S2 ATO SECURITY WORKSHOP
Muscat, Oman; 17th – 20th October 2010

BACKGROUND

The S2 ATO Workshop four-day workshop is designed to instruct security, law enforcement, and military personnel in effective strategies and tactics for protecting facilities against terrorist attack. The objective of this workshop is to prepare anti-terrorism personnel for assignments that require planning security for facilities or providing physical protection to facilities against terrorist attack. The fourth day is a hands-on demonstration of search techniques and search exercises.

The information presented in this workshop reflects best practices in Anti-Terrorism as may be applied to a wide range of government and commercial facilities. The strategies and tactics presented in this workshop are based on the instructors' decades of experience in protecting facilities against terrorist attacks, critical evaluation of hundreds of terrorist incidents, and analysis of methods for managing terrorism-related problems pioneered by organizations ranging from the London Metropolitan Police to the United States Army.

WORKSHOP DETAILS

- Duration: Four Days, 17th – 20th October 2010, 8:30am - 4:30pm;
- Fees: RO 1,275 (including workshop materials, lunch & breaks at the venue);
- Venue: Muscat, Oman;
- Presenter: Craig Gundry, CPS, ATO, CHS-III.

WHO SHOULD ATTEND

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

METHOD OF INSTRUCTION

The method of instruction includes a balanced mixture of classroom lecture and hands-on demonstrations designed to teach students important theoretical concepts as well as practical application of anti-terrorim measures. This type of combined instruction has proven very successful in previous S2 anti-terrorism workshops.

Please contact us for further information or click here to register
Precept Management Consultancy, P.O. Box 255, P.C. 112, Sultanate of Oman
Tel: +968 24497123, Fax: +968 24497222, E-mail: precept@omantel.net.om
Website: www.preceptmanagement.com

CONTENTS

Students attending the S2 Anti-Terrorism workshop will acquire the following skills and competencies:

- Recognising risks associated with contemporary terrorism including an in-depth understanding of contemporary terrorist modus operandi

- Identifying general security requirements essential to reducing terrorism related risk

- Implementing Operations Security (OPSEC) and protective counterintelligence principles to impair terrorists' ability to gather target intelligence, including:
  - Implementing appropriate sound information security principles
  - Recognising possible attempts to collect target intelligence
  - Documenting suspicious activity
  - Investigating and analysing trends of suspicious activity

- Performance-based physical security design as applicable to anti-terrorism

- Screening and searching entrants at facility and building entry points, including:
  - Implementing facility access control procedures
  - Questioning entrants and identifying behavioural signs of deception
  - Recognising indications of falsified or altered identity documents
  - Safely searching hand-carried objects at access control points
  - Safely searching vehicles at access control points
  - Using technical aids for conducting search and screening

- Identifying hazardous devices, possible device components, and risks associated with hazardous devices.

- Recognising indications of terrorist attack or impending terrorist events, including:
  - Recognising possible hazardous device deliveries
  - Screening mail and deliveries for indications of potential hazards
  - Recognising indications of chemical or biological attack

- Safely responding to terrorist incidents and facility-level security response planning:
  - Bomb threats
  - Suspicious hand-carried objects
  - Suspicious vehicles (Possible vehicle bomb deliveries)
  - Suspicious mail
    - Unopened mail
    - Possible contaminated mailings (after opening)
  - Post-Blast Response
  - Chemical/Biological/Radiological attack (Indoor Aerosol/Vapor)
  - Chemical/Biological/Radiological attack (Outdoor Aerosol/Vapor)
  - Chemical/Biological/Radiological attack (Covert)

THE WORKSHOP

DAY 1

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
        - 2.6.8 IEMI/Radio Frequency Weapon Attacks
    - 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 Ordinance
    - 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 Devise 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

DAY 2

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 Counter surveillance
        - 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
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
            - 7.2.2.1 CCTV
            - 7.2.2.2 Stationary Posts
            - 7.2.2.3 Mobile Patrols
            - 7.2.2.4 Intrusion Indicators
            - 7.2.2.5 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

DAY 3

- 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

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
  - 8.5.1Suspect 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 Localised 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 Localised 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

DAY 4

10. Facility Search Techniques
    10.1 Search Safety
    10.2 Two-Man Room Search Technique
        Room Search Exercise
    10.3 Alternative Search Methods for Unconventional
11. Human Entry Screening
    11.1 Initial Considerations
    11.2 Identity Document Examination
    11.3 Entrant Screening Methodology
        11.3.1 Behavioral Threat Indicators
    11.4 Hand Search of Personal Objects
12. Vehicle Entry Screening
    12.1 Initial Considerations
    12.2 Driver Screening
        12.2.1 Driver Documents
    12.3 Vehicle Search Procedures
        12.3.1 VBIED Threat Indicators

Vehicle Search Exercise

THE COMPANY

Since 1998, the S2 Safety & Intelligence Institute has trained thousands of security, intelligence, and law enforcement professionals in critical public safety topics. With a staff of world class instructors, S2 has earned a reputation as one of the U.S.'s premier sources of security and public safety training.

S2 provide traditional classroom instruction and hands on training at their facility in Clearwater, Florida and at host locations throughout the United States. Through their sister company the, S2 Online Academy, they also deliver high quality distance education to students thought the world.

S2 students represent hundreds of corporations and government organisations. Some examples of S2 clients include the Federal Bureau of Prisons, US Capitol Police, US Department of Justice, and US Special Operations Command.

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

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 management, 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 specialising 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 on issues relating to terrorism and weapons of mass destruction and has provided expert commentary for numerous media organisations, including CNN.

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 from over 30 nations.