



Anti-Terrorism Officer (ATO) Course

Seminar Description & Outline

Copyright 2004 by the S2 Safety & Intelligence Institute
S2 Safety & Intelligence Institute, 1261 South Missouri Ave, Clearwater, FL 33756
Tel. (727) 461-0066 / Fax (727) 449-1269 / WEB: <http://www.s2institute.com>

Class Details

Description: The Anti-Terrorism Officer (ATO) Program is designed to prepare frontline officers and emergency personnel for deployment in environments where terrorism is a critical threat. This program provides an exploration of contemporary terrorist methods and basic anti-terrorism skills and knowledge that all officers and emergency responders should possess.

Audience: Security Supervisors, Security Officers, Force Protection Personnel, Police Officers Assigned to Anti-Terrorism Activities

Restrictions: Verified Security, Law Enforcement, and Government Employees Only.

CEU/In-Service Training Credit: CHS-certified practitioners are eligible for 16-hours of CEUs through the American College of Forensic Examiners.

Presentation Time: The S2 Anti-Terrorism Officer classroom program is presented in two 8.5-hour days. Classes typically start at 8:30AM and finish by 5:00PM.

Class Outline

DAY ONE

1. Anti-Terrorism Officers (ATOs)
 - 1.1 ATO Functions & Responsibilities
 - 1.2 ATO Skills
2. Introduction to Terrorism
 - 2.1 Definition
 - 2.2 Ideological Motives
 - 2.3 Strategic Objectives
 - 2.4 Types of Terrorist Targets
 - 2.5 Target Selection Criteria

- 2.6 Categories of Terrorism Related Risk
 - 2.6.1 Explosive Attack
 - 2.6.2 Kidnapping
 - 2.6.3 Armed Attack
 - 2.6.3.1 Hijacking
 - 2.6.3.2 Armed Occupation
 - 2.6.3.3 Barricaded Hostage
 - 2.6.4 Arson
 - 2.6.5 Chemical/Biological/Radiological (CBR)
 - 2.6.6 Nuclear
 - 2.6.7 Cyber Attack
- 2.7 Terrorist Planning and Execution Phases

3. Threat: Explosive Attacks

- 3.1 Types of Explosive Devices
- 3.2 Characteristics of Chemical Explosions
- 3.3 High vs Low Explosives
- 3.4 Sensitivity of Explosives
- 3.5 Initiation
 - 3.5.1 Blasting Caps
 - 3.5.2 Detonating Cord
 - 3.5.3 Boosters
 - 3.5.4 The Firing Train
- 3.6 Common Explosives
 - 3.6.1 Commercial Explosives
 - 3.6.2 Military Explosives
 - 3.6.3 Improvised Explosives
 - 3.6.4 Conventional Ordnance
- 3.7 Gas Enhanced IEDs
- 3.8 Activation
 - 3.8.1 Time Delay
 - 3.8.2 Anti-Disturbance
 - 3.8.3 Environmental Change
 - 3.8.4 Command Detonation
 - 3.8.5 Unique Terrorist Modus Operandi
- 3.9 Device Concealment
- 3.10 Damage Potential
 - 3.10.1 Types of Destructive Forces
 - 3.10.2 Estimating Charge Size
 - 3.10.3 Overpressure Range Effects Estimation
- 3.11 Explosive Employment Scenarios: Land Facilities
 - 3.11.1 Hand Delivered IEDs
 - 3.11.1.1 Covert
 - 3.11.1.2 Overt
 - 3.11.1.3 Deceptive
 - 3.11.1.4 Naïve
 - 3.11.2 Vehicle Borne IEDs
 - 3.11.2.1 Covert
 - 3.11.2.2 Overt
 - 3.11.2.3 Deceptive
 - 3.11.2.4 Naïve
 - 3.11.2.5 Proxy
 - 3.11.3 Projected Charge Attacks
 - 3.11.3.1 Direct Fire
 - 3.11.3.2 Indirect Fire

- 3.12 Explosive Employment Scenarios: Piers & Watercraft
 - 3.12.1 Limpet Mine Attacks
 - 3.12.2 Submerged Proximity Charges
 - 3.12.3 Surface Vessel Borne IEDs

4. Threat: Chemical & Biological Terrorism

- 4.1 Common Assumptions About CB Terrorism
- 4.2 Why Use CB Agents?
- 4.3 CB Terrorists
- 4.4 Challenges faced By CB Terrorists
- 4.5 Requisite Characteristics of CB Agents
 - 4.5.1 Terrorist vs Military Agents
- 4.6 Routes of Exposure
- 4.7 Symptoms
- 4.8 Chemical Agents
- 4.9 Agents of Biological Origin
- 4.10 Dissemination of CB Agents
- 4.11 CB Employment Scenarios
 - 4.11.1 On-Site Facility Attacks
 - 4.11.1.1 Point Source Contamination
 - 4.11.1.2 IDD Attacks
 - 4.11.1.3 Contaminated Deliveries
 - 4.11.2 Off-Site Facility Attacks
 - 4.11.2.1 Point Source Contamination
 - 4.11.2.2 Outdoor Aerosol/Vapor Attacks
 - 4.11.2.3 Projected Charge Weapons

5. Anti-Terrorism Planning

- 5.1 Integrated Countermeasures Theory
- 5.2 Proactive Countermeasures
- 5.3 Reactive/Mitigative Countermeasures

6. Operations Security (OPSEC)

- 6.1 Terrorist Intelligence Requirements
- 6.2 Terrorist Intelligence Collection Methods
- 6.3 Complexity of Intelligence Requirements
- 6.4 Protective Counterintelligence/OPSEC
- 6.5 Information Security
- 6.6 Employee/Contractor Screening & Monitoring
 - 6.6.1 Background Flags
 - 6.6.2 HUMINT Indicators
- 6.7 Countersurveillance
 - 6.7.1 Surveillance Detection Guidelines
- 6.8 Suspicious Activity Investigation
 - 6.8.1 Suspicious Telephone Inquiries
 - 6.8.2 Possible On-Site Reconnaissance
 - 6.8.3 Possible Off-Site Surveillance
 - 6.8.4 Possible Elicitation Contacts
 - 6.8.5 Recruitment Approaches
 - 6.8.6 Theft of ID Cards, Company Vehicle Stickers, etc.
- 6.9 Suspicious Activity Reporting & Analysis

DAY TWO

7. Physical Security & Access Control

7.1 Physical Security Theory

- 7.1.1 Physical Security System Functions
- 7.1.2 Integrated Systems
- 7.1.3 Performance Definition
- 7.1.4 Common Design Flaws
- 7.1.5 System Design Guidelines

7.2 Physical Security Components

- 7.2.1 Intrusion Detection Systems
- 7.2.2 Area Surveillance
 - 7.2.1.1 CCTV
 - 7.2.1.2 Stationary Posts
 - 7.2.1.3 Mobile Patrols
 - 7.2.1.4 Intrusion Indicators
 - 7.2.1.5 Bomb Delivery indicators
- 7.2.3 Barriers
 - 7.2.3.1 Conventional Barriers
 - 7.2.3.1.1 Delay Time Calculation
 - 7.2.3.1.2 Barrier System Design
 - 7.2.3.2 Vehicle Barriers
 - 7.2.3.2.1 Kinetic Energy Calculation
 - 7.2.3.2.2 Vehicle Barrier System Design
 - 7.2.3.3 Vehicle Entry Points
 - 7.2.3.3.1 Entry Point Design
 - 7.2.3.3.2 Active Barriers

7.3 Access Control

- 7.3.1 Planning Considerations
- 7.3.2 Types of Entrants
- 7.3.3 Entrant Identification
- 7.3.4 Access Screening Technologies
 - 7.3.4.1 X-Ray Based Technologies
 - 7.3.4.2 Explosive Trace Detection
 - 7.3.4.3 Nuclear Detection Systems
 - 7.3.4.4 Explosive Detection Canines

7.4 Additional Proactive Security Issues

- 7.4.1 Limited Concealment Opportunities
- 7.4.2 Obscuration
 - 7.4.2.1 Projected Charge Weapon Dynamics
 - 7.4.2.2 Obscuration Screens
- 7.4.3 Point Source Protection
 - 7.4.3.1 Physical Security for Possible Contamination Points
 - 7.4.3.2 Cafeteria and Break Room Countermeasures
 - 7.4.3.3 Water Filtration
 - 7.4.3.4 Air Filtration

8. Mail Security

8.1 Types of Hazardous Mailings

- 8.1.1 Mail Bombs
 - 8.1.1.1 Characteristics of Letter Bombs
 - 8.1.1.2 Characteristics of Package Bombs
- 8.1.2 Contaminated Mailings
- 8.1.3 Improvised Projectile Devices

- 8.2 Mail Security Planning
 - 8.2.1 Initial Considerations
- 8.3 Physical Mail Screening
 - 8.3.1 Threat Indicators
 - 8.3.2 Case Studies
- 8.4 Technical Mail Screening
- 8.5 Response to Hazardous Mailings
 - 8.5.1 Suspect Mail Bomb Response
 - 8.5.2 Response to Contaminated Mailings

9. Response to Terrorist Incidents

- 9.1 Incident Response Scenarios
- 9.2 Response Priorities
- 9.3 Responsibilities
- 9.4 Weapons of Mass Destruction
 - 9.4.1 WMD Response Authority
- 9.5 Bomb Threat Response
 - 9.5.1 Bomb Threat Motives
 - 9.5.1.1 Malevolent Bomb Threat Strategies
 - 9.5.2 Bomb Threat Planning Considerations
 - 9.5.3 Search and Response Approaches
 - 9.5.3.1 Security Team Search
 - 9.5.3.2 Employee Work Area Search
 - 9.5.3.3 Police Directed Search
 - 9.5.4 Search Safety
 - 9.5.5 Security Team Search Walk Through
 - 9.5.5.1 Managing Bomb Threat Calls
 - 9.5.5.2 Search Procedures
 - 9.5.6 Response to Suspicious Objects
- 9.6 Suspicious Vehicle Response
 - 9.6.1 Initial Alert & Refuge
 - 9.6.2 TSWG Evacuation and Refuge Guidelines
 - 9.6.3 Refuge Procedures
 - 9.6.4 Evacuation Procedures
- 9.7 Post-Blast Response
 - 9.7.1 Types of Post-Blast Scenarios
 - 9.7.2 Localized Bombings
 - 9.7.2.1 Characteristics of Localized Bombings
 - 9.7.2.1.1 Facility Damage
 - 9.7.2.1.2 Casualties and Injury Types
 - 9.7.2.1.3 Post-Blast Hazards
 - 9.7.2.2 Localized Response Procedures
 - 9.7.3 Conventional Weapon of Mass Destruction Incidents
 - 9.7.3.1 Characteristics of CWMD Incidents
 - 9.7.3.1.1 Facility Damage
 - 9.7.3.1.2 Casualties and Injury Types
 - 9.7.3.1.3 Post-Blast Hazards
 - 9.7.3.2 CWMD Public Safety Response
 - 9.7.3.2.1 CWMD Response Scenario
 - 9.7.3.2.2 Triage
 - 9.7.3.3 CWMD Facility Response Guidelines
 - 9.7.3.3.1 Important Safety Guidelines
 - 9.7.3.4 Post-Incident Recovery Issues
- 9.8 Chemical & Biological Attack Response
 - 9.8.1 Unique Response Issues

- 9.8.2 Key Players
- 9.8.3 Responsibilities
- 9.8.4 Public Safety Response Sequence
- 9.8.5 Facility-Level Response
 - 9.8.5.1 Attack Recognition
 - 9.8.5.1.1 Chemical Attack Indicators
 - 9.8.5.1.2 Biological Attack Indicators
 - 9.8.5.2 Response to Indoor Aerosol/Vapor Attacks
 - 9.8.5.2.1 Evacuation
 - 9.8.5.2.2 Expedient Respiratory and Skin Protection
 - 9.8.5.2.3 Emergency Decontamination
 - 9.8.5.3 Response to Outdoor Aerosol/Vapor Attacks
 - 9.8.5.3.1 Shelter-In-Place Procedures
 - 9.8.5.3.2 Emergency Evacuation Procedures
 - 9.8.5.4 Response to Covert CB Attacks

About the Instructor

The primary instructor for the S2 Anti-Terrorism Officer seminar is Craig S. Gundry.

Craig S. Gundry, CPS, ATO, CHS-III

Craig Gundry, the Vice President of Special Projects for Critical Intervention Services (CIS), is the primary instructor for S2's Anti-Terrorism courses. Mr. Gundry is responsible for directing CIS consulting and training projects pertaining to terrorism and security, including the development of doctrine and training for the CIS Anti-Terrorism Officer Division. Prior to joining CIS, Mr. Gundry was the President of Palladium Media Group, a company specializing in training and consulting on explosive, chemical, and biological terrorism. Mr. Gundry's expertise in anti-terrorism began as a specialist in force protection with the United States Army.

Mr. Gundry is the author of the acclaimed Bomb Countermeasures for Security Professionals CD-ROM and a new book on assessing terrorism-related risk. Mr. Gundry is also a frequent consultant to the news media on issues relating to terrorism and weapons of mass destruction.

As an instructor, Mr. Gundry has been training security, police, and emergency responders in terrorism-related issues for over 10 years. His previous students have included security professionals, facility managers, military personnel, police officers, and federal officials.

Student Comments

Following are some recent statements from students who have attended the S2 Anti-Terrorism Officer course.

"I personally give thanks to S2 and CIS for the opportunity to attend the Anti-Terrorism Officer (ATO) training sessions. In all of my travels and training, military and civilian, I rarely have the pleasure of encountering such professional instructors and presentations. The knowledge possessed and demonstrated by the instructor staff sets the bar for all civilian training agencies to

follow...The training you are providing to security personnel, military personnel and law enforcement professionals, is unmatched by civilian readiness training for the war on terror.”

J. White
Advanced Training Section, U.S. Special Operations Command

“The instructor knew all the subjects like the back of his hand...A+++!”

SMSgt G. Enwright
Office of the Secretary of the Air Force, USAF

“Met and exceeded all of my expectations...no shortcuts during the delivery of the lectures. The instructor should be the standard by which all instructors should be judged.”

L. McMillan
Embassy of Trinidad & Tobago

Hosting a Program

As an alternative to attending a scheduled Anti-Terrorism Officer course at the S2 training facility in Clearwater, organizations that would like to train their staff internally may host a seminar at their facility.

Prices and Fees

The price for presenting the two-day classroom version of the S2 Anti-Terrorism Officer program is \$3,400.00. This price includes all instructor classroom time and travel time within the domestic United States. If the host facility is located outside of the United States, there may be additional charges for travel time. If the host organization would like to add a third day of hands-on search and screening training, the additional day is charged at a rate of \$1,500.00.

The host will be charged for all instructor transportation and lodging expenses, including airfare, rental car or taxi fees, and hotel expenses. The host may coordinate travel and lodging directly or may leave travel coordination to the S2 staff.

Each student attending the program will receive a 150-page training manual. The host will be provided with a copy of the training manual in PDF-format for duplication prior to the scheduled class. If the host wishes S2 to provide the training manuals, manuals will be produced for the course for a fee of \$20.00 per manual.

Student Restrictions

S2 requests that all students attending the Anti-Terrorism Officer course are actively employed as security or law enforcement practitioners and have been subjected to background checks prior to their employment in their current positions. There are no restrictions on the number of students that may attend the two-day classroom program. Hands-on training sessions should be limited to 20 students.

Presentation Requirements

The host will need to provide the following items on the day of the scheduled class:

1. Private classroom with appropriate seating for the number of students in attendance
2. Windows-compatible audio-visual projector (and extra bulb)
3. Projection screen and presentation table

Although the instructors will bring their own laptop computer for presentation, it is recommended that the host have an extra laptop computer with MS PowerPoint available in the event of a technical problem during the presentation.

Scheduling

Due to our busy project schedule, we recommend contacting us at least 60 days prior to any proposed training dates to confirm the instructor's availability. Once dates have been agreed upon, the host must provide a purchase order or a signed letter of agreement to secure the dates.

To schedule an S2 Anti-Terrorism Officer seminar, contact:

Tim O'Rourke, Executive Director
S2 Safety & Intelligence Institute
1261 South Missouri Ave
Clearwater, FL 33756
Tel. (727) 461-0066
Fax (727) 449-1269
Email: tim@s2institutue.com