CALIFORNIA COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

Basic Course Workbook Series

Student Materials

Learning Domain 43
Terrorism Awareness
Version 3.1

Basic Course Workbook Series
Student Materials
Learning Domain 43
Terrorism Awareness
Version 3.1

Published January 2007
Revised July 2008
Correction October 2014
Revised October 2020
Revised November 2020

POST COMMISSIONERS

Joyce Dudley - Chair	District Attorney, Santa Barbara County
Rick Braziel – Vice Chair	Educator, Humboldt State University
Lai Lai Bui	Sergeant, Sacramento Police Department
Alan Barcelona	Special Agent, Department of Justice
Eve Berg	Chief, Torrance Police Department
Robert Doyle	Sheriff, Marin County
P. Lamont Ewell	Public Member
Barry Donelan	Sergeant, Oakland Police Department
John McMahon	Sheriff, San Bernardino County
Geoff Long	Public Member
James O'Rourke	Officer, California Highway Patrol
Jethroe Moore, II	Public Member
Batine Ramirez	Sergeant, Placer County Sheriff's Department
Laurie Smith	Sheriff, Santa Clara County
Michael D. Tubbs	Mayor, City of Stockton
Walter Vasquez	Chief, La Mesa Police Department
Ed Medrano Representing Xavier Becerra Attorney General Ex-Officio Member	Chief Director of Division of Law Enforcement

THE ACADEMY TRAINING MISSION

The primary mission of basic training is to prepare students mentally, morally, and physically to advance into a field training program, assume the responsibilities, and execute the duties of a peace officer in society.

FOREWORD

The California Commission on Peace Officer Standards and Training sincerely appreciates the efforts of the many curriculum consultants, academy instructors, directors and coordinators who contributed to the development of this workbook. The Commission extends its thanks to California law enforcement agency executives who offered personnel to participate in the development of these training materials.

This student workbook is part of the POST Basic Course Training System. The workbook component of this system provides a self-study document for every learning domain in the Basic Course. Each workbook is intended to be a supplement to, not a substitute for, classroom instruction. The objective of the system is to improve academy student learning and information retention and ultimately a police officer dedicated to service and committed to safety.

The content of each workbook is organized into sequenced learning modules to meet requirements as prescribed both by California law and the POST Training and Testing Specifications for the Basic Course.

It is our hope that the collective wisdom and experience of all who contributed to this workbook will help you, the student, to successfully complete the Basic Course and to enjoy a safe and rewarding career as a peace officer serving the communities of California.

MANUEL ALVAREZ, Jr.
Executive Director

LD 43: Terrorism Awareness

Table of Contents

Topic	See Page
Preface	**iii**
Introduction	iii
How to Use the Student Workbook	iv
Chapter 1: Terrorist Threats and Ideologies	**1-1**
Overview	1-1
Terrorism	1-3
Typical Terrorist Tactics, Techniques, and Procedures (TTP)	1-5
Domestic Terrorist Ideologies	1-6
Special Interest Terrorist Ideologies	1-8
International Terrorist Ideologies	1-9
Chapter Synopsis	1-12
Workbook Learning Activities	1-13
Chapter 2: Prevention/Deterrence Concepts	**2-1**
Overview	2-1
National Terrorism Advisory System	2-3
Terrorism Indicators, Tactics, Techniques, and Procedures (TTP)	2-4
Law Enforcement Prevention/Deterrence Actions	2-8
Public Safety Information Sharing Resources	2-10
Chapter Synopsis	2-11
Workbook Learning Activities	2-12

Continued on next page

Table of Contents, Continued

Topic	See Page
Chapter 3: Critical Infrastructure Protection	**3-1**
Overview	3-1
Local Critical Infrastructure Sectors	3-3
Basic Concepts of Critical Infrastructure Protection, including:	3-6
- Threats	3-6
- Vulnerabilities	3-7
Chapter Synopsis	3-9
Workbook Learning Activities	3-10
Chapter 4: Intelligence Cycle and Intelligence Resources	**4-1**
Overview	4-1
The Intelligence Cycle	4-2
Intelligence Resources	4-5
Suspicious Reporting (SAR)	4-9
Chapter Synopsis	4-10
Workbook Learning Activities	4-11
Glossary	**G-1**

Preface

Introduction

Student workbooks

The student workbooks are part of the POST Basic Course Instructional System. This system is designed to provide students with a self-study document to be used in preparation for classroom training.

Regular Basic Course training requirement

Completion of the Regular Basic Course is required, prior to exercising peace officer powers, as recognized in the California Penal Code and where the POST-required standard is the POST Regular Basic Course.

Student workbook elements

The following elements are included in each workbook:

- chapter contents, including a synopsis of key points
- supplementary material
- a glossary of terms used in this workbook

How to Use the Student Workbook

Introduction

This workbook provides an introduction to the training requirements for this Learning Domain. You may use the workbook in several ways: for initial learning, for test preparation, and for remedial training.

Workbook format

To use the workbook most effectively, follow the steps listed below.

Step	Action
1	Begin by reading the: Preface and How to Use the Workbook, which provide an overview of how the workbook fits into the POST training program and how it should be used.
2	Refer to the Chapter Synopsis section at the end of each chapter to review the key points that support the chapter objectives.
3	Begin reading the text.
4	Complete the workbook learning activities at the end of each chapter. These activities reinforce the material taught in the chapter.
5	Refer to the Glossary section for a definition of important terms. The terms appear throughout the text and are bolded and underlined (e.g., **term**).

Chapter 1

Terrorist Threats and Ideologies

Overview

Learning need

Peace officers must become familiar with what terrorist threats are; the definitions, tactics, groups, and potential targets.

Learning objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Recall the definition of terrorism	43.01.01
• Identify typical terrorist tactics, techniques, and procedures (TTP)	43.01.02
• Identify domestic terrorist ideologies	43.01.03
• Identify special interest ideologies	43.01.04
• Identify international terrorist ideologies	43.01.05

Continued on next page

Overview, Continued

In this chapter

This chapter focuses on providing a basic understanding of terrorism, their methods, tactics and groups.

Topic	See Page
Overview	1-1
Terrorism	1-3
Typical Terrorist Tactics, Techniques, and Procedures (TTP)	1-5
Domestic Terrorist Ideologies	1-6
Special Interest Terrorist Ideologies	1-8
International Terrorist Ideologies	1-9
Chapter Synopsis	1-12
Workbook Learning Activities	1-13

Terrorism

Introduction

Terrorism has touched the United States at several locations over the years. After the September 11, 2001 attacks on the United States, we no longer viewed terrorism as just a foreign problem. Terrorism took on various types of threats with the introduction of chemical, biological, radiological, nuclear, and explosive weapons, cyber attacks, armed assaults, vehicle rammings, actions by lone offenders and guerrilla warfare. The first step in preparing to respond to incidents of this kind is to understand the nature of the threat and proactively develop measures to effectively prevent terrorism.

Protecting the safety and well-being of the people it serves, is one of the highest priorities for peace officers. Therefore, prevention of terrorism must be an on-going collaborative effort among federal, state, local, tribal and territorial agencies through information-sharing partnerships.

Leadership

The peace officer will often be the first-person people look to for leadership during a terrorist attack. If the peace officer fails to display leadership or take command of the situation the officer will be the first person criticized during and after the event.

In the beginning it is the first responding officer who will be in charge and everyone will look to that officer for leadership. It is imperative peace officers conduct themselves in a calm, rational manner, make sound decisions based on experience and training. Peace officers must move about their business with self-assurance and project a high degree of confidence. Behaviors like this will cause victims and other people involved in the event to believe that sooner or later "everything will be OK."

Continued on next page

Ethics

Terrorist attacks create chaos and confusion. The peace officer's job will be to start managing the chaos and confusion. It is at this time when ethical behavior and decision making will take on a most important role. The peace officer will be called on to make life and death decisions. Peace officers carry on their shoulders the reputations of their agency, their community, and to a larger extent, the country. The September 11, 2001 attacks on the United States proved this.

Terrorism defined

There is no single, universally accepted, definition of terrorism.

United States Code Title 22, Section 2656f(d) defines terrorism as: premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents usually intended to influence an audience.

Terrorism is defined in 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).

The FBI further classifies terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorist organization (group).

Domestic Terrorism: Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.

International Terrorism*:* Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

Typical Terrorist Tactics, Techniques, and Procedures (TTP)

Introduction

Research and study of terrorist ideologies show they provide a set of beliefs that justify certain behaviors of groups or individuals and have specific tactics, techniques, and procedures (TTPs). In the upcoming segment you will become familiar with specific tactics, techniques, and procedures.

Tactics, techniques, and procedures (TTPs)

Specific terrorist tactics, techniques, and procedures include:

- a desire to further political, religious or social objectives
- target civilian population, government personnel and U. S. Armed Forces
- intent to coerce a government or its civilian population
- threats to create fear among the public
- target critical infrastructures or disrupt lines of communication
- exploit exposed vulnerabilities
- recruiting and radicalization

Domestic Terrorist Ideologies

Introduction

Domestic terrorists usually include extremists, who seek to advance ideological goals through fear and unlawful acts of force or violence.

Domestic Terrorist Ideologies

Domestic Terrorist Ideologies		
Ideologies	**TTP**	**Targets**
• Race Supremacy • Anti-government • Anti-taxation • Anti-abortion • Anti-Authority • Radical Religion	• Bombings • Arson • Homicide • Vandalism • Harassment / Frivolous lawsuits or legal actions • Poison attempts • Vehicle rammings • Active Shootings • Secondary Explosive Device • Swatting • Impersonation of First Responders • Diversion	• Federal, State and Local Governmental Agencies and their representatives (e.g., first responders) • Places of Worship • Educational Facilities • Commercial Centers (e.g. critical infrastructures) ○ Large retail shopping centers

Continued on next page

Domestic Terrorist Ideologies, Continued

Domestic Extremists Ideologies

Types of Domestic Extremists Ideologies include:

Radical Religious Extremists
Anarchist Extremists
Sovereign Citizen Extremists
Racially Motivated Violent Extremists
Militia Extremists

Note: It is legal to have hateful or extremist beliefs as long as you don't commit crimes or violence based on those beliefs.

Domestic Extremists Attacks

Examples of Domestic Extremists attacks include:

- Oklahoma City bombing
- Charleston church shooting
- Dallas police shooting
- West Memphis, Arkansas police shooting
- El Paso Walmart shooting

Special Interest Terrorist Ideologies

Introduction

Special Interest ideologies may be individuals, persons who are part of a group or organizations who pursue specific, extremist objectives through unlawful violent acts.

Special Interest Terrorist Ideologies

Special Interest Terrorist Ideologies		
Ideologies	**TTP**	**Targets**
• Animal rights • Environmental preservation • Reproductive rights	• Bombings • Arson • Sabotage • Threats/Vandalism • Homicide	• Law enforcement • Government entities • Laboratories • Animal and genetic research facilities • Healthcare facilities • New commercial development

Special Interest Extremists

Types of special interest extremists include:

- Environmental extremists
- Animal rights extremists
- Abortion extremists (includes pro-life and pro-choice)

International Terrorist Ideologies

Introduction

International terrorist ideologies usually include state sponsors of terrorism, designated foreign terrorist organizations and loosely affiliated radical homegrown violent extremists who are inspired to commit criminal acts to advance ideological goals promoted by foreign terrorist organizations or states.

International terrorism

International terrorism is usually perpetrated against the United States by individuals and/or groups. They are usually based and/or directed by individuals, foreign terrorist organizations or countries outside the United States.

International Terrorist Ideologies

International Terrorist Ideologies		
Ideologies	**TTP**	**Targets**
• State sponsors of international terrorism • Formalized terrorist groups • Loosely affiliated international radical extremists	• Bombings • Hijackings • Assassinations • Targeted violence • Active shootings • Vehicle ramming	• Symbolic targets • Mass destruction • Mass casualties • Government buildings • Military • Law enforcement • Critical infrastructures

State Sponsors

International terrorists view terrorism as a tool of foreign policy and engage in terrorism activities by fund raising, organizing, networking, and providing other support.

State sponsors include Iran, Syria, Sudan, and North Korea.

Continued on next page

International Terrorist Ideologies, Continued

Examples of Designated Foreign Terrorist Organizations

Designated foreign terrorist organizations are autonomous factions with their own infrastructure, personnel, financial arrangements, and training facilities.

- Al Shabaab
- Al- Qa'ida
- Boko Haram/ISIL-WA (West Africa)
- Hamas
- Hizballah
- ISIL- Islamic State of Iraq and the Levant / (ISIS) - Islamic State of Irag and ash-Sham

Loosely affiliated radical extremists

Those loosely affiliated radical extremists are neither surrogates of, nor strongly influenced by, any one nation. They are considered international "wild cards." They can tap into a variety of official and private resources.

These organizations include but are not limited to: Al Qaeda and ideological groups "affiliated" with Al Qaeda, such as Abu Sayyaf (ASG) and Anssar al-Islam (AAI).

Examples of International terrorist attacks in US

Examples of international terrorist attacks in the U.S. include:

- NYC World Trade Center (NY) airline attack
- The Pentagon (VA) airline attack
- Ft. Hood (TX) shooting
- San Bernardino (CA) shooting
- The Pulse (FL) nightclub shooting
- Ohio State (OH) vehicular//knife attack
- Boston (MA) Marathon bombing
- New York City (NY) vehicular attack

Continued on next page

International Terrorist Ideologies, Continued

Homegrown Violent Extremist (HVE)

An HVE is a person of any citizenship who has mostly lived in the U.S. and who engages in a terrorist activity to advance an ideology. This person is influenced or inspired by Foreign Terrorist Organizations.

Terrorist threats have evolved from large-group conspiracies toward lone-offender ("lone wolf") attacks. These individuals often radicalize online and mobilize to violence quickly. Because of this, lone offenders are challenging to identify, investigate, and disrupt

Examples of HVEs include:

- Anwar al-Awlaki (used the phrase in propaganda)
- Samir Khan (used the phrase in propaganda)
- Matthew Llaneza,
- Zale Thompson

Examples of HVE target locations:

- San Bernardino
- Pulse Night Club
- Ft. Hood

Chapter Synopsis

Learning need	Peace officers must become familiar with terrorism, including terrorism's elements, tactics, ideologies, and potential targets.
Terrorism defined [43.01.01]	Definitions of terrorism are found in USC title 22, Section 2656(d), the U.S. Department of Justice and the Federal Bureau of Investigation (FBI). Law Enforcement generally uses the definition provided by the FBI.
Terrorist tactics, techniques, and procedures [43.01.02]	Terrorists use tactics, techniques and procedures to accomplish goals, some techniques are specific to the terrorist group. Each terrorist act has some ideology attached to the act and can vary depending on the terrorist group's goals. Tactics can vary and they are generally specific to the terrorist group. International Terrorists prefer high profile bombings while some domestic groups use arson or sniper attacks.
Domestic terrorist ideologies [43.01.03]	Domestic Terrorists ideologies are defined by their political or personal views; they can include religious, anti-government and radical religious extremists.
Special Interest Terrorist ideologies [43.01.04]	Special Interest terrorist ideologies may be individuals, persons who are part of a group or organizations who pursue specific objectives through unlawful violent acts.
International terrorist ideologies [43.01.05]	International terrorist ideologies can be state sponsored or foreign terrorist organization such as Hizballah. International terrorist ideologies mostly have purely political motivations for their acts, and they use tactics that create mass destruction and large casualty counts.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided, however, by referring to the appropriate text, you should be able to prepare a response.

Learning activity

1. Identify the different definitions of terrorism provided by the workbook and analyze the differences and similarities between each one.

2. Chart out different tactics, techniques, and procedures of terrorists known to the world today to include domestic, international, and special interest ideologies

Continued on next page

Learning activity (continued)

3. Define domestic terrorism, identify current ideologies located in the United States today.

4. Define international terrorism and list known foreign terrorist organizations found around the world today

Chapter 2

Preventing/Deterring Terrorism

Overview

Learning need

Peace officers must become familiar with their role in preventing/deterring terrorism.

Learning objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Identify the National Terrorism Advisory System	43.02.01
• Recognize terrorism indicators, tactics, techniques, and procedures (TTP)	43.02.02
• Identify law enforcement prevention/deterrence actions	43.02.03
• Identify public safety information sharing resources	43.02.04

Continued on next page

Overview, Continued

In this chapter

This chapter focuses on understanding counterterrorism measures as they apply to threat levels, pre-incident indicators, prevention and public information sharing. Refer to the chart below for specific topics.

Topic	See Page
National Terrorism Advisory System	2-3
Terrorism Indicators, Tactics, Techniques, and Procedures (TTP)	2-4
Law Enforcement Prevention/Deterrence Actions	2-8
Public Safety Information Sharing Resources	2-10
Chapter Synopsis	2-11
Workbook Learning Activities	2-12

National Terrorism Advisory System

Introduction

After the terrorist attacks on September 11, 2001, the Department of Homeland Security (DHS) was created by the President of the United States. DHS communicates information about terrorist threats. Additionally, law enforcement, by necessity, adopted an expanded role and assumed new responsibilities for responding to possible terrorist attacks.

National Terrorism Advisory System (NTAS)

The Department of Homeland Security's National Terrorism Advisory System was created by Presidential Directive to provide a "comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, local, and tribal authorities and to the American people."

The NTAS consists of an advisory system that provides bulletins and alerts. Bulletins are issued in order to communicate developments or general trends regarding threats of terrorism. Alerts are issued when there is specific, credible information about a terrorist threat. Alerts are elevated or imminent.

Federal threat levels

An "elevated" alert would advise of a credible threat of terrorism against the U.S. It probably would not specify timing or targets, but it could reveal terrorist trends that intelligence officials believe should be shared in order to prevent an attack.

An "imminent" alert would be shared if it is believed the threat is credible, specific and impending in the very near term.

Terrorism Indicators, Tactics, Techniques, and Procedures (TTP)

Introduction

There are sixteen indicators/behaviors of defined criminal activity and potential terrorism nexus activity.

Terrorism indicators

The chart below shows the sixteen indicators of defined criminal and potential terrorism nexus activity. Indicators fully described in the Nationwide SAR Initiative (NSI).

Terrorism Indicators/Behaviors	
Indicators/Behaviors	**Descriptions of Activities/TTPs**
Breach/Attempted Breach	• Unauthorized personnel attempting to enter or actually entering a restricted area • Impersonation of authorized personnel
Misrepresentations	• Presenting false information of ID to misrepresent one's affiliation to conceal possible illegal activity
Theft/Loss/Diversion	• Stealing or diverting something associated with a facility (e.g. badges, ID, technology etc.)
Sabotage/Tampering/Vandalism	• Damaging, manipulating, defacing or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	• Compromising or attempting to compromise or disrupt an organization's technology infrastructure
Expressed or Implied Threat	• Communicating a spoken or written threat to commit a crime that will like result in death or bodily injury to another person or damage a secured protected facility

Continued on next page

Terrorism Indicators, Tactics, Techniques, and Procedures (TTP), Continued

Terrorism indicators (continued)

Terrorism Indicators/Behaviors	
Indicators/Behaviors	**Descriptions of Activities/TTPs**
Aviation	• Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property.
Eliciting information	• Questioning individuals or soliciting information beyond mere curiosity about a public or private event, facets of a facility, operational security, etc. that would arouse suspicion of terrorism or criminality in a reasonable person.
Testing or Probing of Security	• Deliberate interactions with, or challenges to installations, personnel, or systems that reveal physical, personnel or cybersecurity capabilities that would arouse suspicion of terrorism or criminality in a reasonable person.
Recruiting/Financing	• Providing direct financial support to operations teams and contacts, banking data, etc. that would arouse suspicion of terrorism or criminality n a reasonable person.
Photography	• Taking pictures or video of persons, facilities, installations or infrastructure in a unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include access points, checkpoints, perimeter fencing etc.

Continued on next page

Terrorism Indicators, Tactics, Techniques, and Procedures (TTP), Continued

Terrorism indicators (continued)

Terrorism Indicators/Behaviors	
Indicators/Behaviors	**Descriptions of Activities/TTPs**
Terrorist claim of responsibility	• Media statements • Direct formal notification to government • Witnesses • Extremist BLOGS and writings • Law enforcement investigation
Reduce public support of government	• Shows government cannot protect the people • Protracted loss of life undermines public support • Fear of more attacks causes public to call for policy changes • Fear causes unrest and uncertainty • Government must maintain strong appearance
Acquisition of Expertise	• Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or other tactics that would arouse suspicion of terrorism or other criminality in a reasonable person

Continued on next page

Terrorism Indicators, Tactics, Techniques, and Procedures (TTP), Continued

Terrorism indicators (continued)

Terrorism Indicators/Behaviors	
Indicators/Behaviors	**Descriptions of Activities/TTPs**
Weapons Collection/Discovery	• Collection or discovery of unusual amounts of types of weapons, including explosives, chemicals or other destructive materials that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector Specific Incident	• Actions associated with a characteristic of unique concern to specific sectors (e.g. public health sector) with regard to their personnel, facilities, systems or functions in a manner that would arouse suspicion or criminality in a reasonable person.

NOTE: Race, ethnicity, gender, national origin, religion, sexual orientation or gender identity must not be considered as factors creating suspicion. But attributes may be documented in specific suspect descriptions for identification purposes.

Law Enforcement Prevention/Deterrence Actions

Introduction

The role of peace officers in preventing/deterring terrorism is by continually changing your mindset, applying community policing techniques, and recognizing and reporting suspicious activity.

Adopting a new mindset

Terrorism is a long-term public safety issue. Terrorism is both a national and local law enforcement problem and acts of terrorism can occur in any community. Public confidence rests upon us.

Changing your patrol mindset

Since 9/11, law enforcement officers should have a thorough understanding of their role in preventing and deterring terrorist acts. The responsibility has increased to include constant vigilance in their pursuit to recognize possible terrorist activity.

Community policing

Community policing opens lines of communication and trust between peace officers and the public. Officers regularly have direct interaction with the public, which is an important-step towards the identification of suspected terrorist activity. Community policing seeks community involvement in preventing/deterring terrorism and regional threats.

Officers should continually evaluate their daily functions (e.g. contacts with people, calls for service, traffic stops) to determine if they observe any indicators of possible terrorist activity. Officers should have a heightened situational awareness.

Continued on next page

Law Enforcement Prevention/Deterrence Actions, Continued

Recognizing suspicious activity

Recognizing Suspicious Activity	
• Traffic Stops - Questionable identification - Unusual behaviors - Suspicious literature and documents - Surveillance items - Material and equipment	• Residences - Unusual number of persons in the households - Suspicious literature and documents - Lack of furniture - Uniforms - Extremist materials - Weapons and components

Reporting suspicious activity

As with all aspects of law enforcement, it is crucial that officers both document and report any possible terrorist-related activity so that information can be shared, evaluated, and analyzed.

When reporting suspicious activity, information and observations must be documented.

Information must be shared with appropriate persons or organizations to be of value and seemingly trivial information may prove to be of crucial value.

Public Safety Information Sharing Resources

Introduction

Sharing information between public agencies is a vital responsibility of a number of federal, state and local agencies.

Public information sharing

A number of federal, state and local agencies have responsibilities for information sharing of terrorism intelligence. Agencies include but are not limited to:

- Department of Homeland Security
- Federal Bureau of Investigation
- Alcohol, Tobacco, Firearms and Explosives
- California Office of Emergency Services
- U.S. Armed Forces
- State Threat Assessment System
- California State Public Safety and Emergency Service Agencies
- Federal, State, and Local Law enforcement agencies

Chapter Synopsis

Learning need	Peace officers must become familiar with their role in preventing/deterring terrorism.
National Terrorism Advisory System [43.02.01]	National Terrorism Advisory System communicates information about terrorist threats by providing information through bulletins and alerts.
Terrorism Indicators, tactics, techniques, and procedures [43.02.02]	There are a number of indicators/behaviors of defined criminal activity and potential terrorism nexus activity.
Law enforcement prevention/ deterrence methods [43.02.03]	Law enforcement must develop new and improved methods of prevention and deterrence. Those methods include, but are not limited to, adopting a new mindset and recognizing and reporting suspicious activity.
Public information sharing resources [43.02.04]	Peace officers need to be aware of governmental, public and private sources of information that are accessible to them.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity

1. List and define the types of advisories for the Department of Homeland Security's National Terrorism Threat System

2. List two of the terrorism indicators/behaviors associated with a potential terrorist threat or act and explain their significance.

Continued on next page

Activity (continued)

3. List three of the prevention/deterrence factors.

4. List three of the public agencies law enforcement personnel can share information with and get information from.

Workbook Corrections

Suggested corrections to this workbook can be made by going to the POST website at: www.post.ca.gov

Chapter 3

Critical Infrastructure Protection

Overview

Learning need

Peace officers must recognize the types and significance of critical infrastructure.

Learning objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Identify local critical infrastructure sectors	43.03.02
• Identify the basic concepts of critical infrastructure protection, including: o threats o vulnerabilities	43.03.03

Continued on next page

Overview, Continued

In this chapter

This chapter focuses on providing a basic understanding of threat and vulnerability assessment. Refer to the chart below for specific topics.

Topic	See Page
Identification of Local Critical Infrastructure Sectors	3-3
Concepts of Critical Infrastructure Protection	3-6
Chapter Synopsis	3-9
Workbook Learning Activities	3-10

Identification of Local Critical Infrastructure Sectors

Introduction

Critical infrastructure sectors are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or combination of those matters. – U.S. DHS 2013, National Infrastructure Protection Plan.

Peace officers need to be aware of critical infrastructures located in their local jurisdictions.

Critical infrastructure sectors

Critical infrastructure sectors can be dependent on one another and are identified in the National Infrastructure Protections Plan (NIPP) as the following:

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense Industrial Base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and Public Health
- Information technology
- Nuclear reactors, materials and waste
- Transportation systems
- Water and wastewater systems

Continued on next page

Identification of Local Critical Infrastructure Sectors,
Continued

Owners and Operators

The vast majority of the Nation's critical infrastructure is owned and operated by the private sector to include:

- Utility providers
- Sports stadiums
- Hospitals
- Agriculture
- Telecomm Services

Non-governmental organizations (NGO) have critical infrastructure, which includes:

- Places of Worship
- Veterans groups
- Community social and sports clubs/events
- Local Charities

Public sector critical infrastructure would include:

- Law enforcement and fire departments
- Courthouses
- Military bases
- State and Federal buildings
- Dams

State, local, regional, and territorial officials play an important role in leading or supporting their respective critical infrastructure security and resilience programs and in the overall implementation of the National Infrastructure Protection Plan (NIPP). They provide jurisdictional focus, facilitate bottom-up information sharing and collaborations for local, state, and Federal critical infrastructure protection.

Identification of Local Critical Infrastructure Sectors,
Continued

Potential targets Important infrastructure elements and high impact targets that peace officers should consider include, but are not limited to:

- High occupancy events or locations such as:
  - Theme parks
  - Stadiums
  - Tourist attractions
- Symbolic targets such as:
  - State and National landmarks
  - Historical monuments
  - Political events
- Targets of single-issue terrorists such as:
  - Abortion providers
  - Embassies, consulates, residences
  - Religious sites and facilities
- Targets of radical environmentalists such as:
  - genetic research
  - biotechnology
  - fur breeders
  - firms doing animal research
- Key assets such as:
  - Firehouses
  - Law enforcement facilities
  - Utility towers and power substations
  - Schools
  - Government buildings
  - Government agencies

Concepts of Critical Infrastructure Protection

Introduction

In the post 9/11 world, law enforcement officers have been thrust into and assumed new responsibilities with respect to critical infrastructure protection. This segment provides some information as it applies to threat and vulnerabilities to critical infrastructure.

Peace officers should discuss the need to identify vulnerabilities within our communities, identify potential targets of terrorist attacks, and describe tools (methodologies) available to conduct vulnerability assessments.

Threats to critical infrastructure

Threats are events that may damage or incapacitate an asset, system, network, or community. Threats are generally estimated as the likelihood and or occurrence the hazard will impact critical infrastructure. Threats to critical infrastructure are broken down to 3 categories include:

- Human-caused hazards (Biological, Chemical, Cyber, Explosives, Radiological, Sabotage, School & Workplace Violence)
- Natural hazards (Avalanche, Animal disease outbreak, Drought, Earthquake, Epidemic, Flood, Hurricane, Landslide, Pandemic, Tornado, Tsunami, Volcanic eruption, Wildfire, Winter storm)
- Technological hazards (Airplane crash, Dam failure, Levee failure, Mine accident, Hazardous materials, Power failure, Radiological release, Train derailment, Urban conflagration)

Terrorist target selection criteria

The probability that an individual/location will be targeted by a terrorist is a function of several factors to include:

- attractiveness of a target
- the potential for success
- the potential for avoiding identification and capture

Keep in mind that some terrorists are willing to die for their cause and will select targets regardless of the probability of their identification or capture.

Continued on next page

Concepts of Critical Infrastructure Protection, Continued

Targets

Terrorist may select their targets based on the following:

- A key element is symbolism
- The higher the profile, the better
- Depending on the group's motivations, the greater the potential for mass casualties, the better
- Potential for major economic impact

Timing

The timing of a terrorist attack is often dictated by a date significant to the terrorist.

Vulnerability assessment

Vulnerability assessments involve identifying areas of weakness whose exploitation by a threat could result in consequences of concern. Vulnerabilities may be associated with physical, cyber and human factors. For example, broken fences, access control, broken lighting, and vegetation overgrowth.

Reasons to conduct assessments

Assessments are conducted for a variety of reasons including:

- Identifying potential targets
  - Guides patrol and intelligence efforts
  - Secure identified targets
- Threat level to targets
  - Suspicious activity reports (SAR)
  - Intelligence information
- Benefits
  - Whole community resilience
  - Interagency interaction and coordination
  - Familiarity with infrastructure elements will aid if response is needed in future.
  - Vital communication links
- Essential services

Continued on next page

Risk Assessment

Vulnerabilities can be mitigated by various physical security countermeasures referenced in FEMA 452 – Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings.

Examples of mitigation include:

- Barriers for stand-off distance
- Bollards for ramming attacks
- Closed Circuit Television (CCTV)
- Restricted access
- Fencing
- Safety and security window film
- Anti-cut padlocks and chains
- Security signage
- Designated safe rooms

Chapter Synopsis

Learning need	Peace officers must recognize the types and significance of critical infrastructure.
Identification of local critical infrastructure sectors [43.03.01]	Critical infrastructure sectors are those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or combination of those matters.
Concepts of critical infrastructure protection [43.03.02]	Peace officers should gain an understanding of their role in critical infrastructure protection, identification of potential targets and threats, and the purpose of vulnerabilities assessments.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity questions

1. Discuss examples of critical infrastructures and what observed activity may be suspicious.

2. How can you mitigate vulnerabilities at a school or place of worship?

Chapter 4

Intelligence Cycle and Intelligence Resources

Overview

Learning need

Peace officers must have a basic understanding of the intelligence cycle and the intelligence resources available to them.

Learning objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Identify the intelligence cycle	43.04.01
• Identify intelligence resources	43.04.02
• Discuss Suspicious Reporting (SAR), including an introduction into the intelligence cycle	43.04.03

In this chapter

This chapter focuses on the California Intelligence System and other resources. Refer to the chart below for specific topics.

Topic	See Page
The Intelligence Cycle	4-2
Intelligence Resources	4-5
Suspicious Activity Reporting	4-8
Chapter Synopsis	4-10
Workbook Learning Activities	4-11

The Intelligence Cycle

Introduction

Peace officers in the State of California have at their disposal several intelligence resources. It is important for law enforcement to understand the intelligence cycle and intelligence resources available to report suspicious activity, criminal acts or attempted criminal acts that might have a nexus to terrorism.

Definitions

Information: Anything we know about any person, place or thing, from any source. Raw data.

Intelligence: Information that has been analyzed and vetted through the intelligence cycle.

Open Source Information: Data collected from publicly available sources.

Suspicious Activity Reports (SAR): A suspicious activity report (SAR) is used to document any observed unusual or suspicious behavior that could indicate possible terrorism or criminal related activities.

Classified Intelligence: Any intelligence that has been given a classification by an appropriate agency that is legally authorized to make such classification.

The Intelligence Cycle

The Intelligence Cycle is the process of developing raw information into finished intelligence for policymakers to use in decision making and action. There are five steps that constitute the Intelligence Cycle.

1. Planning and Direction
This is management of the entire effort, from identifying the need for data to delivering an intelligence product to a consumer. It is the beginning and the end of the cycle--the beginning because it involves drawing up specific collection requirements and the end because finished intelligence, which supports policy decisions, generates new requirements.

2. Collection
The gathering of the raw information needed to produce finished intelligence. There are many sources of information including open sources such as foreign broadcasts, newspapers, periodicals, and books. Finally, technical collection--electronics and satellite photography--plays an indispensable role in modern intelligence.

Continued on next page

The Intelligence Cycle, Continued

The Intelligence Cycle, cont.

3. Processing
Converting the vast amount of information collected to a form usable by analysts through decryption, language translations, and data reduction.

4. All Source Analysis and Production
The conversion of basic information into finished intelligence. It includes integrating, evaluating, and analyzing all available data--which is often fragmentary and even contradictory--and preparing intelligence products. Analysts, who are subject-matter specialists, consider the information's reliability, validity, and relevance. They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for the affected agencies.

5. Dissemination
The last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers, the same policymakers whose needs initiated the intelligence requirements. Finished intelligence is hand-carried daily to the President and key national security advisers. The policymakers, the recipients of finished intelligence, then make decisions based on the information, and these decisions may lead to the reevaluation and levying of more requirements, thus triggering the Intelligence Cycle.

NOTE: Dissemination of intelligence information must follow your agency's protocol and policies.

Continued on next page

The Intelligence Cycle, Continued

Diagram of the Intelligence Cycle

Intelligence Resources

Introduction

The federal government and the state of California have many resources available to peace officers to report suspicious activity and aid in the identification of potential threats.

Information resources available

Available information resources are:

- Terrorism Liaison Officer (TLO)
- State Threat Assessment Center (STAC)
- Regional Threat Assessment Centers (also referred to as Fusion Centers):

Fusion Centers

Fusion centers are components of a nationwide network of state and urban centers to contribute to the Information Sharing Environment. They serve as a collaborative effort between the federal government and state, local, tribal, territorial and private sector agencies for the receipt, analysis, gathering and sharing of threat-related information (e.g. Suspicious Activity Reports).

Fusion centers in California are:

- Northern California Regional Intelligence Center (NCRIC)
- Central California Intelligence Center (CCIC)
- Joint Regional Intelligence Center (JRIC)
- Orange County Intelligence Assessment Center (OCIAC)
- San Diego Law Enforcement Coordination Center (SD-LECC)

Terrorism Liaison Officer (TLO)

A TLO is any peace officer, firefighter, state investigator, federal agent, military investigative personnel, or anyone working closely within the public safety/homeland security community, who has been properly certified by the appropriate Regional Fusion Center.

Continued on next page

Intelligence Resources, Continued

State Threat Assessment Center (STAC)

The State Threat Assessment Center (STAC) is California's state primary fusion center, as designated by the Governor of California, and is operated by the California Highway Patrol (CHP), the California Governor's Office of Emergency Services (Cal OES), and the California Department of Justice (Cal DOJ).

The State Threat Assessment Center (STAC) serves as California's information sharing clearinghouse of strategic threat analysis and situational awareness reporting to statewide leadership and the public safety community in support of efforts to prevent, prepare for, mitigate and respond to all crimes and all hazards impacting California citizens and critical infrastructure, while preserving civil liberties, individual privacy, and constitutional rights (www.calstac.org).

The STAC and The Regional Threat Assessment Centers are components within the State Threat Assessment System (STAS) for sharing and disseminating information within the information sharing environment (ISE).

Terrorist Screening Center

The Terrorist Screen Center (TSC) is a multi-agency center administered by the Federal Bureau of Investigations (FBI). The TSC maintains the consolidated watch list of known or suspected terrorists and helps resolve encounters with individuals who may be watch listed.

Continued on next page

Intelligence Resources, Continued

Joint Terrorism Task Force (JTTF)	The FBI's Joint Terrorism Task Forces, or JTTFs, are based in cities nationwide, including at least one in each of the 56 field offices. The task forces coordinate their efforts largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs and beyond.
National Counter Terrorism Center (NCTC)	Located in Washington D.C, the NCTC serves as the primary organization in the federal government for integrating, analyzing and fusing foreign and domestic counterterrorism information. NCTC collates more than 30 intelligence, military, law enforcement and homeland security networks to facilitate robust information sharing.

Suspicious Activity Reporting (SAR)

Introduction

Suspicious Activity Reports, or SARs, are suspicious behavior is documented. This behavior could indicate possible terrorism or other related criminal activity. Peace officers should use the indicators laid out by the Nationwide SAR Initiative (NSI) to report those activities by submitting a SAR.

Nationwide SAR Initiative (NSI)

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a partnership of agencies at all levels that provide law enforcement with another tool to help prevent terrorism and other related criminal activity.

Submitting a SAR

A SAR is submitted by accessing your respective regional threat assessment center (fusion center's) website and submitting it electronically. When submitting the SAR include as many details as possible and describe the suspicious activity in detail.

Suspicious Activity Report (SAR)

A Suspicious Activity Report (SAR) contains information about a suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring. *Suspicious activity* is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity."

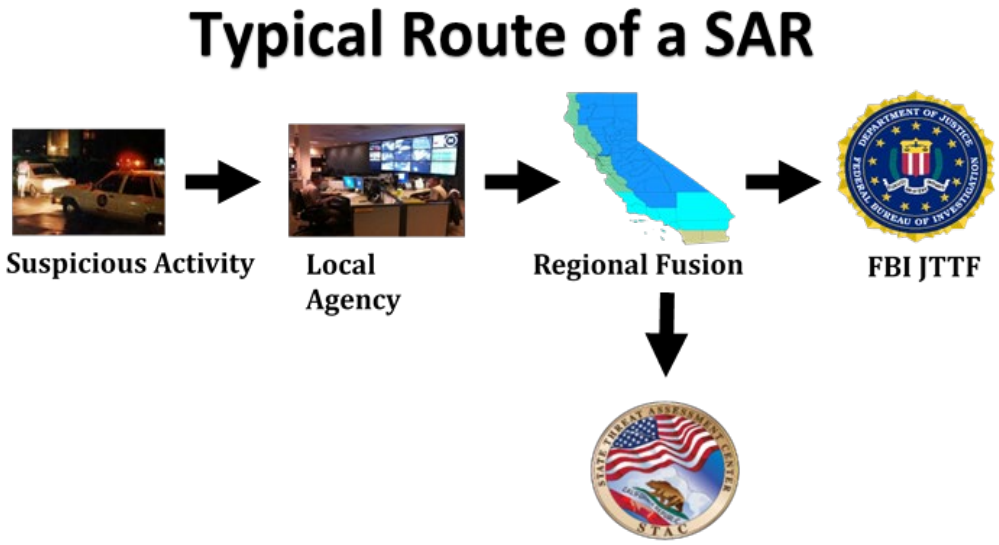
Peace officers have daily opportunities to observe, identify, and report suspicious activity:

- Minor details or incidents may prove vital in identifying and thwarting a potential terrorist attack and/or criminal activity
- Indicators/behavior that would arouse suspicion in a reasonable officer
- Does NOT have to be criminal in nature
- Anything that you can articulate as 'suspicious' based on your training and experience
- With further investigation, is behavior explained or are more questions raised?

Continued on next page

Typical Route of a SAR

The following image demonstrates the typical route of a SAR:



Report activity

Reporting suspicious activity should be directed to the appropriate regional threat assessment center (fusion center).

- SD-LECC – www.sd-lecc.org
- OCIAC – www.ociac.ca.gov
- JRIC – www.jric.org
- CCIC – www.sacrtac.org
- NCRIC – www.ncric.org

Chapter Synopsis

Learning need	Peace officers must have a basic understanding of the intelligence cycle, and the intelligence resources available to them.
Intelligence cycle [43.04.01]	The overview of the intelligence cycle – planning/direction, processing/collation, analysis, dissemination, and reevaluation and covers the definitions for information, intelligence, open source information and classified information.
Intelligence resources [43.04.02]	The federal government and the State of California have many resources available to officers to report and aid in the identification of potential terrorist activity.
Suspicious Activity Reporting [43.04.03]	A SAR is used to document any reported or observed activity or any criminal act or attempted criminal act that an officer believes may reveal a nexus to terrorism.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity questions

1. Peace officers are dispatched to an address in a working-class neighborhood. When they respond they are told by the reporting party (RP) that three males have moved in next door. The RP said the males are renting the house. The RP knows the landlord, who told the RP the males paid for their rent six months in advance with cash. The RP tells the officer the males talk to each other all of the time in Arabic and are collecting unusual quantities of unknown chemical materials. The officers asked the RP how they know it is Arabic being spoken. He tells the officer he spent three years in the Army and one year of that was spent in Saudi Arabia and he knows what the Arabic language sounds like.

2. Describe the intelligence cycle you will put this information through.

Continued on next page

Activity questions (continued)

3. List the agencies and people you think you will need to contact?

4. Do you need to submit a SAR about this information

Continued on next page

Activity questions (continued)

5. What other steps could you take to handle this information?

Workbook Corrections

Suggested corrections to this workbook can be made by going to the POST website at: www.post.ca.gov

Glossary

classified intelligence	Any intelligence that has been given a classification by an appropriate agency
information	Anything we know about any person, place or thing from any source
intelligence	Information that has gone through the intelligence cycle
National Terrorism Advisory System	The Department of Homeland Security's National Terrorism Advisory System was created by Presidential Directive to provide a "comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, local, tribal and territorial authorities and to the American people."
open source information	Publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access.
Suspicious Activity Reporting (SAR)	A suspicious activity report (SAR) is used to document any observed unusual or suspicious behavior that could indicate possible terrorism or criminal related activities.
Terrorism Liaison Officer (TLO)	A TLO is any peace officer, firefighter, state investigator, federal agent, military investigative personnel, or anyone working closely within the public safety/homeland security community, who has been properly certified by the appropriate Regional Fusion Center.
incapacitating agents	Most of these substances are lachrymators (tear producers), however, exposure can create other physical and psychological symptoms