142 W. 62nd Street
Chicago, IL 60621
www.2WSecurity.com

20-HOURS
UNARMED SECURITY GUARD
TRAINING COURSE

Everything You Need To Know To Become A Qualifed Security Guard

Security Officer Unarmed 20 Hours Training Course

Day 3	Location: Classroom	4 hours

- Report Writing (DVD/Quiz/Sample Report)
- Interview Techniques (Lecture/Quiz)
- Patrol II (Video/Quiz)
- Terrorist Patrol (Video/Quiz)
- Control Systems Security Program (Lecture/Quiz)

4 hours

- Fire Prevention, Fire Equipment, and Fire Safety
- Employment in the Security Industry
- PERC application
- Fingerprint/Background Check
- Photo
- 20 Hour Certificate

REPORT WRITING

General Concept;

A report is an official document and is discoverable for the defense. The information contained in a report becomes a permanent record of an event or situation. A report has a direct reflection on the officer's professionalism and job skills. The report needs to contain the required elements of information such as; Who, What, When, Where, How, and Why.

1. Administrative

(a). Planning

(b). Directing

(c). Organizing-Specific facility problems

2. Legal Function

(a). For review by the courts

(b). Years down the road

Important future information, relevant details, protect against future lawsuits and report writing skills may lead to recognition/ promotion.

Rules of Good Report Writing

1. Good Note Taking Skills

a. Critical information

b. Relevant notes

c. No need to write complete sentences

d. Facts rather than conclusion

e. Brief statement of participants

(Time, Date, Names; ID's Locations, Descriptions)

2. The Five W's

a. Who

b. What

c. When

d. Where

e. Why

f. How

Be objective; include only facts, no opinions

3. Organize

Organize reports using the following guidelines:

- Chronological
- Location
- Cause & Effect, Routine Procedure
- Facilities

Content of Good Reports

1. Clear- Simple and direct, state objective

2. Relevant- Only info related to incident

3. Brief- Relative and short to be useful- avoid repetition

4. Complete- Cover the subject-all facts bearing to case

5. Current- Date and Time in addition to date and time of incident

6. Accurate- No errors, investigate as necessary

7. Fair- All facts, fairness using facts no speculation

8. Informative- Few or no questions left

9. Objective- Legal aspects may be read in court

10. Proper Form- Use correct form of facility

11. On Time- submit timely

Additional Information

a. Work from notes

b. Check spelling and punctuation

MILITARY 10-Series Code Signals

Following is a list of standard 10-series code signals that are used in radio communication to describe certain conditions or circumstances in a clear and succinct manner. Like most such series, this one has been adapted from the method used by the US Army Security Agency. The listing that have been left blank may be used as required by the particular security mission. If security operations approve, the standard 10-series may be replaced by a different system, as required.

Call	**Description**
10-4	Acknowledge/Understand
10-7	This unit out of service/off duty
10-8	This unit in service/on duty
10-9	Repeat last transmission
10-10	Fight in progress at this location
10-12	All units stand by
10-13	Officer requires immediate assistance
10-15	Disturbance in progress at this location
10-20	Identify location or position
10-21	Unit/officer telephone or land-line number
10-22	Disregard previous transmission
10-23	Unit/Officer on scene/in position
10-24	Assignment complete
10-28	Identify vehicle by scene license plate number
Call	**Description**
10-30	Riot in progress at this location
10-32	Subject with weapon at this location
10-33	Emergency
10-37	Suspicious activity/vehicle
10-41	Start patrol
10-42	End patrol
10-46	Stranded vehicle at this location
10-50	Vehicular accident at this location
10-51	Wrecker required at this location
10-55	Intoxicated motorist at this location
10-56	Intoxicated individual at this location
10-60	Unit/Officer in general vicinity
Call	**Description**
10-70	Fire/explosion

10-77	Estimated time of arrival. (ETA)
10-78	Estimated time of departure (ETD)
10-79	Coroner required at this location
10-80	Bomb/explosion threat
10 - 100	Launch strike/assault force

Military Date

In the military system, a date is expressed in this sequence: day month year. For example; the date January 1, 1999 is written as 01 JAN 99.

Military Time

The US military uses a 24-hour system of expressing time, as shown below. The civilian equivalents are given in the second column.

Military Time	**Civilian Equivalents**
2400 hours	12:00 midnight
0100 hours	1:00 AM
0200 hours	2:00AM
0300 hours	3:00 AM
0400 hours	4:00 AM
0500 hours	5:00 AM
0600 hours	6:00 AM
0700 hours	7:00AM
0800 hours	8:00AM
0900 hours	9:00AM
1000 hours	10:00AM
1100 hours	11:00 AM
1200 hours	12:00 noon
1300 hours	1:00 PM

1400 hours	2:00PM
1500 hours 1600 hours	3:00 PM 4:00PM
1700 hours	5:00PM
1800 hours	6:00PM
1900 hours	7:00PM
2000 hours	8:00PM
2100 hours	9:00PM
2200 hours	10:00PM
2300 hours	11:00PM

PHONETIC ALPHABET

Letter	ITU Phonetic Alphabet	Common US Law Enforcement	Letter	ITU Phonetic Alphabet	Common US Law Enforcement
A	Alfa	Adam	**N**	November	Nora
B	Bravo	Boy	**O**	Oscar	Ocean
C	Charlie	Charlie	**P**	Papa	Paul
D	Delta	David	**Q**	Quebec	Queen
E	Echo	Edward	**R**	Romeo	Robert
F	Foxtrot	Frank	**S**	Sierra	Sam
G	Golf	George	**T**	Tango	Tom
H	Hotel	Henry	**U**	Uniform	Union
I	India	Ida	**V**	Victor	Victor
J	Juliett	John	**W**	Whiskey	William
K	Kilo	King	**X**	X-Ray	X-Ray
L	Lima	Lincoln	**Y**	Yankee	Young
M	Mike	Mary	**Z**	Zulu	Zebra

INTERVIEW TECHNIQUES;

Four Basic Types of interviews

1. Victim
2. Witness
3. Informants
4. Suspects

6 Interview Objectives

1. Obtain information on who is involved
2. Obtain information on what occurred
3. Obtain information on when did it occur
4. Obtain information on how did it occur
5. Obtain information on what occurred
6. Obtain information on why did it occur

1. INTERVIEWING VICTIMS
   - Victims may be very emotional and may have suffered an emotional, physical or economic loss. Officers' need to control the interview in a calm and professional manner.
   - The victims need to provide information in their own words.
   - The victims may withhold information based on being embarrassed appear to make them look incompetent.
   - They may over exaggerate their loss or injury. This makes their case or situation look more dramatic.
   - Verify information from victim independent sources if possible.
   - Victims who are emotionally unable to respond to an interview can be assisted by having a friend, relative or co-worker help them calm down. There are known people to the victim and have a much better chance of assisting the victim gain their composure.

2. INTERVIEWING WITNESSES

- Determine if witness is related or friends with any involved parties.
- A relationship with any party can result in bias information of support for one party over the other.

- Interview witnesses as soon as possible to obtain fresh information and hopefully before witness can be influenced by involved parties.
- Some witnesses may not want to become involved based on having to testify in court or being subject to some form of retaliation.

3. INTERVIEWING INFORMANTS

- Informants are usually the least resistive persons with information as they usually come forward and identify themselves.
- Informants can provide information that is biased or prejudiced and verification of information is very important.
- One factor to consider is the motive why an informant provides inf01mation. Often it is for reward, praise, dislike of the suspect or just being a good citizen.
- Informant's information an often be considered "hearsay" and possible "rumors" and should be verified as to the validity or actual truth before proceeding on this information.

4. INTERVIEWING SUSPECTS

- Suspect interviews offer the greatest challenge for the security officer. Suspects can range from uncooperative to totally cooperative with many increments in between.
- Interviews of suspects require the utmost control by the officer to avoid the suspect taking control of the interview or providing w011hless information not relevant to the questions being asked.
- Avoid questions with an open answer. These questions usually have the words, " is it possible", "What do you think", or "Could it be that". These questions are not specific and anything is possible.
- Ask questions that are specific and direct. These questions require a YES or NO answer.
- Suspects are the last to be interviewed as the officer needs to know as much about the case prior to talking with the suspect. Information can help overcome a suspect's answer to a question the officer already knows to be true.
- If possible, record the interview for accuracy as this will prevent the suspect from changing information at a later date.
- Make no deals with the suspect as this can be used against the officer by the suspect claiming he provided information based on an agreement not based on the truth.

INTERVIEW CONSIDERATIONS;

a) The interview location must be private and free from distractions.
b) Information developed must be kept confidential with dissemination only those that have a need to know.

c) The interviewer must at all times conduct themselves in a professional manner.
d) The interviewer must treat all people with dignity and respect regardless of their relationship to the case at hand.
e) If possible, record the interviews. This requires the recording device to be already in the interview room so as not to create a surprise to the person being interviewed.
f) Keep the number of persons conducting the interview to the very minimum. One or two interviewers at the most.
g) Attempt to schedule interviews at the convenience of the person being interviewed. This is appreciated buy them and can have some positive effects on their cooperation.

PATROL II (VIDEO/QUIZ)

TERRORIST PATROL (REVIEW)

CONTROL SYSTEMS SECURITY PROGRAM/CSSP (QUIZ)

The Department of Homeland Security National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP) to guide a cohesive effort between government and industry to improve the security posture of control systems within **the nation's critical infrastructure**. The CSSP assists control systems vendors and asset owners/operators in identifying security vulnerability and developing measures to strengthen their security posture and reduce risk through sound mitigation strategies.

What are the critical infrastructure sectors?

There are 18 critical infrastructure sectors and key resources;

1. Agriculture and Food
2. Banking and Finance
3. Chemical
4. Commercial Facilities
5. Critical Manufacturing
6. Dams
7. Defense Industrial Base
8. Drinking Water and Water Treatment Systems
9. Emergency Services
10. Energy
11. Government Facilities
12. Information Technology
13. National Monuments and Icons
14. Nuclear Reactors, Materials, and Waste
15. Postal and Shipping
16. Public Health and Healthcare
17. Telecommunications
18. Transportation Systems

There are 7 signals of terrorism listed below;

1. **Surveillance** - Suspicious persons recording or monitoring activities, note taking, drawing, drawing diagrams, annotating maps, use of vision enhancing devices.

2. **Elicitation** - Any one attempting to gain information about military operations, critical infrastructures, or people.

3. **Acquiring Supplies** - Purchasing or stealing explosives, weapons, ammunition, chemical equipment law enforcement equipment/identification, theft of documents or manuals, theft of military uniforms, decals, flight manuals, passes or badges.

4. **Suspicious Persons** - People who don't seem to belong in the workplace, building, neighborhood, or business establishment.

5. **Tests of Security** - Driving by the target/casing targets, moving into sensitive areas, attempts to penetrate physical security barriers in order to assess strengths and weaknesses.

6. **Dry Runs** - Mapping out routes and determining the timing of traffic lights.

7. **Deploying Assets** - Getting into position and getting supplies in place before the act.

THEATS AND CONSEQUENCES OF CYBER ATTACKS

Example: Drinking Water and Water Treatment Systems

(U) As used in this assessment, the general term "Industrial Control System" (ICS) refers to any device, system, or combination of devices and systems that process electronic signals to physically initiate, monitor, or control the functioning of mechanical equipment used to perform a physical process. ICS includes any automated control system and it hardware, software, and firmware components, including, but not limited to:

- (U) Process control systems (PCS)
- (U) Distributed control systems (DCS)
- (U) Supervisory control and data acquisition system (SCADA)
- (U) Remote terminal units (RTU)
- (U) Programmable logic controllers (PLC)
- (U) Intelligent electronic devices (IED)

Approximately 160,000 drinking water utilities produce and distribute 51 billion gallons of water each day through 2.3 million miles of pipeline.

Threats

Ultimately are People

- Cyber Threat Actors: are people who have or have had authorized access to and direct knowledge of the utility's ICS.
- Outsiders: people who are not authorized to access ICS.
- Unknown: people who could not be identified an insider or outsider based on available information.

Access Methods;

- Direct Access: requires being physically present where the ICS isinstalled and usage devices physically connected to and provided as part of the system, including wired, wireless, infrared, and radio devices such as controllers, computers, and personal electronic devices.
- Remote Access: is equipment and systems specifically designed to provide . access to the ICS from a location where direct access is not available. It is commonly used by system administrators, operators, engineers, and vendors.
- Internet Access: is connecting to the ICS from a device connected to the internet. While internet access is a form of remote access, it is distinct in that it does not use a designed system method, such as an authorized VPN or modern connection.

Types of Attack;

Attacks can be viewed as directed or undirected. Water Sectors ICSs are vulnerable to both type of attack, either of which could bring down an ICS.

- Directed: attacks that are focused on a specific target system or group, as when an attacker uses a utility's remote access line to get into an JCS.
- Undirected: are broadcast out to the network and attempt to affect anything that is connected, such as a computer virus or a program that dials blocks of telephone numbers looking for any connection.
- Precursors: are events, such as physical surveillance, equipment theft, or stated threats. The FBI judges that such events could be indicators of or help facilitate future activities, including cyber-attacks.

Consequences of Cyber Attacks

The FBI assesses, with high confidence, that a successful cyber-attack on a US Water Sector utility's industrial control systems could disrupt service, under-dose or over-dose treatment additives into the water supply, and disable equipment. The FBI also judges that the consequences of a successful cyber-attack would be similar to other physical incidents managed by Water Sector utilities in the course of normal operations.

FIRE PREVENTION, FIRE EQUIPMENT, AND FIRE SAFETY

Fire Protection

Fire is a chemical reaction that requires three elements to be present for the reaction to take place and continue. The three elements are:

- Heat, or an ignition source
- Fuel
- Oxygen

These three elements typically are referred to as the "fire triangle." Fire is the result of the reaction between the fuel and oxygen in the air. Scientists developed the concept of a fire triangle to aid in understanding of the cause of fires and how they can be prevented and extinguished. Heat, fuel and oxygen must combine in a precise way for a fire to start and continue to burn. If one element of the fire triangle is not present or removed, fire will not start or, if already burning, will extinguish.

Ignition sources can include any material, equipment or operation that emits a spark or flame-including obvious items, such as torches, as well as less obvious items, such as static electricity and grinding operations. Equipment or components that radiate heat, such as kettles, catalytic converters and mufflers, also can be ignition sources. Fuel sources include combustible materials, such as wood, paper, trash and clothing; flammable liquids, such as gasoline or solvents; and flammable gases, such as propane or natural gas.

Oxygen in the fire triangle comes from the air in the atmosphere. Air contains approximately 79 percent nitrogen and 21 percent oxygen. A hazardous atmosphere is one which is oxygen-deficient because it has less than 19.5 percent oxygen, or oxygen enriched because it has greater than 23.5 percent oxygen. Either instance is regarded as an atmosphere immediately dangerous to life and health (IDLH) for reasons unrelated to the presence of fire. Depending on the type of fuel involved, fires can occur with much lower volume of oxygen present than needed to support human respiration.

The key to preventing fires is to keep heat and ignition sources away from materials, equipment and structures that could act as fuel to complete the fire triangle.

Fire Classifications

Fires are classified as A, B, C, D or K based on the type of substance that is the fuel for the fire, as follows:

Class A - fires involving ordinary combustibles, such as paper, trash, some plastics, wood and cloth. A rule of thumb is if it leaves an ash behind, it is a Class A fire.

Class B - fires involving flammable gases or liquids, such as propane, oil and gasoline

Class C - fires involving energized electrical components

Class D - fires involving metal. A rule of thumb is if the name of the metal ends with the letters "um," it is a Class D fire. Examples of this are aluminum, magnesium, beryllium and sodium. Class D fires rarely occur in the roofing industry.

Class K - fires involving vegetable or animal cooking oils or fats; common in commercial cooking operations using deep fat fryers

Fire Extinguishers

There are different types of fire extinguishers designed to put out the different classes of fire. Selecting the appropriate fire extinguisher is an important consideration. The wrong extinguisher actually may make a fire emergency worse. For example, failing to use a Crated extinguisher on energized electrical components may endanger people by causing the extinguishing material to be electrified by the energized components that are on fire. C-rated fire extinguishers put out the fire by using a chemical that does not conduct electricity.

Class of Fire	Type of Fire	Type of Extinguisher	Extinguisher Identification	Symbol
A	Ordinary combustibles: wood, paper, rubber, fabrics, and many plastics	Water, Dry Powder, Halon		
B	Flammable Liquids and Gases: gasoline, oils, paint, lacquer, and tar	Carbon Dioxide, Dry Powder Halon		
C	Fires involving Live Electrical Equipment	Carbon Dioxide, Dry Powder Halon		
D	Combustible Metals or Combustible Metal Alloys	Special Agents		
K	Fires in Cooking Appliances that involve Combustible Cooking Media: Vegetable or Animal Oils and Fats			

Using Fire Extinguishers

When using fire extinguishers, employees should employ the "PASS" system of early-stage firefighting.

P-Pull the pin on the extinguisher

A-Aim at the base of the fire

S-Squeeze the handle

S-Sweep at the fire, moving from side to side

Employees should be instructed that if a fire cannot be extinguished using one full extinguisher, they should evacuate the site and let the fire department handle the situation.

Fire Prevention

FIRE SAFETY MEASURES

Fire can create huge destruction in the workplace. If it's not too bad, it causes minor injuries or none at all. If it's a major one, it results in serious injuries and even fatalities. In reality, it's impossible to completely get rid of fire hazards in your worksite. But that's not to say that you can't utilize fire safety measures.

FIRE PREVENTION IN YOUR WORKPLACE CONSISTS OF FOUR STEPS:

1. Implement a program that includes preparation, prevention, and recognition of fire hazards.

2. Make sure you practice proper handling of combustible and flammable material.

3. Maintain safe housekeeping practices that reduce the risk of fire danger.

4. Always keep adequate fire suppression equipment in your work area to extinguish fire before it goes out of control.

GENERAL SAFETY MEASURES

The following are general safety measures in establishing and maintaining fire protection in the workplace:

- Never pile or lay material in a way that it covers or blocks access to firefighting equipment.
- Make sure to use only approved containers for the separation and disposal of combustible refuse. Remember to always replace the lid.
- Never store flammable materials within 10 feet of a building or other structure.
- Stack and pile all materials in orderly and stable piles.
- Never let unnecessary combustible materials get accumulated in any part of your work area.
- Make a periodic clean-up of entire work site and keep grass and weeds under control.
- Regularly dispose of combustible debris and scrap from your work area.
- Use only approved containers and tanks for storage, handling, and transport of combustible and flammable liquid.

- Always perform evaluation procedures before performing operations that present fire hazards like welding.

MORE FIRE SAFETY MEASURES

Fire extinguishers are commonly used as fire suppression equipment. You may also add fire hoses to your emergency box/glass in the workplace. Here are guidelines you must follow in using fire equipment:

- First, inspect and maintain firefighting equipment regularly.
- Place an adequate number of firefighting equipment in plain view in your work areas. When appropriate, label the location of each one and make sure it is properly rated.
- Provide employees with proper training in fire prevention and protection.
- Prohibit smoking at or around work areas where fire hazards are present. Put up signs, saying NO SMOKING or OPEN FLAMES.
- Configure an alarm system that consists of both visual and audible signals (bells, sirens, whistles, blinking lights).
- Post reporting instructions and local Fire Department codes on info boards, common areas, and areas near the phone.

WHERE DO WE GO FROM HERE?

Employment Opportunities in The Field of Security