistance with you.
• Refrain from using “Fight Starting” phrases. For example — “Come on, you think you’re tough.”
• Limit the time of restraint so as not to exceed a “reasonable amount.”
• If the suspect is female have a female present. If the suspect is male have a male present.
• Ask for consent to search. Conduct your search for dangerous weapons only.
• Notify the police immediately.
• Do not engage in high-speed or long chases.
• Move the person to a private place.
• If the arrestee confesses, attempt to get the statement in writing.
• Complete your reports accurately.

The law does not require a private citizen to give the Miranda Warnings, but this may be required by the client; therefore you should be familiar with the post orders at your particular site.

■ What Is Your Arrest Authority?

Security officers’ powers to arrest are the same as those of any other citizen. The laws which govern a citizen’s arrest vary from state to state. Be sure that you understand the rules for your state. If you exceed your authority you may face criminal or civil actions. Police and other law enforcement personnel are granted their powers of arrest by federal, state or local government agencies. Some of you may be commissioned to make an arrest.

Definition of Arrest

“An arrest is the taking of another into custody for the actual or purported purpose of bringing the other before a court, body or official, or of otherwise securing the administration of the law. Mere words will not constitute an arrest, while on the other hand no actual physical touching is essential, an assertion of authority and purpose to arrest followed by submission of the arrestee constitutes an arrest. There can be no arrest without either touching or submission.”

— “Arrest is the taking of a person into custody in order that he may be forthcoming to answer for the commission of an offense.”
Sec. 18, Code of Criminal Procedure, American Law Institute.

**Brief Overview of Arrest Authority**

As a security officer you must have clear and probable cause for making an arrest. Probable cause is the belief that the individual being arrested has committed a crime as defined by federal, state or local statute. If you overstep your boundaries, you may incur legal and financial penalties. It is important to remember that you are a representative of PGS, as well as the client you are serving. Consequently, you, your client and PGS, can be held accountable for violations of individual rights.

**Is the Use of Force Ever Justified?**

The use of physical force must be avoided. When used, it must be the minimum force necessary to control a situation. The use of force must always be done in a reasonable manner using your best judgment. These are some instances in which the use of force are recognized:

- Self defense — it must be clearly justified.
- The protection of others.
- To stop a physical attack.

Force should be used to gain control only after all other methods to gain compliance have failed. Some guidelines for the use of force are as follows.

- Force can only be used after all other methods of control have been exhausted.
Lesson Objectives

When you have completed this chapter you should know

- understand the importance of post orders.
- what is theft prevention.
- provide you with the skills necessary for telephone and radio communication.
- guidelines for effective report writing.

Post Orders

Once a security officer is assigned to a specific site, that site assignment is referred to as a post. Although PGS security officers report to their posts with a solid knowledge base enabling them to effectively protect our clients’ assets, the minute details of each post cannot be committed to memory. For this reason each post has a set of post orders that explain the expectations and duties particular to that assignment. These site-specific post orders enable security officers to successfully and effectively perform those duties required for optimal protection of that site. Your supervisor will review your post orders with you once you have been assigned to a post. This orientation is important because each security officer is held accountable for the information contained in the post orders. Site post orders are written jointly by local management and the client enabling PGS to meet our customers’ specific site needs. Post orders are thought of as a guidebook to meeting customer needs, effectively protecting and securing both you and your post.

What Are Post Orders?

Post orders are the procedures developed by PGS and the client for the purpose of preventing property loss through theft, vandalism or fire, as well
as protecting the safety of the client’s employees and visitors. Post orders are written by local management and submitted to the client for approval. These collaboratively written post orders ensure that information contained in them reflects both the client’s knowledge of the site, as well as Pinkertons’ knowledge of the implementation of security procedures. Thus, when post orders are closely followed, the site is optimally protected.

What Types of Information Do Post Orders Contain?

Post orders contain the information necessary for security officers to perform the duties of a specific post. They are crucial to security’s success because they contain site-specific information regarding protective measures of the site and those assigned to protect it. Always check to ensure you understand how post orders are organized, where specific information is located and that all sections are clearly marked. It is your responsibility to contact local PGS management with any questions regarding the understanding of information covered in your post orders. Remember, post orders are a valuable tool designed to assist security officers in carrying out their duties, but as with all tools, they are only effective when they are utilized correctly and consistently.

Post orders should include, but are not limited to, the following information:

• purpose of the post or patrol
• hours of coverage
• procedures for the opening and closing of the post
• officer’s duties by shift, day of the week and specific time
• access control procedures for employees, vendors and visitors during business hours
• patrol rounds
• clock key locations
• alarm systems
• actions to be taken in case of an emergency or disaster
• emergency services telephone numbers
• proprietary and confidential information.
Even the most seasoned security officers cannot anticipate nor commit to memory the answer to each and every question or situation that arises when carrying out security duties. Therefore the information contained in post orders will range from general to specific.

Some of the more specific types of information found in post orders are

- location of security posts.
- specific officer assignments.
- keys and equipment instructions.
- alarm systems for:
  - Fire
  - Security
  - Medical
- evacuation procedures and routes.

**Types of Patrols and Duties**

As a security officer one of the most crucial duties you perform is patrol. An effective patrol is one of the best preventative measures a security officer has to detect security threats. Remember, patrol is not just walking or riding around. It is a very definitive activity with specific objectives and instructions which depend upon your site and your specific post orders.

There are many different types of patrols and duties that security officers are asked to perform. They will depend upon the client’s needs and the specifics of the assigned post. The different types of patrols and duties found in post orders are

- Inspections
- Daily Activity Report Entry Requirements
- Patrol Key Locations
- Escort Duties
- Truck Gate Operations
- Parking Rules and Regulations
- Safety Responsibilities

Keep in mind that these procedures were developed with your specific post in
mind; consequently the patrol techniques outlined in post orders provide the best coverage and protection of the site. Follow them closely and make sure you understand all aspects of your duties.

Your site’s post orders may include several other specific actions depending upon the client contract. Post orders are essentially a guidebook that needs to be carefully followed.

Post orders must be reviewed periodically for any required changes, such as new emergency phone numbers or evacuation routes. Changes must be communicated to all personnel involved with the post. Keep abreast of all changes because often they reflect new security features, which will assist you in effectively carrying out your duties. An awareness of all aspects of your post duties enables you to provide the best possible security service to our clients.

**Post Order Changes Should Be:**
- Read
- Reviewed
- Initialed
- Passed Down!

### Theft Prevention

#### What Is Theft Prevention?

The largest percentage of asset loss is from theft, so companies work diligently to prevent theft. Theft prevention consists of those procedures used to control and prevent loss of company assets, such as computer lock-down devices. As stated earlier, billions of dollars are lost each year through employee and public theft. Preventing theft means lessening the opportunities.

In other words, rather than attempting to catch an individual in the act, preventive measures are taken to avoid the act from occurring in the first place.
What Is Theft?

The legal definition of theft is the unlawful stealing of property of another with the intent to deprive the rightful owner of their possession.

Many think of theft as a single act in which something of considerable value or quantity is stolen. However, theft of small amounts of money or equipment taken over time accrue into millions of dollars in a very short period of time. When employees engage in this type of theft, it is called pilferage. By some estimates, pilferage is one of the highest costs incurred by an organization.

Why People Steal

Motivation to steal arises from a variety of reasons such as need, desire, psychological disorder and/or compulsion.

It is more likely that individuals will steal out of desire, actual need and/or perceived need rather than psychological disorder or compulsion. An individual may feel they need a particular item for their personal use, such as a computer. The individual may desire something because they believe it will make their life easier. Regardless of whether the individual is justified in their actions, desire and need are powerful motivations. Individuals will go to great lengths to get what they want or need. It is also important to remember that individuals will also steal in retaliation for policies and procedures they do not like or think are unfair.

Other causes of theft include drug-addicted individuals looking for a way to feed their addictions.

How to Prevent Theft

Though we in security do not have direct control over some of the methods used to prevent theft, we must always be on the lookout for ways to help our clients identify possible theft situations.

To have an effective theft-deterrence program the client should have a written policy in regard to theft, an effective loss-prevention program and a well-trained security force. We will next discuss how we can better prevent theft and some of our responsibilities in regard to theft issues.
**Facility Theft Prevention**

Theft prevention in the facility is a primary objective of security officers. Officers are responsible for the observance, detection and elimination of situations conducive to possible theft. Be aware of the following:

- “Hot items” left laying around. “Hot items” are highly desirable items that have a high potential of being stolen.
- Excess number of “hot items” in the work area.
- “Hot items” must be stored and locked up during non-production times.
- Unusual employee actions
  - employees loitering in storage areas
  - employees loitering in restricted areas
  - employees in possession of material not used on their particular jobs.

**Parking Lots and Perimeter Fence Lines**

A security officer’s responsibilities for theft prevention also include parking lots and along fence lines. Any outside perimeter area should be considered a possible theft route. Officers should be observant of and report all discrepancies along the fence lines and in parking lots. Some of the items to be aware of concerning fence lines are listed below.

- loose fencing
- cut fencing
- damaged barbed wire or concertina wire
- gaps at the bottom of the fence
- material stacked next to the fence
- isolated areas.

Employee parking lots should be patrolled to prevent theft of employee property, as well as to detect possible theft of company property. Some points that may indicate possible theft from parking lots are listed below.

- personnel loitering in parking lots
- personnel looking into vehicles
- vehicles driving around slowly or at unusual hours
- personnel having difficulty entering a vehicle.
Any unusual activity along the perimeter fence lines or in the parking lots should be reported to your supervisor immediately.

**Recognizing Theft or Intent**

**Facility Entrance**

The security officer’s skill as an observer is vital in the detection of theft. Keen observance of people, property and unusual activity can play a major role in deterring theft. Theft prevention at a facility entrance involves three important areas.

1. before the entrance
2. at the entrance
3. after the entrance.

Officers should be observant of the following signs that may indicate theft:

- adjustment of clothing
- bulges in clothing
- loitering employees
- attempted exit when officer is distracted
- employee who watches officer for period of time
- arms held in an unusual manner
- unusual walk — stiff arm or leg
- books or magazines folded in a manner to conceal property
- personal clothing in a roll or bundle
- diversions
- shifting packages from side to side
- employees in a hurry
- employees walking on the far side of a group
- overly friendly employees.
Responding to theft

When a security officer finds it necessary to approach an employee suspected of theft, the following steps should be followed:

1. Request the employee step into the gatehouse (if at an entry/exit point).
2. Identify employee.
3. Request employee reveal contents of
   - packages
   - pockets
   - bulge in clothing.
4. If employee refuses:
   - Inform employee failure to comply will result in violation of company policy and could result in detention.
5. Contact security supervisor.
6. The supervisor will contact Labor Relations or other client personnel.
7. Contact employee’s supervisor.
8. Collect all evidence of theft.

Theft control is largely a matter of procedures, faithfully followed, and records kept accurately and completely.

Communication

Telephone Skills

The telephone plays an integral role in almost all businesses today. Take a moment to reflect on the role of the telephone at your site. As a PGS security officer you may be required to fulfill receptionist duties. It is important for you to have telephone skills as the telephone is a key source of contact between you and your district office as well as the client’s customers.

Telephone communications are as important as face-to-face interaction with customers. First impressions are often formed over the telephone. A recent study found that first impressions formed over the phone are based primarily on vocal cues (such as tone, professionalism and courtesy) and account for 82% of our first impressions made, while only 18% are based on the types of
words used when communicating on the telephone. These figures are given to demonstrate just how critical it is that your voice be pleasant, concerned, patient, informed and caring.

Send a positive attitude when using the telephone!

**Telephone Courtesy**

Having telephone skills is crucial to PGS’ success. When you are on the telephone with a customer, you are representing PGS. In other words, you are PGS and your actions send a clear message about our organization. You must remember that the individual on the other end of the telephone does not have visual cues provided by your body language or facial expressions to analyze the situation or gauge your feelings. The individual has only your voice to gauge the social situation. This makes your tone of voice very important. It is also important to remember that individuals you speak with on the telephone are current or potential customers. The only information available to them is your telephone communication skills, such as your voice and finesse in handling the telephone call.

It is imperative that PGS employees exhibit a professional attitude when answering all telephone calls. The mood we convey on the telephone is important. When a customer cannot see your concerned face, they need to hear concern in your voice. There are two critical aspects to making sure the message you send over the telephone is a positive and caring one:

1. The manner in which you speak.
2. Active listening.

**How a Positive Speaking Manner Is Achieved**

You can see how critical it is that your voice tone be pleasant, concerned, patient, informed and caring. When a customer cannot see your concerned
Even if your voice is pleasant, you may still be annoying customers if you have irritating habits such as gum chewing, eating, covering the receiver to talk to co-workers or leaving the customer on hold too long.

Speak in a pleasant tone of voice, at a rate that is not too fast nor too slow, and in a volume that is not too loud nor too soft. Each time you answer the telephone, identify yourself and the area in which you work.

**Example:** “Security, Officer Chris Smith, how can I help you?”

If you work in an area that receives telephone calls from persons outside your particular facility, also identify the corporation.

**Example:** “Boeing Defense and Space, Security Officer Pat Jones, how can I help you?”

**Active Listening**

Active listening is another important aspect of effective telephone communication. By assuming an active listening role, you are more able to understand what the call is about and meet the customer’s needs. Let’s take a look at some simple listening skills that should be used while you are on the telephone.

- Seek first to understand what your caller wants.
- Be polite by saying please and thank you.
- Display a professional attitude.
- Minimize interruptions.
- Be calm, sincere and interested.
- Give appropriate verbal responses. Allow the speaker to continue speaking while remaining interested. Use terms such as:
  - “Yes, really?”
  - “Gee.”
  - “You don’t say?”
Taking Telephone Messages

Taking messages accurately is another important part of telephone courtesy. Take a moment to reflect on the last time you were frustrated by receiving an inaccurate telephone message. What were the consequences — a missed appointment? How did you feel? When taking telephone messages from a caller, listen clearly, re-state the information of the telephone message to the caller and explain the action you are going to take so that customer satisfaction is reassured. Write and record the time of the call, your name, and forward it promptly to the appropriate individual(s).

Helpful Hints for Telephone Communications

The following is a list of actions for effective telephone communications. As you read through this list, take a few moments to consider how it applies to your particular job assignment.

- Show interest.
- Make an effort to understand what the person is trying to say.
- Make an effort to understand the other person’s point of view (empathy) even if you don’t agree with it.
- Acknowledge the other person’s viewpoint and let him or her know your opinion.
- Let him or her ask your opinion.
- If a problem exists, try to identify it.
- Help the other person see the relationship between the cause and the problem.
- Encourage the other person to solve his or her own problems.
- Wait and listen when silence is the best answer.

Radio Communications

One of the most important pieces of equipment you will use on the job is a two-way radio. Your radio provides you the ability to respond quickly to problems and can also provide you with personal safety. It is essential that you use your equipment properly and professionally. When using any form of radio communication, the message must be clear and concise.
How Two-Way Radios Work

Radio units transmit and receive signals on a specific radio frequency. The frequency is a point on the “dial” or spectrum of radio frequencies. The frequency is assigned by the Federal Communications Commission (FCC). Several users may be assigned to the same frequency.

Signals

Radio signals require three basic components:

- transmitter
- antenna
- receiver.

The transmitter provides the energy to transmit signals, the antenna “spreads” the energy into the atmosphere, and the receiver catches and processes the signals then converts them to audio or printed text signals.

Radio wave units are line-of-sight devices, that is, they operate best on flat ground where there is nothing to get in the way of the signal. When obstacles such as mountains, hills or large buildings are present a repeater is needed. A repeater is an antenna placed at a very high point. The base station transmits the signal to the repeater, the repeater then transmits the signal to the receivers. In this way the signal is lifted up and over the obstacles. Now that we have touched on some of the technology in regard to radios, let’s take a look at how to use the radio.

Recommended Techniques

Following is a list of Dos and Don’ts for radio communication. These common radio techniques should be adhered to at all times. Remember that prevention is always the best practice, always be sure your equipment is in good working order and report any damage to your supervisor immediately.
DO

• Conduct a radio check when you receive your radio.
• Verify with the base station your “radio check and number.”
• Wait for a response before speaking.
• Speak slowly into the microphone.
• Hold the microphone 2–3 inches away from your face.
• Begin speaking when contact has been established.
• Make sure no one else is broadcasting.
• Use codes when applicable.
• Use unit numbers for identifying personnel.
• Know areas of interference.
• Be clear and understandable.
• Broadcast only essential information.
• Use a telephone for lengthy messages.
• Be courteous.
• Keep transmissions brief and to the point.
• Plan your messages.

DON’T

• Use personal names.
• Transmit information that could alarm the general public. Remember, the same frequency may be used by several different radio users.
• Express anger or sarcasm.
• Use profanity.
• Start talking until initial contact has been received.
• Broadcast over others.
• Broadcast long messages.
• Use humor or horseplay.
• Argue with or chew someone out.
### 10-Codes

There are a number of “10” codes and phonetic codes utilized by different agencies. Know your site code system. In the event of an emergency be aware that outside agencies may have a code different from yours. Always be professional and assume personal responsibility for correct radio use.

This is a sample of a 10-Code System.

**General Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-1</td>
<td>Receiving Poor</td>
</tr>
<tr>
<td>10-2</td>
<td>Receiving Well</td>
</tr>
<tr>
<td>10-3</td>
<td>Stop Transmitting</td>
</tr>
<tr>
<td>10-4</td>
<td>Message Received OK</td>
</tr>
<tr>
<td>10-5</td>
<td>Request Radio Check</td>
</tr>
<tr>
<td>10-6</td>
<td>Rest-Room Break</td>
</tr>
<tr>
<td>10-7</td>
<td>Out of Service</td>
</tr>
<tr>
<td>10-8</td>
<td>In Service</td>
</tr>
<tr>
<td>10-9</td>
<td>Repeat</td>
</tr>
<tr>
<td>10-10</td>
<td>Supervisor Needed</td>
</tr>
<tr>
<td>10-11</td>
<td>Meet Complainant at ...</td>
</tr>
<tr>
<td>10-12</td>
<td>Registration Check</td>
</tr>
<tr>
<td>10-13</td>
<td>Meet (unit) (location)</td>
</tr>
<tr>
<td>10-14</td>
<td>Escort (person) (location)</td>
</tr>
<tr>
<td>10-15</td>
<td>No Apparent Problem</td>
</tr>
<tr>
<td>10-16</td>
<td>Pickup (locate)</td>
</tr>
<tr>
<td>10-17</td>
<td>Deliver (location)</td>
</tr>
<tr>
<td>10-18</td>
<td>Proceed With Caution Go</td>
</tr>
<tr>
<td>10-19</td>
<td>Go to (location)</td>
</tr>
<tr>
<td>10-20</td>
<td>Location</td>
</tr>
<tr>
<td>10-21</td>
<td>Phone</td>
</tr>
<tr>
<td>10-22</td>
<td>Crime in Progress</td>
</tr>
<tr>
<td>10-23</td>
<td>Please Stand by</td>
</tr>
<tr>
<td>10-24</td>
<td>Security Alarm</td>
</tr>
<tr>
<td>10-25</td>
<td>ID Check</td>
</tr>
</tbody>
</table>
Report Writing

■ The Purpose of Reports

The purpose of a written report is to provide a permanent record of a particular incident. It is important that this record is written immediately following the time of the incident and as accurately as possible. The report may

• Inform your superiors of conditions at your facility.
• Provide details to authorities of various events and conditions that require their attention.
• Provide a written record which may prove vital in subsequent investigations and discussions such as
  – disciplinary matters.
  – fire investigations.
  – theft investigations.
  – safety related concerns.
  – medical response.
  – traffic accidents.
  – statements.

When to Write a Report

The time between when your report is written and the incident is critical to the accuracy of the report. If you experience an incident, take notes immediately to ensure accuracy of the facts. An incomplete document is of little value to anyone who reads it. Reports should be submitted when

• They are required by your department rules and regulations.
• A fire occurs at your facility.
• A theft occurs at your facility.
• An injury or illness of an employee requires action by the Security Department.
• A safety hazard is observed.
• A traffic accident takes place on company property.
• You observe a condition within your facility or department that you think can be improved.
• Policy or procedural rules are violated.

If a Security Officer is Involved a Report Must Be Written!
Using a Field Notebook

One of the most useful tools you can carry with you is a small field notebook. While on patrol or investigating an incident, your field notebook entries will provide you with the necessary information to properly complete your report. You may have a great memory, but don’t rely on it to remember all the facts. Carry the field notebook. The best kind to use is one with a glued binding. Refillable notebooks may not be reliable due to the fact that pages can be removed or inserted.

**Information to Be Entered in Your Field Notebook**

Your notebook should not only contain the information you have observed in the field, it should also contain information that you can use in the field. This information might include

1. **Telephone Numbers:**
   - Security Headquarters
   - Branch Office
   - Investigations Unit
   - Local Police Departments
   - Local Hospital
   - Labor Relations
   - Info Line
   - AlertLine

2. **Addresses:**
   - Branch Office
   - Security Department
   - Local Police Department
   - Local Hospitals
   - Other pertinent addresses

3. **Other information:**
   - date of observations
   - your assignment
   - your supervisor’s name

**At the scene of an incident note the following:**

- the name(s), telephone numbers and addresses of persons contacted at the incident
- details of any searches conducted (property or person)
- first observations of the scene
• names of other security personnel at the scene
• law enforcement officers present at the scene
• emergency response personnel
• sketches of a scene
• your actions at a scene.

**Your Field Notebook Is One of the Best Tools for Effective Report Writing!**

One final note on your field notebook. Do not enter any personal information in your field notebook; keep it business only!

- **Specific Qualities in Report Writing**

  There are many specific qualities that constitute a good written report. Attention must be given to each report to ensure that it is complete, concise, clear and accurate.

  **Complete** – Obtain the necessary information to complete the report. Give attention to detail to ensure that all items on the report form have been completed.

  **Concise** – Reports must be as brief as possible, while still addressing all essential information. Sentences must be short and as simple as possible. Technical words or phrases must not be used unless they are necessary for clarification.

  **Clear** – The report must clearly state what the writer observed and heard, and any action taken by the writer. A written report must help a person who wasn’t at the incident understand exactly what went on.

  **Accurate** – Reports must be precise. Only facts should be included in the report unless your opinion is specifically requested. When quoting an individual you must use their exact words — paraphrasing is insufficient. Use quotation marks when documenting direct quotes.

  Precision is essential when recording times, dates, witnesses, descriptions and locations.
The qualities and characteristics of effective report writing are accomplished by adhering to the 4 Ws of Report Writing: Who, What, When and Where.

**Who**
- Identify the parties involved and obtain their identification numbers (badge #, S.S.#, driver’s license #).
  - Who was the victim?
  - Who reported the incident?
  - Who else was involved (employee, contractors, etc.)?
  - Who was the perpetrator?
  - Who should be notified for further action (supervisor, Labor Relations, police agency, etc.)?

**What**
- Identify the incident that occurred.
  - What is the violation?
  - What did you observe?
  - What did you say, hear and do?
  - What statements were made by the violator?
  - What statements were made by witnesses?
  - What evidence did you gather?
  - What did you do with the evidence?

**When**
- Identify the exact time you first became aware of the incident.
  - What was the exact date, day and time?
  - When did the incident take place?
  - If exact information is unknown or unavailable, provide the estimated time parameter during which the incident occurred.
  Note that the time is “approximate” in your report.

**Where**
- Identify where the incident took place.
  - If outside, be as specific as possible about the location (cross streets, address, etc.).
  - If inside, note by location, complex area, etc.
  - Where were you when you were made aware of the incident?
  - Where are the relevant items located?
Why not “How”? – Many times individuals ask why “How” is not included as a key component to effective report writing. When reporting “How” an incident occurred, there is a tendency for the writer to speculate and be inclusive or opinionated. An opinion is a conclusion without any evidence or investigation. Always be prepared to support your inferences with proper evidence or avoid using them in your report.
Lesson Objectives

When you have completed this chapter you should know

- a working knowledge of Physical Security.
- be familiar with the types of technology security officers use.
- general rules for information security.

Physical Security

What Is Physical Security?

Physical Security measures are the systems and processes designed to protect the physical assets of the client.

Perimeter Controls

Perimeter refers to the outermost boundaries of the property. The perimeter of a property most often is protected by barriers. Perimeter security devices are designed to keep people out and define property lines. The perimeter is usually referred to as security’s first line of defense.

Barriers

Barriers can be either man made or natural. Some examples of natural barriers are lakes or rivers, mountains, swamps or even deserts. Man-made barriers include walls, fences, security bars and turnstiles. Barriers are any structure used to define property lines, impede or deter entry or exit, delay intruders, restrict traffic and otherwise assist the security personnel in their responsibilities. Barriers also serve as a psychological deterrent, to detect intruders and decrease the need for additional security personnel.
Internal Controls

Internal controls may take the form of cameras, access control, lock and key systems, motion detectors, computer security, fire alarms and many more systems that may be applicable to your facility.

Access Control

The primary purpose for internal controls is limiting access. There are a number of access systems utilized at various client sites. There are four general categories of access control.

- Unmonitored Public Access
- Monitored Public Access
- Low-Security Limited Access
- High-Security Limited Access

Key Control

Issues to Review Regarding the Issuance and Control of Keys

It should be the responsibility of the key-holder and the supervisor who authorized issuance of the key(s) to ensure that all controlled keys are returned to key control employees. Keys should be returned if the key-holders transfer to another department, are terminated or have a change of assignment which make it unnecessary for the key-holder to have certain keys. Other issues you may want to review in a client’s workplace include:

- Keys should ideally be issued in person only, by designated key control employees, as authorized by a completed key request form, and should be signed for by the person to whom keys are assigned.
- Key control employees should conduct periodic physical audits of keys assigned.
- Outside contractors should only check out keys from key control employees when such keys are necessary for completing authorized work. Such keys should be returned at the end of each day’s work.
- The transfer of controlled keys between employees or between departments and employees should not be permitted. All assignment of controlled keys shall be through key control employees.
• The loss or theft of any key shall be reported immediately to the key-holder’s supervisor, key control employees and security. Replacement of lost, misplaced or stolen keys should be made in accordance with procedures for original issue.
• Individuals should be assessed replacement charges for lost controlled keys.
• All keys should be accounted for upon change in employment status, either by returning the issued key(s) or by paying the lost key charge, as specified above.

It is possible that your post orders will require that you control a significant number of the keys to the client’s facilities. Even if you do not maintain all of the client’s keys, security officers must maintain proper control over the keys within their possession.

■ Technologies That May Be Used on Your Site

Below is a list of some common forms of technology that security officers may work with in carrying out post orders.

• ID Card Readers
• Closed-Circuit Television
• Alarm Glass
• Pressure Mat Sensors
• Stress Detectors
• Motion Detectors
• Fire Alarms
• Photoelectric Controls
• Light Sensors
• Bar Coding

• Switch Sensors
• Vibration Sensors
• Cellular Telephones
• Laser System Sensors
• Doppler Sensors
• Infrared Sensors
• Flame Detectors
• Smoke Alarms
• Sprinkler Alarms
• Biometrics Detectors

Proprietary Alarm Systems?

Contractual security services and products provided by private security organizations such as PGS seek to protect the assets of business, government, communities and private clients. Proprietary security includes the methods implemented, equipment used and personnel employed by a security organization to carry out the fundamental role of protecting client assets. In
providing security to organizations, security systems seek to manage access by

1) controlling and monitoring access.
2) preventing and detecting unauthorized intrusions.
3) protecting property from theft, fire and vandalism.

Although the fundamental role of security remains the same, technological advancements modify the manner in which security is provided, assisting security officers in meeting our clients’ security needs.

**How Do Proprietary Alarm Systems Work?**

A proprietary alarm system contains switches and sensors which activate an alarm when access into an area has been forced; temperatures in a given area reach certain levels or instruments fail to function properly. When sensors detect one of the above, the alarm is activated signaling the security officer monitoring the area that a problem exists. The security officer’s response to the sounding of an alarm will vary depending upon the site post orders. As with all alarms, immediately notify the site supervisor and/or call 911 as prescribed in the site post orders.

**How Do Access-Control Systems Work?**

Access management or access-control systems deny or grant access based on the proper identification of an individual. The three main ways in which individuals are identified are

- through the use of codes entered into a key pad either manually or vocally.
- the use of cards containing coded information identifying the card holder.
- the identification of a biometrics attribute such as a voice, finger print, hand print or retina pattern.

Access is granted only after the electronic control unit has confirmed that information given is valid by checking it against an authorization file. This initial step ensures that the information, whether it is a PIN number, biometrics attribute or embossed card, matches that of an individual who has been cleared for access. Authorization files actually define when PIN numbers, biometrics attributes and prints permit admittance into the secured...
area. Additionally, authorization files respond to those circumstances that may arise suddenly, such as alarm activation. For example, alarm activation on the 6th floor of a building may prevent entrance to any secured area within the building.

Computer-controlled access systems have five main components: 1) the electrically operated locking device which controls the door lock; 2) the access credential — either the embossed card, the PIN number or the biometrics attribute; 3) the reading device which transmits the access credential information to the decision-making processor; 4) the electronically based decision-making processor which processes the information and determines whether or not access is granted; and 5) the monitoring device which records the who, what, where and when of access.

Computer-controlled access systems operate in the following manner. The card reader components generate electronic signals that are sent to the computer for processing. The computer program then verifies the request as valid or invalid via preprogrammed data, which resides in the computer’s data base, and then makes a logic decision to allow or deny access. The computer and computer programs come in a wide variety of configurations with numerous system features. Typical features include programmed entry/exit to limit access, system scheduling to permit schedules for various days, weeks and holidays.

■ **Intrusion Detection Methods**

Technology has not only allowed us to control access at authorized entrance points, but can also be used to detect unauthorized entry at the perimeter, into restricted areas, and even prevent access to objects.

There are a number of intrusion sensor devices in use today. The following is a list of common sensors and where they may be used.

- **Metallic Foil** – The foil is a thin metallic tape that carries an electrical current. Once the tape is broken the alarm is triggered. It is usually installed on glass.

- **Magnetic Switches** – These detectors are one part magnet with a switch assembly
connected to an actuator. When the connection is broken, the alarm is signaled. These detectors are often found on doors.

**Screen Detectors** – This detector is used to enhance window security. An alarm wire is woven through a window screen. If the screen or wire is cut, the alarm is activated.

**Pressure Mats** – This detector activates the alarm when weight is applied to the surface. It is often found in office areas and is placed under the carpeting.

**Capacitance Detectors** – This system is also known as an electrostatic intrusion detection system. This system can be found on walls, safes and even large openings. The system establishes an electrostatic field around an object. If this field is disturbed, the alarm is activated.

**Microwave Detectors** – This system operates on radio waves. Radio waves are transmitted into an area to an antennae. If all objects in the area remain stationary the reflected waves return at the same frequency. If there is a difference in the waves, an alarm is activated.

**Audio Detectors** – These are microphones that pick up sound and activate an alarm.

### What Is Closed-Circuit Television?

Closed-circuit Television (CCTV) is the form of technology most commonly used by security professionals. CCTV systems are widely used in industrial, commercial, residential and hospital settings throughout the world. The basic function of a CCTV system is to monitor an area for security threats such as intrusion, theft or fire. Essentially, CCTV is a security officer’s second set of eyes enabling him or her to monitor several areas at one time, or to monitor large areas. Occasionally, CCTV systems are combined with alarm systems.

This combination of technology and security personnel is an efficient and effective alliance. Another significant, but less obvious benefit of CCTV systems is the psychological effect a highly visible protection system has on individuals who are aware of it. In other words, most individuals who are aware the area is being monitored by CCTV systems modify their behavior accordingly.
**Basic CCTV Terminology**

Before discussing the technology behind CCTV, let’s take a moment to become familiar with some basic CCTV terminology.

- **Fixed Camera** – Views one area constantly rather than moving around the area.
- **Pan and Tilt** – A camera which may move up and down and side to side from a remote area.
- **Console** – An area that contains monitors, controls, or other devices which operate technology particular to that site or area.
- **Switcher** – A device which alternates the monitoring of the different cameras.

**How Does Closed-Circuit Television Work?**

In most applications, the operating principles of a CCTV system are basically the same and can be divided into three main components; the camera, the transmission channel and the monitor. These components operate together to capture, transmit and display the occurrences in a given area enabling security officers to provide the highest level of security which best protects our clients’ assets.

CCTV systems greatly assist in the monitoring and observing of parking structures and open spaces that clients contract PGS security officers to protect. The advancements in technology have not only enabled security officers to view more than one area at once, but in greater detail. Another benefit is the ability to record information seen through the CCTV, greatly assisting clients in the recovery of assets.

**General Rules for Information Security**

Most facilities have regulations and local policies set by the corporation or individual site for the handling of sensitive information. Security personnel should be made aware of all corporate and local policies and actively seek to implement them. When you observe a potential security threat, identify and report it to your supervisor so that the problem can be eliminated. The solution may be as simple as securing access to information through the use
of locks or passwords. Security has the responsibility to inform our clients and their employees who may not understand nor recognize problem areas. Listed below are some general techniques which when implemented will protect sensitive information.

- Check to see that all computer hardware and software is “locked-up” and “locked-down.”
- Observe and report any unusual activity or condition which may lead to possible information loss or disclosure such as unauthorized use of computers/terminals.
- Restrict access of information to authorized personnel. Ensure proper paperwork for outgoing material.
- Maintain visual inspection of sensitive areas such as computer rooms, file cabinets, etc.

By following these guidelines you are better able to protect information which is important to our clients as well as PGS.

**Why Safeguard Information?**

The reasons for protecting information whether it is PGSSs’ information, or one of our clients, are the same.

Information is protected to prevent:

- loss of a competitive advantage.
- loss of product information.
- loss of clients.
  - an individual’s loss of privacy.
- asset loss.

- disclosure of information.
- espionage.
- fraud and embezzlement.
- service disruption.
What Assets Need to Be Protected?

Paper, microfiche, computer hard drives and floppy discs are just some of the different ways in which sensitive information is stored. The type of sensitive information needing protection varies from site to site. For example, sensitive information existing on a classified site may differ from that at a non-classified location. Although the type of sensitive information may vary, the means by which it is protected are the same.

- Computer Hardware/Software
- Data
- Strategic Marketing Plans
- Laptop Computers
- Trade secrets
- New Technologies
- Contract Information
- Blueprints/Drawings
- Patent Information
- Experimental Equipment
- Classified Information
- Personnel Information
- Legal Documents
- Customer Data Base
Lesson Objectives

When you have completed this chapter you should know

- your role in an emergency.
- bomb threat procedures.
- terrorism basics.

Security’s Role in an Emergency Response

Security personnel play an important and critical role in the development and execution of emergency plans at a client’s site. This may include responsibilities such as evacuation of site personnel, protection of nearby residents, or providing medical treatment to any injured people at the location of the emergency. Information may be requested by investigating fire and/or police agencies, which the officer must be able to provide with clarity and efficiency, under stressful and sometimes difficult conditions. Further demands on security officers require them not only to protect all property as contracted by the client, but to restore daily routines after the disaster has been resolved.

The security officer is generally delegated to notify emergency services. You may very well be the one to initiate the emergency response, which may include the communication of emergency instructions to personnel at the site. Fire fighting, rescuing personnel, and assisting fire or police agencies are also critical roles in which security officers may find themselves during an emergency response.
Action Plans Needed

In order to be able to meet the demands of such responsibilities, it is critical that the security officer be well trained and have a well-rehearsed plan to implement at the facility being served. The amount of planning and training performed by all personnel concerned will directly influence the effectiveness of the response. Therefore, all plans should be continually reviewed and updated on a regular basis.

An emergency response plan needs to be constructed with the input of all employees on the site to which it applies. Such locally developed plans should be comprehensive enough to include all emergencies pertinent to that site. The Occupational Safety and Health Act (OSHA) dictates the specifics that must be covered. For those organizations that must comply with OSHA regulations, the plan must be in writing and be delivered to all site personnel verbally. Such requirements are exemplary guidelines for all sites to adopt when devising their own emergency plans. OSHA further requires the following information be outlined in the plan:

- emergency escape procedures and routes
- procedures for critical operations personnel remaining on site
- procedures for personnel accountability
- rescue and medical duties
- fire and other emergencies
- reporting procedures
- chain of command to contact regarding duties
- telephone numbers of your supervisor, client contacts, the police, fire department or other emergency responders
- access control procedures for employees, vendors and visitors during

Work place maps are an essential article in any emergency plan. They must clearly show the emergency escape routes and safe areas that personnel are to use. Work place maps should be posted in highly visible locations in each room or at each exit on the premises. Employees should be notified of their existence when they are hired and indoctrinated to the site. All employees should be told what actions need to be taken during any possible emergencies
that may occur, including a designated meeting place after evacuation. The 
plan should be reviewed with all employees upon development, whenever the 
emergency plan is changed and whenever any employee’s responsibilities 
change. Printed copies of the site emergency plans should be readily 
available, perhaps on an employee bulletin board for all to review. Input from 
the client or organization that constructed the emergency plan should be 
continually solicited, in an effort to keep the plan maintained.

**Chain of Command During a Disaster Response**

A well-defined chain of command is vital for emergency situations to be 
handled in an organized manner. This begins with selecting responsible 
individuals who are capable, and would be willing to coordinate the work of 
the emergency response team. The position, usually referred to as the 
“Emergency Response Team Coordinator,” is responsible for the overall site 
operations and personnel during any given emergency. This position may fall 
under the responsibility of the security officer on duty. The responsibilities 
include, but are not limited to:

**Assessing the situation:** The Emergency Response Team Coordinator should 
be able to quickly determine if an emergency actually exists on the premises. 
In order to do this, they must be thoroughly familiar with the physical plant — 
both internal and external facilities. They should be knowledgeable of all 
personnel assigned to the site and the potential danger for each in any given 
emergency. The assessment of the situation should have the safety of the 
people involved as its primary objective.

**Activate procedures:** Emergency procedures that have been established at a 
given site need to be put into place. The security officer on duty and/or the 
Emergency Response Team Coordinator who is responsible must follow these 
procedures so that all employees on site will know what to expect throughout 
the emergency. This may range from announcing on an intercom the fact that 
the site is currently in an emergency situation, to turning on an alarm switch 
that audibly alerts the employees of the emergency. Have names of emergency 
contacts, and telephone numbers of police, fire and ambulance services posted 
and accessible. The Emergency Response Team Coordinator and/or security
The officer’s responsibility would be to activate the emergency procedures without undue alarm or hazard to any site personnel. This includes contacting the police, fire department or other emergency responders.

**Evacuation and directing efforts of personnel:** If appropriate, calmly direct personnel to exit to a safe location. Although personnel should be well-informed, and have practiced evacuation procedures for the various emergencies that may occur, the security officer and/or the Emergency Response Team Coordinator needs to oversee such operations. This would include knowledge of all personnel present at the location prior to the emergency, including visitors, customers, and facilities available to emergency personnel such as water sources and gas outlets. Under stressful conditions, procedures need to be followed strictly so that all personnel are safe.

**Assisting emergency personnel:** Should emergency professional services be needed on the premises, it may be the security officer’s responsibility to initiate or confirm that such a call has been made. The call, either by the officer or another individual at the scene, needs to be documented as soon as possible. This pertains to police agencies, fire departments and medical personnel called upon to assist in such situations. Provide information to the police, fire department or other emergency responders. Through your directions, they can attend to the needs for which they have been trained without delay or interference. Assist as appropriate and/or as directed. A disaster may require a security officer to work beyond prescribed hours, locations and duties. A security officer must be willing to work a problem through to conclusion. Never abandon the client, the site or its employees.

**Directing shut-down operations:** The last responsibility of the Emergency Response Team Coordinator would be to direct the shutdown of the facility’s operations. Prior disaster response planning would generally have the shutdown of different sections of the site assigned to various employees. These people would, in turn, be responsible for vital efforts as necessary to prevent further emergencies (i.e., securing keys, cutting main electrical power supplies, turning off any gas mains, etc.). By following the proper chain of command, each person assigned to a particular job reports “upward” to the
next assigned disaster response supervisor until reaching the Team Coordinator. In order to verify the information, a written documentation system should be in place at all levels in the “chain.” A thorough shutdown of the entire facility not only ensures that all dangers are addressed, but will generally minimize the exposure of further danger to all individuals in the area.

**Area Security**

It is the responsibility of the security officer at the work site to keep the client’s operation secure and safe. However, in times of emergency, the level of security needed may stretch the limits of the security personnel assigned to the site. This includes securing the area to prevent unauthorized personnel from entering the location. Also important is establishing an atmosphere of normalcy for the employees. Whether directed by an Emergency Response Team or by security, an off-limits area must be established by cordoning off the emergency area with ropes, signs or barriers. Securing or retrieval of records belonging to the client may also be the responsibility of security or the Emergency Response Team. These may include accounting files, legal documents, personnel files, classified information and computer software. These records should be protected within the facility.

**Bomb Threats**

■ **What Is a Bomb Threat?**

Any verbal or written warning that declares an explosive or incendiary (burning) device is about to be set off on the premises is considered to be a bomb threat. Be aware, however, that for every real bombing incident, only one in five (20%) actually has any warning given prior to the explosion. That is why knowledge of the site and alertness to anything out of place or suspicious is important to a security officer. A security officer must always be alert and assume that all threats are real.

Bomb threats affect the client by creating

- possible danger of human injury and/or death.
- possible structural damage to the site and materials housed at the site.
Reacting to the bomb threat or incident can be very costly to the client in terms of lost time at work, lost wages and accompanying stress on all personnel.

**Factors to Consider**

The overall likelihood that a device has been or will be introduced can be minimized if certain controls have been considered in initial site security planning. Should a call, note or other communication indicate the existence of a bomb the following should be considered as quickly as possible:

- Could an authorized person have brought in an explosive or incendiary device without security detection?
- Could an unauthorized person have gained access to the facility without observation for the purpose of bringing in an explosive or incendiary device?
- Could a device have been introduced through a receiving department, by way of mail channels, delivery truck, vendor car, boat or rail?
- Could a device remain on the site premises without detection?
- Could an explosive or incendiary device be created on the premises?
- Could a device be introduced by some unusual delivery system (i.e., sling, rocket launcher, etc.)?

Keeping these factors in mind will reduce the possibility of the existence of an actual device onsite. The probability can be reduced even further by protective, cost-effective countermeasures taken by a security officer. These countermeasures include thorough investigation of all areas under a security officer’s supervision and an objective approach to the probability that an incendiary or explosive device could be placed on the site by anyone at any time. The importance of security patrols in spotting anything unusual or out of place and reporting such suspicions to the supervisor cannot be over-emphasized.

In the worse-case scenario, extreme damage can be caused when a large number of people are exposed to an explosive device. They might not have protective shelter or time in which to escape. Direct property damage and damage by secondary effects such as fire following the explosion need to be part of security’s planning. Related loss of property may also be a factor as it
affects delayed or deferred operations, schedules and/or nonproductive wages. Emergency equipment damage must be considered as well. This is important in situations such as when sprinklers are put out of commission from an explosion, but are needed to extinguish subsequent fires that have started. As a security officer you must be aware of alternatives, such as extinguishers and their locations.

Frequently, losses to the client may be reduced if security responds according to a well-conceived emergency response and evacuation plan or by preventing the incident altogether. Approved emergency evacuation instructions by the client are often the key to minimizing loss, as well as planned rehearsals by personnel to respond to possible incidents/bomb threats.

**Threats by Telephone**

If you receive a bomb threat over the telephone, it is important to keep the person talking to get as much information as possible. When this happens, signal another person to help. Write information down and get your team member to relay the information to dispatch or the supervisor. Upon receipt of the information, report it immediately to the police. Negotiations with the individual who allegedly placed the bomb or is making the threat is not your job. The information that you have gathered is to be turned over to the appropriate authorities as soon as possible.

The client’s facility should have a bomb threat procedure. Should you be the individual taking the call and determine that it is a bomb threat, it will be one of two types of calls:

- bomb on the site at unknown location
- bomb on the site at a specific location.

These types of phone calls are serious and should be answered with care and calmness. Never show fear in your voice. The caller should be kept on the line as long as possible.
Listen carefully to the caller’s conversation/message so that you can get the basic information to locate the bomb, and the exact time it is set to explode. Some facilities provide an audiotape on the phone system for taping suspicious calls. Assume that the call is not a mere threat and the longer the individual talks to you the more you can learn and report.

Do your best to clearly and accurately write down the answers to the following questions in order of priority:

• “Where is the bomb?”
• “What time is the bomb set to go off?”
• “May I ask who is calling?”
• “Is there only one bomb?”
• “How large is the bomb?”
• “What kind of a bomb is it?”
• “What kind of timing device is on the bomb?”

Write down the exact time the call is being made.

The first two questions need to be confirmed before moving to the other questions. Any other questions that you can think of to keep the caller on the line will give you a chance to study voice patterns, vocabulary and mood of the caller.

In such a situation, try to determine where the bomb is located, get off the line and notify your superior at once. Tell no one other than those authorized to know such information about the call. Special care should be taken so that people in the vicinity of the phone will not overhear your questions. Overheard conversations about a bomb threat may very well cause a panic that could spread throughout the site.

**Written Bomb Threats**

When a bomb threat has been made via written communication, it may be delivered by the actual perpetrator, by a third party or communicated by way of computer electronic mail. The security officer on site that may receive such a message is to contact the supervisor immediately and document the threat on an Incident Report when the incident is over.
The Usual Delivery Methods and Placement of Bombs

Placement and transportation means of explosive or incendiary devices are dependent upon the attacker’s nerve and knowledge of the premises. In a common public structure, locations that would ordinarily be unlocked and/or without surveillance are the most vulnerable. The following are examples of susceptible locations:

- washrooms/lavatories
- janitors’ closets/trash containers
- fire stairs
- telephone booths/terminals
- receiving platforms
- tenant common areas
- hallways/lobbies
- elevators.

Potential bomb placement may occur using lakes, rivers and ponds at facilities that use these natural resources on the premises. Security officers need to be aware of such potential placements. The same is true for incoming vehicles such as railroad cars, trailers, tractors, etc., which should undergo some form of security check before entering the premises. Most bombs are delivered through standard access routes by conventional means.

If you discover a suspicious bomb device while you are on a search, or on one of your regular site inspections

- **DO NOT TOUCH IT.**
- **DO NOT ATTEMPT TO MOVE IT.**
- **NEVER TRANSMIT BY RADIO OR USE A LIGHT SWITCH IN THE IMMEDIATE AREA NEAR A SUSPECTED BOMB.**
- **CLEAR EVERYONE, INCLUDING YOURSELF, OUT OF THE IMMEDIATE AREA.**

The security officer should make a request for immediate assistance from the contact person for such discoveries, usually your supervisor or the police.
This call should be made by telephone in order to avoid possible detonation by use of a radio. Frequency exposure from the use of the radio could trigger the bomb.

Your report should include an accurate description, time and location of the device found. If the client management or bomb-search leader authorizes an evacuation, you may be asked to

- Evacuate the area around and above the device.
- Barricade and block all entrances to the area.
- Open all windows and doors in the area to permit any blast wave to escape.
- Establish access controls to prevent personnel from re-entering the area/building.
- Ensure that evacuated personnel are in a safe area away from possible flying debris if the device does explode.
- Shut off gas and fuel lines at main switches.
- Assist responding emergency personnel.

A professional explosives team will quite often be the main contacts dealing with the search and containment of any discovered device. Unless requested to assist this team, the security officer is to assist in keeping the employees and site visitors in a calm state during their possible confinement while a search is being conducted. A security officer may be assigned to control access of media personnel that have been informed of the search or location of the device.

**DO NOT SPEAK TO THE MEDIA REGARDING THE ONGOING ACTIVITY** or any activity on the client’s site. According to the site security plan or prior planning with the client’s management, refer all inquiries that are made to the client spokesperson.
Evacuation Procedures

Bomb threats that provide specific information concerning bomb location and time of explosion normally result in evacuation, but even then rapid searches of evacuation routes are necessary. When the designated person with the authority to call for evacuation decides to make the order, you will be a highly critical factor in the safety and effectiveness of the operation. In a partial evacuation, which would take place after certain floors or areas have been searched, a general alarm would not be sounded. This applies to high-rise complexes where an entire floor is evacuated but not necessarily the entire site or similar locations.

A security officer is usually responsible for crowd control in assembly areas. These areas, given all geographical possibilities available, should be located at least 300 feet from the building or location where the danger is reported to occur. The security officer’s leadership will be necessary to avoid panic during the evacuation. Management expects the security officer to be familiar with their responsibilities, and to give guidance and direction to those needing it. It is also important for the security officer to know their responsibilities during post-evacuation procedures.

The client needs to have their facility returned to normal operation as soon as possible. Personnel need to return to their work locations with a feeling of safety and assurance that all measures have been taken for their security. Any person observing the operation needs to receive the message that the facility is tightly protected against any further threats. The professional action of the security officer has an important impact in all these areas.

Introduction to Terrorism

Definition of Terrorism

Terrorism is defined in the U.S. by the Code of Federal Regulations as: "..the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85)
Most terrorists do not consider themselves terrorists but view their cause as righteous and their actions acceptable in religious or political terms. One of the primary goals of these organizations is to bring attention to their cause and turn a nation’s citizens against government policies.

**Types of Terrorist Organizations**

Terrorist organizations can be into two different groups, domestic or “home grown” terrorists and international terrorists. Since September 11, 2001, much of our focus has been on the Islamic terrorist organization Al-Qaeda, but domestic terrorists have been active throughout North America for decades.

**Domestic Terrorists**

The 1995 bombing of the Oklahoma City federal building, which killed 168, remains the deadliest act of terrorism against the nation by a U.S. citizen. Domestic terrorism involves groups or individuals whose activities are directed at elements of the government or our population without foreign direction. The people and groups range from white supremacists, anti-government types and militia members to eco-terrorists and people who hate corporations. They include violent anti-abortionist and black and brown nationalists who envision a separate state for blacks and Latinos.

**International Terrorists**

Terrorist activities that are foreign-based and/or are directed by countries or groups outside of the United States are considered international terrorist organizations. Presently, the Department of State lists seven countries as state sponsors of terrorism: Iran, Iraq, Sudan, Libya, Syria, Cuba, and North Korea. Of these, Iran represents the greatest terrorist threat to the United States. Despite a moderation in its public anti-U.S. rhetoric since the election of Mohammed Khatemi as president, the Government of Iran remains controlled by conservative clerics opposed to reform and normalization of relations with Western countries. The Government of Iran continues to target dissidents living outside the country and supports financially and logistically anti-Western acts of terrorism by others.
The Role of the Security Officer

PGS security officers are not counterterrorism experts, but they do play an intrical part in the deterance and detection of terrorist activity. By conducting effective patrols, and following post orders you can ensure that our PGS clients are not an easy target.

Security officers should be alert for the following:

- Anything out of the ordinary, such as backpacks, briefcases, and boxes abandoned with no owner in sight.

- Suspicious activity. For example, possible terror suspects may conduct reconnaissance at an area prior to an attack.

- Maintaining proper access control. While it is difficult to secure common areas, officers should make certain that restricted areas have appropriate levels of security as determined by management.

- Monitoring public access areas. Public access areas are our greatest vulnerability.

With regard to people, officers should look for and be aware of the following:

- People in restricted areas.

- Anyone looking lost, especially in non-public areas.

- Anyone who appears to be conducting surveillance (e.g. using a camcorder, camera, cell phone camera) in non-public areas.

- Anyone causing disruptions or who appears to be intentionally creating a distraction.

- Someone who abandons an item and leaves the area quickly.

- Any vehicle parked illegally, driving erratically, or otherwise suspicious.
For suspicious items, officers should focus on the following:

- Anything left abandoned, both left in the open and hidden, that appears to be suspicious or dangerous such as a canister, tank, metal box, bottle, etc.

- Anything emitting a mist, gas, vapor, or leaking in anyway.

- Items with visible wires, timers, pipes, etc.

- An item in an area that might be the cause of people coughing, having trouble breathing, losing consciousness, or exhibiting any other medical condition.

The terrorism threat is a constantly changing dynamic in today’s world. As a security professional you should be aware of possible threats to PGS clients’ personnel and property. Use the websites below to stay abreast of the latest intelligence available on suspected terrorism.

http://wits.nctc.gov/Reports.do

http://www.dhs.gov/dhspublic

http://nsi.org/terrorism.html

http://www.fbi.gov/terrorinfo/counterrorism/waronterrorhome.htm
Lesson Objectives

*When you have completed this chapter you should know*

- understand safety awareness at the client site.
- basic fire prevention and extinguishment.
- bloodborne pathogens.
- hazardous communication.

Assessing the Client’s Safety Risk

As a PGS security officer, your part in helping maintain a safe, healthy work place minimizes risk. Risk management is essential for even the smallest clients. A work injury that disables a worker can seriously harm the financial viability of the client. Injuries to customers or passers-by can damage the client’s good name and impact their future earnings. The total cost of even minor injuries can be high in terms of lost time or income to the client.

Prevention of work-place injury and illness is the objective of all types of businesses, regardless of industry, size or complexity. One of the goals of the security officer is to help their customer maximize safety in the work place. As a security officer, one of your goals is to control risks arising from the interaction of these elements at the client’s work place:

- people
- equipment
- materials
- work environment.
Ask Yourself These Questions

Are customers and members of the public protected from the operational risks of the client’s business?

Examples:

• providing a defined public area for customers to wait in.
• providing fences around pits and hazardous work areas.

When visitors are admitted to the client’s work area, are their movements restricted to non-hazardous areas? Are repair or maintenance contractors made aware of hazards existing in the area where they will be working? In the ideal work place, they will be.

Is the Equipment Safe?

All of our clients rely on equipment of some sort. During the course of your patrol, make sure to do the following:

• Information and Training. Before using equipment make sure you have been trained properly. If applicable to you and the equipment you use, make sure specified manufacturer maintenance schedules are followed.
• Regular Inspections. Equipment can suffer damage or wear and tear in normal usage. Make sure inspections are performed by a trained professional according to regular maintenance schedules. Are materials used safely?
• Client Equipment. If you observe client equipment being used improperly or not maintained, report it up the chain of command.

Materials in the client’s business might include everything from stock items in a cleaning room, to sheet steel used in manufacturing, or fertilizer sold by the landscape supplier. No matter what materials are involved in the client’s business, the following are the most common safety problem areas.

Handling and Storage. Strains, sprains and serious long-term injuries to backs, shoulders, arms and hands are the most common work-place injuries. Though finding the solutions rest with the client, as a security officer you may observe problems and should report them to your supervisor. Both you and your supervisor might recommend possible solutions to the client, such as
• using mechanical lifting aids
• changing the work process, where possible, to reduce the need for continuous manual handling tasks
• storing heavy items at waist level to minimize bending and reaching
• ensuring items in racks can be reached safely.

Hazardous Substances. It is necessary that any hazardous or dangerous substances are identified, correctly handled and stored. Suppliers provide safety information on hazardous substances by labeling containers and making Material Safety Data Sheets (MSDS) available. The labels can be used by the client to select the safest substance for the job and to ensure that it is used, stored and disposed of safely.

If you see something out of the ordinary, such as a spill, seek the advice of the client prior to handling any hazardous material. Contact the client and your supervisor immediately when confronting a hazardous material situation and alert anyone who might be impacted by that hazardous material in the immediate area.

Can You Help Create a Safe Work Environment?

While the safety of the equipment, materials and work processes all impact you, the client’s employees and other people, the nature of the working environment is also a major factor. Examples of environmental factors to be controlled to improve safety can include:

• buildings and fixtures
• air quality
• temperature
• lighting
• noise
• electrical fittings
• clear access to work areas and exits
• floor surfaces
• emergency equipment
• first aid kits
• conditions of stairways.

Regular inspections of these elements of the client’s work place are necessary
to ensure that they do not pose a health or safety risk. To reduce the risks to health and safety in the client’s business, it is necessary to follow a few simple steps. Costs are generally very low, but benefits to the client’s business and its operators, workers and customers can be enormous.

**Information**

It is not sufficient for a client’s business to rely on its own risk experience, as this may be too limited. Industry-wide information is important to review. Additional sources of information may be

- business, industry and trade associations
- workplace health-and-safety agencies at the community, state and federal level
- plant or equipment manufacturers and suppliers
- material safety data sheets
- suppliers of materials and substances.

**Analysis**

Once armed with the available hazard information about the client’s type of business, look for the hazards during the course of your patrol. What could prove a risk to you, or others in the client’s workplace? Don’t forget to ask the clients what they consider hazardous.

When you report a hazard, the client will identify the equipment or situation that may prove to be a risk. They will consider that risk according to possible severity in terms of life, suffering and dollar cost by analyzing the following:

- past accident and loss information
- maximum potential for loss
- likelihood of reoccurrence
- number of people at risk.

**Control**

Know your post and post orders. Be aware of hazards and hazardous materials. Have emergency numbers accessible to contact your supervisor, the client and emergency responders. Once the hazards have been identified on your report, and the risks assessed, your supervisor could recommend control measures that may be used to reduce the risk of injury. There are a number of
ways to control risks, and our recommendations might include

- eliminating the hazard
- reducing the hazard source
- removing or reducing the extent of people’s exposure of to the hazard
- supplying and using Personal Protective Equipment.

■ What You Should Inspect During Your Patrol

As a security officer, you should have a goal of promoting industry standards for safety to prevent people from being injured or becoming ill as a result of activities at the client’s work place. During the patrol of the client’s work place, identify potential hazards and associated risks that could cause injury. Decide what you can recommend to remove or minimize these risks. While on patrol, observe and report on the following general hazard areas:

- manual handling procedures
- hazardous substances
- plant machinery
- noise
- work-place environment.

■ Controlling the Work Place Environment

A PGS security officer can, as a result of his or her normal patrol, help control the risks of injury where they work. The client’s work environment can affect you, the clients and customers. All people should be protected from the client’s work-place risks.

Given the range of risks that can be associated with the work environment, injuries can differ. For instance, slips, trips and falls can result in sprains or fractures, while extremes of temperature can result in heat stress or hypothermia.

In the discussion on hazard areas, the term “work environment” is very broad and includes

- floor surfaces, buildings and fixtures, air quality, temperature, lighting and
electrical fittings in the client’s work-place
• general housekeeping at the work place, such as making sure that aisles and exits are not obstructed
• an emergency plan so that people can respond quickly and effectively to any incident that happens in the work place
• other work environment issues like infectious diseases, violence, sun exposure, shift work, confined spaces and working at heights, etc.

Assessing the Risks
In assessing the risks associated with the work environment, the following could be considered:

• the number of people at risk
• the likelihood of an incident happening
• the seriousness of the injury or illness should an incident happen.

How the Risk Can Be Reduced
After discovery of a risk during your patrol, you may recommend to your supervisor:

• replacing the material with a less hazardous one, (example: wearing shoes with nonskid soles when working on slippery flooring)
• redesigning the individual work place layout to reduce manual handling risks
• isolating, closing-off or guarding (example: keeping the hazard and people apart by shutting a door on a noisy, confined space)
• adjusting the time and conditions of the client’s exposure to the risk (example: rotating tasks so you do not spend too long in hot or cold conditions)
• using Personal Protective Equipment when other ways of controlling risks cannot be used (example: bringing appropriate clothing when you are going to be working in a freezer).
The risk-reduction measures outlined above are only examples. Examine the client’s work place during your patrol, and recommend to your supervisor any risk reduction measures that are suitable to the work being conducted.

### Personal Protection

Once you’ve been trained, you should know how and when to use Personal Protective Equipment (PPE) and, if applicable, how to care for it. It is your responsibility to follow your client’s instructions about work-place health and safety issues. If you have any questions, ask your supervisor.

**What Should You Do?**

If you use PPE provided by a client, you have an obligation to act responsibly.

Specifically, you should

- Follow the client’s and/or employer’s instructions given to ensure health and safety.
- Not willfully or recklessly interfere with or misuse anything provided by an employer to ensure health and safety.
- Use PPE as you’ve been trained to do.
- Use common sense.

You should be given training in equipment and the proper care for any PPE that you are required to use. Much of this training is required by OSHA and/or state and local regulations.

**Types of Personal Protective Equipment**

**Head protection.** Protective headwear should be worn whenever you are in SAFETY HELMET areas and/or in any place where you risk a hit on the head.

**Eye and face protection.** Many jobs — grinding, drilling, chipping, welding and handling dangerous substances — require PPE for your eyes and face. Ideally, eye-wash stations should also be provided, and you should know their locations.
Ear protection. When the noise level is high, your hearing is in danger. Wear earmuffs or earplugs when grinding or using other high-noise machines. Don’t share ear protection gear with other workers.

Respiratory protection. To protect your lungs where there is a risk from harmful dust, fumes, vapors or gases, you will need the right equipment with the right filters for the particular job. Don’t share breathing protection equipment with other workers or you risk infection.

Hand protection. Various types of gloves are available to protect hands from injury.

Foot protection. Safety footwear can protect feet from some hazards at work. Footwear should be suitable for the job.

Clothing. The clothes you wear should be appropriate for the job you are doing. Loose or torn clothing might catch in machinery or on other items.

Examples of other PPE devices:

- A safety harness or lifeline can protect you from the risks of falling, and can be used to conduct a rescue if you are working in a confined space.
- High-visibility clothing, such as brightly colored fluorescent vests for day work and reflective material on clothes for night work, can help to make you more visible to traffic.
- Life jackets and other rescue materials can provide protection against drowning when working in or near water.
- Showers for hazardous spills or splashes on workers.

Safe Housekeeping and Work-Place Sanitation

Good housekeeping is important for maintaining a safe work place. Each security officer is responsible for maintaining his or her work area in a clean and sanitary condition. All materials should be properly stored.
Are the Client’s Work Place and Equipment Clean?

As a PGS security officer, one of your goals is to minimize the risks of injury and disease associated with a client’s work-place cleanliness. Injuries including lacerations and cuts, can result from the use of or exposure to machinery and equipment. In an unsanitary work place, the risk of subsequent infection, leading to disease, increases dramatically.

You may be able to help make the client’s work place safe by meeting your obligations in

- ensuring your own health and safety and that of others at the work place
- using Personal Protective Equipment in accordance with training instructions
- following instructions given to ensure health and safety
- not willfully or recklessly interfering with or misusing anything provided by the client to ensure health and safety.

The client may have measures in place to ensure your health and safety. You should use these safety measures. They could save a life!

Fire Prevention

As a PGS security officer you are in the business of protecting individuals and property from theft and damage. Built into a security officer’s job description is the duty to be alert to signals that indicate a threat to human life and/or property. One such threat is fire. As is the case with all safety threats, the surest means to protect lives and property is through constant vigilance and alertness to the potential causes of fire.

Fire Hazards

In order to prevent fires from occurring one must be familiar with the various fire hazards. Listed below are some common fire hazards that are encountered at some sites. Think of these hazards as possible sources of ignition.

- poorly maintained appliances and fire equipment.
- obstruction of fire prevention equipment.
- poor housekeeping and storage practices (e.g., items stored near heat sources).
- hazardous materials improperly stored or marked.
- faulty electrical wiring.
• lack of cutting and welding procedures.

**Work Site Fire Emergencies**

Figures recently released by the United States Fire Administration indicate that although industrial fires account for less than 22% of U.S. fires, they represent 46% of dollar losses incurred from fires. The dollar amounts are greatly reduced when fires are caught in their incipient stages. An incipient fire is one that can be put out with only the use of a portable fire extinguisher. The speed at which fires grow and spread makes a security officer’s duty of activating the alarm system crucial.

**Fire Development**

The National Bureau of Standards for Fire Research in Washington, D.C. has conducted a series of tests to study the development of fires. The tests were conducted in a room measuring 10 feet by 15 feet with a sofa, chair, footstool and bookcases. The ignition source was similar to that of a cigarette dropped on a newspaper. The fire progressed as follows.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 seconds</td>
<td>Smoke drifts from newspaper</td>
</tr>
<tr>
<td>20 seconds</td>
<td>Smoke has risen to ceiling — becoming more dense</td>
</tr>
<tr>
<td>40 seconds</td>
<td>Visible flame over the newspaper</td>
</tr>
<tr>
<td>1 minute</td>
<td>Sofa becomes engulfed in fire flame 3 feet high</td>
</tr>
<tr>
<td>1 min. 30 sec</td>
<td>Smoke flows out of doorway; flames from sofa reach ceiling; ceiling temperature 350°F</td>
</tr>
<tr>
<td>1 min. 45 sec</td>
<td>Entire sofa engulfed in fire; smoke level increasing rapidly</td>
</tr>
<tr>
<td>2 min.</td>
<td>Ceiling temperature 800°F dense smoke within 3 feet of floor</td>
</tr>
<tr>
<td>2 min. 15 sec</td>
<td>Flames emerge from doorway — ceiling temperature 1,000°F</td>
</tr>
<tr>
<td>2 min. 30 sec</td>
<td>Carpet ignites; heavy flame and smoke to ceiling — temperature 1,500°F</td>
</tr>
<tr>
<td>2 min. 45 sec</td>
<td>All contents of the room are involved; thick black smoke and toxic gases; room temperature peaks at 1,800°F</td>
</tr>
<tr>
<td>20 min.</td>
<td>Fire begins to die down</td>
</tr>
<tr>
<td>25 min.</td>
<td>Only small flames remain; room temperature is 800°F</td>
</tr>
</tbody>
</table>

Remember, all fires start small, but they grow and spread rapidly, destroying property and lives in a matter of seconds. So your initial response needs to be
swift and accurate. Commit to memory the location of fire alarms and extinguishers as emergencies don’t provide time to locate them.

The information found on the list below should be committed to memory or written down in a highly visible location. This information will serve as a guide to help you prepare for a fire emergency.

- the location of all fire alarm boxes
- the location of all fire extinguishers
- the type of fires each extinguisher is rated for
- the fire rating of the materials in your work area
- your site’s established escape routes
- your site’s evacuation procedures

Two Important Questions to Ask if a Fire Emergency Occurs:

Remember a PGS security officer’s position regarding fires is one of prevention. Security officer training does not provide officers with the necessary expertise to fight fires like trained fire fighters. Therefore a security officer’s first response is alarm activation. Beyond activation of an alarm, do not initiate other actions unless two criteria have been met: necessity and safety. These two criteria are said to have been met when “yes” applies to both of the questions listed below.

- Is what I am about to do SAFE?
- Is what I am about to do ABSOLUTELY NECESSARY?

The answers to these questions are not evident until one assesses the type of fire and the extinguishing method most appropriate for intervening. The following sections are designed to assist security officers in accurately assessing the extent to which the above criteria have been met.

Above all else, activate the alarm prior to asking these questions. If either response is “NO” or if there is any doubt, WAIT FOR ASSISTANCE!!!!
Fire Equipment

The following segment is designed to provide security officers with the knowledge needed to correctly intervene in those instances where it is safe and absolutely necessary to do so. It is important that the distinctions among the various types of fires as well as their fuel sources are known as improper intervention (e.g., using the wrong type of fire extinguisher) is dangerous to the individual fighting the fire and may fuel the fire rather than extinguish it. Essential to basic fire knowledge are the classifications of fire and the type of extinguishing method to be used with each fire type. We will briefly discuss the classifications of fire and fire extinguishers.

Classification of Fires and Selection of Portable Fire Extinguishers

To better understand how fire extinguishers work, it is important to have a basic understanding of the fire triangle upon which fires are classified. As stated earlier, there are three elements needed to ignite and sustain a fire: oxygen, fuel and heat. Fire extinguishment is based on the elimination of one or more of these elements.

Fire extinguishers are often referred to as the “first aid” of fire protection as they are the first line of defense against a fire. Hand-held fire extinguishers are for use on fires of limited sizes, such as incipient stage fires. Fire extinguishers are rated A, B, C, and D correlating with the type of fire they are designed to extinguish. Extinguishers may contain water, foam, dry chemical, carbon dioxide, halon or dry powders. It is very important to choose the right extinguisher for the type of fire, as the wrong extinguisher can make the fire worse, and in extreme cases cause death.

Traditional Labeling

Not all fire extinguishers can be used on all fires. Fire extinguishers are rated according to their suitability for use on specific classes of fire. Suitability for use is identified by classification of fire and traditional symbols:

- Class A = Green triangle with an “A”
- Class B = Red square with a “B”
Class C = Blue circle with a “C”
Class D = Yellow star with a “D”

The number of symbols present on the extinguisher label indicate its suitability for use on one or more types of fires. For example, the popular ABC extinguisher can be used on A, B and C type fires.

**Rating by Capacity**

In addition to the type of fire, Class A and Class B fire extinguishers are also rated according to their relative capacity to extinguish a fire. A number proceeds the letter (type) classification; the higher the number, the greater the extinguisher’s capacity. As stated earlier, in a fire emergency you do not have the luxury of time so the ability to quickly and accurately read labels is crucial. Seconds in a fire emergency can cost human lives.

To better ensure your own safety as well as the safety of others and property, adhere to the following tips:

- Know where the fire extinguishers are located.
- Know what kind of fire extinguishers you have.
- Know what kind of fire extinguisher is suitable for all materials present on your work site.
- Know how to operate the fire extinguishers on your site.

The key to fire safety is fire prevention. The more prepared you are, the better equipped you are to quickly, calmly and accurately respond to a fire emergency.

**Fire Extinguisher Operation**

Portable extinguishers, regardless of the classification of fire they are designed to extinguish, operate the same way. The acronym PASS will assist security officers in using an extinguisher properly and effectively.

**Learn to P.A.S.S.**

Pull the pin. Some units require releasing of a lock latch, pressing a puncture lever, or other motion. Operating instructions are required by law to be on the extinguisher label.
Aim the extinguisher’s nozzle, horn or hose at the base of the fire.

Squeeze the handle or trigger.

Sweep from side to side at the base of the fire until it is completely extinguished. Watch for re-ignition and reactivate extinguisher as necessary.

**Caution: Fire extinguishers will not operate in an inverted (upside down) position.**

When a security officer makes rounds, it is important to note the last time the extinguishers were inspected by the fire department. Attention should also be given to whether or not the equipment is obsolete or unsafe to use. If it is determined that the fire extinguishers currently in place need to be replaced, immediately report it to the site supervisor.

### Fire Hoses

Although there may be hoses at hand, the use of a fire hose by a PGS security officer is only done under exceptional circumstances or when a security officer who has proper training, is specifically asked to do so by a supervisor. Remember, a fire spreads quickly and in the amount of time it takes to get the hose out and begin hosing the fire, the entire room can be engulfed in flames. Consider this, a fire can consume furniture, floor and ceiling boards, reaching temperatures of 1000°F, in approximately two minutes.

#### Automated or Fixed Systems

Most industrial complexes and office buildings utilize some form of automatic or fixed alarm system. These systems deploy water, foam, dry chemical, CO₂, halon or other neutralizing agents when sensors indicate that temperatures far exceed normal levels. Security officers are not responsible for checking or monitoring these systems unless specified in the site’s post orders. However, if a security officer becomes aware that an automatic system has been activated, contact the site supervisor immediately and wait for further instructions. If given instructions to investigate that particular area, exercise extreme caution and adhere to the following:
• When approaching a room where a fire has been reported, never open the door without first feeling it to see that the door does not exceed room temperature.

• When approaching a building, do so with extreme caution, and visually scan for smoke or the smell of burning substances indicative of fire.

• Do not enter a room immediately after a fixed fire extinguishing system has been discharged without proper personal protection equipment.

Watch the required Bloodborne Pathogen Video
Complete Bloodborne Pathogen Acknowledgment Form

Watch the required Hazardous Communication Video
Successfully pass the Hazardous Communication examination
Complete the Hazardous Communication Acknowledgment Form
Lesson Objectives

When you have completed this chapter you should know

• the sections of the NISPOM
• the non-disclosure agreement
• proxy agreement and FOCI
• required NISPOM threat awareness and defensive security briefings
• the government security classification system.
• employee reporting obligations and requirements.
• security obligations and duties applicable to the site.

National Industrial Security Operations Manual (NISPOM)

Sections of the NISPOM

The following information is provided as a guideline to your duties and responsibilities when working at one of our clients cleared facilities. Each client has his or her own set of security regulations. But all security regulations, regardless of differences in client facilities, are set forth in accordance with the National Industrial Security Operations Manual (NISPOM).

The NISPOM is divided into 11 chapters listed below:

1. General Provisions and Requirements
2. Security Clearances
3. Security Training and Briefings
The Nondisclosure Agreement

The NISPOM (3-105) states that before an individual is given access to classified information, he or she must sign a nondisclosure agreement (SF 312). In addition to asking that the employee read and sign the SF 312, the security professional should verbally communicate to the employee what the agreement represents. SF 312 is essentially a lifetime contract between the employee and the U.S. Government, in which the employee agrees to protect U.S. classified information from unauthorized disclosure.

The agreement may affect the employee in a number of ways. It may require that the employee seek review and approval of any written material prior to its being presented verbally or in written format. It may limit the employee's ability to freely discuss his or her work with colleagues, relatives, and others. Violation of the agreement can result in a wide array of legal actions against the employee, ranging from civil suits to a succession of more severe penalties. Penalties for breaking the nondisclosure contract may include loss of clearance, fines, and criminal prosecution under several statutes. The government may also bring a civil suit against the employee and seize all fees, royalties, remunerations, book and movies rights, etc., generated by the disclosure.
Facility Security Officer (FSO)

The NISPOM states that the government contractor shall appoint a U.S. Citizen employee, who is required to be cleared as part of the Facility Clearance (FCL), to supervise and direct security measures necessary for implementing this manual and related federal requirements for classified information. This person is called a Facility Security Officer (FSO).

Security Procedures Duties and Responsibilities

The primary duty of a PGS security officer is to observe and report as outlined in your Security Officer's Manual. Again, many of our clients have unique requirements; it is not possible to provide information for every topic area that may need to be covered. But all security regulations, regardless of differences in client facilities, are set forth in accordance with the National Industrial Security Operations Manual (NISPOM). Each client site has its own custom tailored training program that responds directly to the client's specific security needs.

Foreign Owned Control or Influence (FOCI)

Proxy Agreement

Pinkerton Government Services (PGS) was formed in 1988 to support Department of Energy contracts with both physical security and consulting and Investigative services. In 1999, PGS was reorganized and combined with the Pinkerton Aerospace Division resulting contracts for cleared services being consolidated into Pinkerton Government Services, a subsidiary of Securitas Security Services U.S.A. Inc.

The proxy agreement is an arrangement between the United States Government and Pinkerton Government Services (PGSI), which constitutes a means to effectively exclude PGS's foreign shareholder (Securitas) and any entities and affiliates the shareholder controls from unauthorized access to classified and controlled unclassified information. It also constitutes a means to prevent the shareholder (Securitas), its entities and affiliates, from exerting direct control and influence over Pinkerton Government Services' business and management in any manner that could adversely impact upon its ability to
perform on classified contracts.

There are three proxy holders or trustees to whom Pinkerton Government Services refers to as the Board of Directors. The Board of Directors exercises all prerogative of ownership of the firm with complete freedom to act independently from the foreign stockholder (Securitas). They provide guidance and oversight ensuring that Pinkerton Government Services is meeting all requirements as established in the National Industrial Security Program Operation Manual (NISPOM).

## Security Training and Briefing Requirements

Prior to a PGS security officer being allowed access to classified information, an employee shall receive an initial security briefing that includes the following:

- A threat awareness briefing.
- A defensive security briefing.
- An overview of the security classification system.
- Employee reporting obligations and requirements.
- Security procedures and duties applicable to the employee's job.

Refresher training is required to be completed and documented annually for all cleared personnel. It must reinforce the information provided during the initial security briefing and cover any changes to security regulations. PGS is also required to conduct a debriefing of all employees at the time of their termination.

## Threat Awareness Briefing

The threat to our nation's security has never been so great. The "walls" are down and the doors are open. We are not only facing the threat of espionage from our nation's enemies but from our allies as well. Espionage is as much a threat today as it has ever been.

The Encarta Encyclopedia defines Espionage in the following manner:
"Espionage, secret collection of information, or intelligence that commonly relates to governmental foreign and defense policy. Espionage, or spying, proceeds against the attempts of counterespionage (or counterintelligence) agencies to protect the secrecy of the information desired. Espionage involves the recruiting of agents in foreign nations; efforts to encourage the disloyalty of those possessing significant information; and audio surveillance, as well as the use of photographic, sensing, and detection devices."

**Threat Awareness and Defensive Security**

*The Foreign Intelligence Threat*

The gathering of information by intelligence agents, especially in wartime, is an age-old strategy for gaining superiority over enemies. Intelligence officers, those individuals working for government intelligence services, are trained to serve their country by gathering information. Spies, on the other hand, betray their country by espionage. Preventing this kind of betrayal is the ultimate goal of the entire U.S. personnel security system.

While espionage has existed since countries began to battle, it was the events of the last few generations—the era of the Cold War—that concern us. During that period we had only one monolithic enemy, the Soviet Union. Our knowledge of Soviet Cold War espionage began with the defection of Igor Sergeievitch Gouzenko, a cipher clerk in the Soviet Embassy in Ottawa. In September 1945, he defected to Canada with documents that eventually led to the arrest of Klaus Fuchs and, from there, to the apprehension of the Rosenberg's and their accomplices. A series of arrests and trials in the early 1950s helped set the climate for an anti-Communist campaign to root out all Communist sympathizers in government and nongovernmental areas alike. Since then, motivations for espionage have changed dramatically. Ideology was supplanted by financial greed and by such other motives as disgruntlement, revenge, wanting to please others, wanting to spy simply for the thrill, or a combination of all these things.

Nobody knows exactly how many spy incidents have occurred since World War II because so many have been kept secret or have never even been prosecuted. But from research done at the Defense Personnel Security Research Center (PERSEREC) we know that at least 130 cases have been
documented in the open literature. This classical form of espionage—the passing of classified information—still continues although since the end of the Cold War the recipients have changed. In a recent informal PERSEREC study of espionage cases since 1991 (found in open sources) six cases were "old" Cold War cases where the Soviet Union or Russia was the recipient, but the remaining nine involved spies who worked for a variety of countries, some of which were U.S. allies.

**The New Threat**

Classical espionage cases still occur, but now we are seeing a bourgeoning of a different kind of spying, an espionage based not just on the theft of classified information, but on theft of high-technology information, classified or not. This economic espionage is not a new phenomenon. It is just that in recent years its frequency has increased greatly. Estimates of current yearly U.S. loss of proprietary business information now range between $20 billion and $100 billion. This loss, and the loss of other technological information is especially detrimental to our economic vitality and may, by extension, have deleterious effects on U.S. security interests, since economic and national security are so closely linked in our highly competitive new world.

By now everyone understands that the end of the Cold War brought massive changes in the global economic structure. An intensified struggle for international economic power has taken the place of military superiority. Currently a host of foreign governments and individuals—present adversaries, former foes and traditional friends—are expending considerable resources in attempting to acquire our technological know-how through economic espionage. Economic espionage is the acquisition by foreign governments or corporations of U.S. high-technology information in order to enhance their countries' economic competitiveness. (Please note that this discussion is limited to espionage conducted by foreign governments against the U.S. Government or U.S. companies, defense-related or otherwise. We are not discussing inter corporate or industrial espionage within the U.S.—American companies spying against each other—although sometimes the methods used are similar.)
The FBI believes that nearly 100 countries are now running economic espionage operations against the U.S. Targets are shifting away from the classified military information sought in the old Cold War days toward basic research and development processes. But they also include the technology and trade secrets of U.S. high-tech companies--everything from cost analyses, marketing plans, contract bids and proprietary software to the high-tech data itself. Any information or process--whether classified, unclassified or proprietary--that leads to cutting-edge technology is plainly in demand. Some products are bought (or stolen) in this country and then physically smuggled abroad. Often the technology is not a physical product; it may be a plan, formula or idea that can be transported on computer or fax machine, or simply carried away inside scientists' heads.

As we have said, the economic espionage threat is not confined to America's traditional adversaries. Allies can be just as interested in U.S. technological know-how as our traditional foes from the Cold War. Countries are aggressively targeting American firms at home and abroad for industrial secrets that are critical to U.S. economic security. American corporations are now facing several foreign competitors who, backed by their intelligence services, are trying to steal trade secrets and technical data on a massive scale.

What kind of people are these new spies? How do they present themselves? They may be informal representatives of their countries or people paid by their countries to spy. They may be visiting the U.S. on scientific exchanges or business tours, or with on-site inspection teams. They may be trade representatives or liaison officers at their embassies here. Some may be foreign moles placed in American companies by their country's government, or students doing research in the U.S. who serve as informal conduits to their home governments. They may be foreign business people who can manipulate long-distance the communications systems of U.S. high-tech companies. Or they may be our very own Americans, disgruntled or greedy employees of U.S. companies who, having volunteered or been recruited, are willing to sell classified, proprietary or high-tech information to other countries. (Fifty percent of attempts to misappropriate proprietary information involve U.S. employees or ex-employees.) Whoever they are, foreign or homegrown; they are generally well educated and technologically sophisticated, and certainly
well able to navigate in high-tech waters.

Many U.S. high-tech industries have been targeted but, according to a recent government report, the following areas are the most vulnerable: biotechnology, aerospace, telecommunications, computer software and hardware, advanced transportation and engine technology, advanced materials and coatings including stealth technologies, energy research, defense and armaments technology, manufacturing processes, and semiconductors. Not yet classified proprietary business information is aggressively targeted. The industries listed above are of strategic interest to the U.S. because they contribute so greatly to leading edge, critical technologies. Clearly, this list does not cover every high-tech area that is being targeted, but it provides a sense of some of the areas that are vulnerable.

The Methods of Espionage

Economic espionage is often conducted by using basic business intelligence-gathering methods. The Internet and dozens of commercial databases are widely available, along with such sources as trade journals and company newsletters and annual reports. So much technical information is available in the U.S. in open sources that it hardly would seem necessary to resort to illegal means; in effect, much of science and technology in this country is here for the taking. There are vast repositories of technical information with the National Technical Information Service (NTIS) and the Defense Technical Information Center (DTIC). Foreigners can make direct requests to the Department of Defense and, of course, a great deal of information is published in academic and technical journals and in newspapers and trade publications, available to anyone.

It is when we get into the gray areas involving such activities as extracting information from executives of competing companies under the guise of job interviews, or hiring away an employee from a competitor just to acquire that person's knowledge that employees need to be alert.
In a world becoming more and more interconnected, systems for exchanging information are clearly necessary in order for research and commerce to thrive. The U.S. invites foreign scientists to its research institutes and laboratories in programs designed to enhance knowledge through the cross-fertilization of ideas. As we enter into exchange agreements with other countries to foster research and development, provide security or technical assistance, and so forth. Less economically developed countries--both allies and foes--do take advantage of the openness of our system. Some caution and awareness are suggested in order to prevent too much information from being disclosed.

A major means for foreign governments to obtain information is by sending their representatives to the U.S. on fact-finding visits or for training. Participants in scientific meetings, trade delegations and trade shows can easily assimilate useful information during their stays here. Other arrangements such as visitor programs, cultural exchanges and military exchanges are also utilized. One fruitful method is sending students and scholars to U.S. universities, or to government research laboratories where they are trained and also participate in research as guests of the U.S. Government. High-tech data, acquired by scientists participating in such programs, is easily transferred back to home countries, through fax, telephone, and the written word, or by memory.

Foreign governments or their representatives often attempt to acquire high-tech information by establishing joint venture companies with Americans. This allows them direct access to U.S. know-how not always available in the public domain, especially if the companies conduct classified work. Other standard business practices in this general category include mergers, strategic alliances, licensing agreements, and corporate technology agreements. It must be noted, however, that the U.S often encourages joint ventures. For example, the Bureau of Export Administration in the U.S. Department of Commerce has programs to encourage such ventures with the newly independent states of the former Soviet Union, as a way to expand U.S. trade in those areas.
Another way of acquiring high-tech information is to purchase U.S. high-tech companies, preferably those with government contracts, or for foreigners to set up their own companies in the U.S. to collect information on certain technologies and to train their own personnel. Related to establishing companies in the U.S. is the commonly used device of creating front companies. These are companies set up to undertake "legitimate" business, but used by the foreign government to further its own economic espionage purposes.

Often foreigners acquire proprietary information under the guise of market research, sending surveys from abroad to ferret out product information. Even personal telephone calls, letters and fax inquiries from abroad can elicit useful information. Callers may pretend to be someone other than who they are; in the parlance of the business intelligence fraternity this is known as pretext calling.

Some economic espionage cases resemble typical old-style espionage operations conducted with the full panoply of tradecraft. Indeed, the very words used to describe the roles of participants in an economic espionage crime are borrowed directly from the classic espionage lexicon: spies, moles, recruiters, defectors.

The "best" way to acquire information from an organization or company is--in classic spy style--to recruit a mole on the inside or to send one of your own people in on a ruse, posing as someone else. Another method is to blackmail vulnerable employees of U.S. companies or to recruit foreign nationals working in U.S. subsidiaries abroad. Not all spies have been recruited. Some, perhaps disgruntled or troubled employees, past or present, of U.S. companies, have stolen materials and then sold them to foreign companies--the volunteer of classic espionage.

Equally as unscrupulous, and also patently illegal, is the outright bribing of employees to steal plans, reports and other proprietary documents, or hiring so-called consultants to spy on competitors, a practice that can include bugging competitors' offices. Other methods include theft and smuggling of goods, theft of intellectual property, tampering with companies' electronics,
and bribery.

**The Damage**

At the industry and company level, the compromise of industrial technology often translates into lost contracts, loss of trade secrets and loss of technology—in the billions—and in the loss of technological edge over our competitors. In this age of shrinking budgets and tighter control over expenses, economic espionage can be very profitable; the less money a company has to spend on research, the greater its profit margin.

**The Old Threat Still Lingers**

All this discussion of economic espionage does not mean, as we pointed out earlier, that traditional, classical espionage has ceased. It only means that espionage has shifted to some degree—away from stealing classified information to a new interest in acquiring high-tech information that might be advantageous to a foreign country. We continue to have our classical spy cases, the most famous case, of course, being Aldrich Ames, a veteran CIA intelligence officer, who volunteered highly secret and sensitive CIA information to Soviet and Russian intelligence from 1985 to 1994. It is known that at least 11 agents lost their lives and that Ames gave the KGB tens of thousand of classified documents, in what will surely be the spy case of the century. Robert Hanssen an agent for the FBI for 27 years, was charged on 20 February 2001 with spying for Russia for more than 15 years. He was arrested in a park near his home in Vienna, Virginia, as he dropped off a bag containing seven Secret documents at a covert location. For most of his FBI career Hanssen had worked in counterintelligence, and he made use of what he learned in his own espionage career. He was charged with espionage and conspiracy to commit espionage. Specifically, Hanssen provided first the Soviets and then the Russian government over 6,000 pages of classified documents and the identities of three Russian agents working for the United States. There have been several other cases recently, involving individuals who were caught before they could do any real harm. For example, Brian Regan, a former Air Force intelligence analyst, was arrested on 3 August 2001 at Dulles International Airport as he was boarding a flight for Switzerland. On his person he was carrying missile site information on Iraq and contact information for embassies in Switzerland. Regan, who had
enlisted in the Air Force at 17, began working for the National Reconnaissance Office in 1995 where he administered the Intelink, a classified Web network for the intelligence community. Following his retirement from the military as a Master Sergeant in 2001, he was employed by defense contractor TRW and resumed work at NRO where he was employed at the time of his arrest. Regan had held a Top Secret clearance since 1980. Computers searched in Regan’s home led to the discovery of letters offering to sell secrets to Libya, Iraq, and China. In the Iraq case, he asked Saddam Hussein for $13 million. Another case in 2004, Ryan Anderson, 26, a Specialist and tank crewman in the Washington National Guard, was arrested and charged with five counts of attempting to provide aid and information to the enemy, Al Qaeda, including sketches of M1A1 and M1A2 tanks, a computer disk with identifying information and photo, and information about Army weapons systems, including “the exact caliber of round needed to penetrate the windshield and kill the driver of an up-armored Humvee.”

Losses caused by theft of U.S. military secrets can be massive. In times of crisis such losses can weaken and even destroy the country's national defense. By alerting enemies of our military plans and new weaponry, often the damage that results from the compromise of military secrets is impossible to repair. The information supplied to the Russians by John Walker, for example, enabled them to gain access to our weapons and sensory data, naval tactics, submarine and airborne training, military operations, and intelligence activities. In short, it permitted the Russians to measure the true capability and vulnerability of the U.S. Navy and to dramatically improve their own military positions.

**Indicators of Espionage**

Studies of traditional espionage cases have revealed a pattern of warning signs displayed by several of the spies in varying degrees. The most common indicators of an individual's espionage activity or potential vulnerability to espionage are mentioned below and should be a matter of concern to security and supervisory personnel.
Signs that an individual might be involved in espionage include attempts to gain access to classified information without a valid need-to-know or without the required security clearance. Other indicators might be unauthorized reproduction or removal of classified material from the work area and secret destruction of documents. Unexplained affluence can be a possible tip-off to ongoing espionage if a legitimate source of increase income cannot be found. Sudden prosperity might be of particular concern when it follows a period of financial difficulties.

Foreign travel, on a regular basis and without sufficient explanation, might be another sign of espionage when individuals with access to classified information are involved. Job and career dissatisfaction or deep grudges against the company or the U.S. Government have also figured as predisposing elements in some cases.

**Facing the Challenge**

In summary, espionage against the U.S., both economic and classical, continues to occur, and the threat it poses to U.S. national security and economic well-being is immense. Increasingly, economic espionage efforts directed against the U.S. come, not only from present foes but from friends and allies, all in search of U.S. high-tech and commercial secrets. With billions of dollars invested in research and development, the U.S. is a tempting target for friendly nations, former foes, and traditional adversaries alike. The current challenge for security professionals is to make employees understand that, despite the vast political changes around the globe, foreign intelligence activities really do continue to be directed against the U.S. Many people believe that there is no longer an espionage danger. Many believe, for example, that it is no longer necessary to restrict the flow of scientific and technical information to our highly industrialized allies or to newly emerging democracies. However, experience has shown that the U.S. often gives away far more than it gets and that scientific "exchange" is more likely than not to be a one-way street. The cheapest way to gain access to economic and scientific information is to take what is freely given (by the U.S.), or to steal it. Employees of the U.S. Government and U.S. industry must be aware of this still-present danger and be able to recognize all warning signals.
Moreover, they must understand their responsibilities to report any suspicions they may have of workmates or visitors so that the appropriate authorities can investigate the situation.

**Defensive Security Briefing**

Anyone with direct knowledge of classified or access to classified information is a potential target for a foreign intelligence agency. Due to the nature of your job you may exposed to classified information. That makes you a target for espionage.

The best defense against foreign intelligence information collection is to be aware of the signs and report any indicator immediately. Foreign intelligence agencies typically target personnel who fall into the following areas:

- Financial difficulties
- Disloyalty to the United States
- Drug Addiction
- Heavy Gambling Habits
- Immoral Behavior

Potential Sign of Foreign Intelligence Recruitment:

- Unexplained or frequent absences from work
- Emotional instability or irrational behavior
- Excessive use of alcohol
- Use of illegal drugs or marijuana
- Sudden unexplained wealth
- Lack of honesty, integrity, or discretion, which could subject an individual to blackmail or bribery
- Obvious violations of security procedures, including attempts to gain information beyond an individual's need-to-know requirement
Contact with foreign nationals

Unreported travel to foreign countries

Unusual, unexplained return to, or presence in, program areas before or after duty hours.

**Overview of the Security Classification System**

Classified Materials may be any type of information, hardware, equipment, raw data, computer media, memos, letters, drawings, production procedures, pictures, technical information, etc., which the Government has designated to be protected in the interest of national security.

**General Definitions:**

**Top Secret**- Information or material which, if disclosed to unauthorized persons will cause "Extremely Grave Damage" to the security of the United States.

**Secret**- Information or material which, if disclosed to unauthorized persons will cause "Serious Damage" to the security of the United States.

**Confidential**- Information or material which, if disclosed to unauthorized persons will cause "Damage" to the security of the United States.

**How will I know if it is classified?**

Classified information must be marked as such. "Physically marking classified information with appropriate classification marks serve to warn and inform holders of the degree of protection required to protect it…" This will be conspicuously marked on the outside front cover (coversheet), on the title page, on the first page and on the outside back cover of the document. Further, markings will be placed on the top and bottom of each page of the document. Documents are marked to highest level of classified information that it contains.
What if classified information appears on the news or other public media?

According to the NISPOM, "The fact that classified information has been made public does not mean that it is automatically declassified." Classified information must still be protected until the government makes an official change in classification. This will be of a formal nature and will be in writing. In either case, you are not authorized to release any information to the public or unauthorized persons. This includes friends and family members. Remember, "Need to Know". Access to classified information is granted only when the person has a clearance level equal to or higher than the classified material and has a specific need to know in association with their job. We do not make the determination for access to classified information.

■ Reporting Obligations and Requirements

What should I report? And to whom?

Changes in Personal Status

You must report any changes in your personal status such as marriage, divorce, name change, citizenship change, or change in residence to the Security Department (Security Processing and Records) as soon as they occur.

Business-Related Visits

Special procedures apply when conducting business-related visits to government and user agency offices as well as subcontractors, vendors, and suppliers. Security procedures are established to comply with the requirements of individual contracts. Contact your responsible program security office for specific instructions prior to conducting these visits.

Attendance at Conventions, Trade Shows, Symposiums

If you plan to attend a convention, trade show, or symposium where there will be an exchange of technical information, you must coordinate your attendance with the program security office.
Suspicious Contacts

You must report to the FSO anyone who expresses an abnormal amount of interest in your job, project, or a special access program.

Loss, Compromise or Suspected Compromise of Classified Information

You must report any actual or suspected loss or compromise of classified information to the security department as soon as possible.

Security Risks

Adverse information (any information that adversely reflects on the integrity or character of a cleared individual) has been identified as a potential security risk that could be detrimental to our national security. You are responsible to notify the FSO if you notice any employee displaying any of the following indicators:

- Financial difficulties
- Unexplained or frequent absences from work
- Emotional instability or irrational behavior
- Disloyalty to the United States
- Excessive use of alcohol
- Use of illegal drugs or marijuana
- Sudden unexplained wealth
- Lack of honesty, integrity, or discretion, which could subject an individual to blackmail or bribery
- Obvious violations of security procedures, including attempts to gain information beyond an individual's need-to-know requirement
- Contact with foreign nationals
- Unreported travel to foreign countries
- Unusual, unexplained return to, or presence in, program areas before or after duty hours.
All reports will be treated with the greatest confidentiality. The Facility Security Officer (FSO) and his assistants have been appointed to assist you; they are knowledgeable about security requirements. If you have any security questions, contact your FSO. Your questions will be answered.

Your primary duty is to observe and report as outlined in your Security Officer's Handbook. Again, many of our clients have unique requirements; it is not possible to provide information for every topic area that may need to be covered. Each client has his or her own set of security regulations. But all security regulations, regardless of differences in client facilities, are set forth in accordance with the National Industrial Security Operations Manual (NISPOM). Each client site has its own custom tailored training program that responds directly to the client's specific security needs. As part of your training, all of your duties and responsibilities will be thoroughly explained at the client's site.
Congratulations on completing the First Star book!

When you are ready to take the First Star exam please contact your PGS Introduction facilitator.