Anti-Terrorism Officer (ATO) Course

Vienna, Austria

18-22 November 2019

Background

On 18-22 November 2019, the S2 Institute, in conjunction with the International Association of Counterterrorism and Security Professionals (IACSP) will be presenting a five-day, 40-hour version of the S2 Anti-Terrorism Officer (ATO) Course in Vienna, Austria.

The S2/IACSP Anti-Terrorism Officer (ATO) Course is designed to prepare security and law enforcement professionals for assignments involving the protection of facilities against terrorist attack. This program provides a detailed exploration of contemporary terrorist methods and essential skills and knowledge that all anti-terrorism personnel should possess.

Who Should Attend?

Security Officers, Security Directors, Risk Management Professionals, Military Force Protection Personnel, and Police Officers Assigned to Anti-Terrorism Activities

Learning Objectives

Students attending the S2/IACSP Anti-Terrorism Officer Course will acquire the following skills and competencies:

- Recognizing 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

- Assessing facility risks and utilizing risk management principles in anti-terrorism planning

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

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

Schedule & Outline

Monday, 18 November 2019 (Day One)

08:00 – 08:30	Class Registration
08:30 – 10:30	Dynamics of Contemporary Terrorism
10:30 – 12:00	Characteristics of Explosive Threats
12:00 – 13:00	Lunch
13:00 – 15:00	Characteristics of Explosive Threats (cont.)
15:00 – 16:30	Chemical and Biological Terrorism

Day One Outline:

- The Certified Anti-Terrorism Officer
  - ATO Functions & Responsibilities
  - ATO Skills
  - IACSP cATO Certification Process
    - Prepping for the cATO Exam and Making Most of the ATO Course
- Introduction to Terrorism
  - Definition
  - Ideological Motives
  - Strategic Objectives
  - Types of Terrorist Targets
  - Target Selection Criteria
    - Threat Analysis and Target Attractiveness
    - EXERCISE: Is my organization a potential target for terrorists?
  - Categories of Terrorism Related Risk
    - Explosive Attack
    - Kidnapping
    - Armed Attack
      - Hijacking
      - Armed Occupation
    - Vehicle Ramming Attack
    - Arson
    - Chemical/Biological/Radiological (CBR)
    - Nuclear
    - Cyber Attack
    - IEMI/Radio Frequency Weapon Attacks
  - Terrorist Planning and Execution Phases
- Threat: Explosive Attacks
  - Types of Explosive Devices
  - Characteristics of Chemical Explosions
  - High vs Low Explosives
  - Sensitivity of Explosives
  - Initiation
  - Common Explosives
  - Gas Enhanced IEDs
  - Activation
  - Device Concealment
  - Damage Potential
    - Types of Destructive Forces
    - Estimating Charge Size
    - Overpressure Range Effects Estimation
  - Explosive Employment Scenarios: Land Facilities
    - Vehicle Borne IEDs
    - Projected Charge Attacks
  - Explosive Employment Scenarios: Piers & Watercraft
- Threat: Chemical & Biological Terrorism
  - Common Assumptions About CB Terrorism
  - Why Use CB Agents?
  - CB Terrorists
  - Challenges faced By CB Terrorists

Tuesday, 19 November 2019 (Day Two)

08:30 – 09:30	Chemical & Biological Terrorism (cont.)
09:30 – 11:00	Risk Management & Anti-Terrorism Security Planning
11:00 – 12:00	Protective Counterintelligence

12:00 – 13:00	Lunch
13:00 – 14:30	Protective Counterintelligence (cont.)
14:30 – 16:30	Physical Security & Access Control

Day Two Outline:

- Threat: Chemical & Biological Terrorism (cont.)
  - Requisite Characteristics of CB Agents
    - Terrorist vs Military Agents
  - Routes of Exposure
  - Symptoms
  - Chemical Agents
  - Agents of Biological Origin
  - Dissemination of CB Agents
  - CB Employment Scenarios
    - On-Target Facility Attacks
      - Point Source Contamination
      - IDD Attacks
      - Contaminated Deliveries
    - 4.11.2 Off-Target Facility Attacks
      - Point Source Contamination
      - Outdoor Aerosol/Vapor Attacks
      - Projected Charge Weapons
    - Attacks Against Employees at Off-Site Venue
      - Food & Beverage Contamination
      - CB Projectile Weapon
- Risk Management & Anti-Terrorism Security Planning
  - Risk Management Principles
  - Risk Assessment for Anti-Terrorism Applications
    - Risk Assessment Process
      - Asset Identification and Valuation
      - Threat Assessment
      - Vulnerability Assessment
      - Risk Analysis
  - Integrated Countermeasures Strategy
    - Proactive Countermeasures
    - Reactive/Mitigative Countermeasures
  - Adapting Risk Management Strategy to Application
    - Unique Facility/Organizational Considerations
    - Soft Targets versus Hard Targets
    - Examples
- Operations Security (OPSEC) & Protective Counterintelligence
  - Terrorist Intelligence Requirements
  - Terrorist Intelligence Collection Methods
  - Complexity of Intelligence Requirements
  - Protective Counterintelligence/OPSEC
    - Information Security
    - Employee/Contractor Screening & Monitoring
    - Surveillance Detection
      - Surveillance Detection Guidelines
      - Active Counter-Surveillance
    - Suspicious Activity Investigation
    - Suspicious Activity Reporting & Analysis
- Physical Security & Entry Control
  - Physical Security Theory
    - Physical Protection System Functions
    - Integrated Systems

        - Performance Definition
        - System Design Guidelines
    - Physical Protection System Components
        - Intrusion Detection Systems

Wednesday, 20 November 2019 (Day Three)

08:30 – 12:00	Physical Security & Entry Control (cont.)
12:00 – 13:00	Lunch
13:00 – 15:30	Physical Security & Entry Control (cont.)
15:30 – 16:30	Additional Proactive Security Measures

Day Three Outline:

- Physical Security & Entry Control (cont.)
    - Physical Security Components (cont.)
        - Area Surveillance
            - CCTV
            - Stationary Posts
            - Mobile Patrols
            - Intrusion Indicators
            - Bomb Delivery indicators
        - Barriers
            - Anti-Personnel Barriers
                - Delay Time Calculation
                - Barrier System Design
                - Barriers and Facility Applications
                - Safe Rooms
            - Vehicle Barriers
            - Vehicle Entry Points
                - Entry Point Design
                - Active Barricades
        - Emergency Exit and Escape Planning
        - Physical Protection System Design & Analysis
            - Performance-Based Analysis Methods
            - EXERCISE: Adversary Paths
            - EXERCISE: EASI Model
    - Control
        - Planning Considerations
        - Types of Entrants
        - Entrant Verification
            - Verification Methods
            - Verification System Design (Risk-Dependent Options)
        - Access Screening Technologies
            - X-Ray Based Technologies
            - Explosive Trace Detection
            - Nuclear Detection Systems
            - Explosive Detection Canines
        - Human Entry Screening
            - Initial Considerations
            - Entrant Screening Methodology
        - Vehicle Entry Screening
            - Initial Considerations
            - Vehicle Search Procedures

Thursday, 21 November 2019 (Day Four)

08:30 – 12:00	Additional Proactive Security Measures
12:00 – 13:00	Lunch
13:00 – 14:30	Group Exercise: Risk Management Strategy & Applications
14:30 – 16:30	Mail Security Planning

Day Four Outline:

- Additional Proactive Security Issues
  - Limited Concealment Opportunities
  - Obscuration
    - Projected Charge Weapon Dynamics
    - Obscuration Screens
  - Chemical & Biological Attack Risk Mitigation
    - Physical Security for Possible Contamination Points
    - Cafeteria and Break Room Countermeasures
    - Water Filtration
    - HVAC System Protection
      - CB Agent Detection Systems
      - Facility Design for Mitigating Airborne Threats
      - HVAC Filtration Systems
  - IEMI Protection
    - Conducted IEMI Protection Strategies
    - Radiated IEMI Protection Strategies
  - Unmanned Aerial Vehicle Countermeasures
    - UAV Detection Systems
    - UAV Countermeasures Options
  - Blast Mitigation & Facility Design
    - Blast Mitigation Strategies
    - Minimizing Fragmentation Hazards
    - Blast Walls
    - Structural Design
    - Façade Construction & Fenestration
      - Wall Reinforcement
      - Glazing Systems
      - Additional Protective Options
    - Emergency Access & Evacuation Requirements
    - Protection of Building Subsystems
    - Utilization & Protective Asset Positioning
- GROUP EXERCISE: Unique Situations and Protective Strategies
  - Shopping Mall
  - Hotel
  - Office Building
  - Electrical Power Plant
  - Military Base

- Mail Security
  - Types of Hazardous Mailings
  - Mail Security Planning
    - Initial Considerations
  - Physical Mail Screening
    - Threat Indicators
    - Case Studies
  - Technical Mail Screening
  - Response to Hazardous Mailings
    - Suspect Mail Bomb Response
    - Response to Contaminated Mailings

Friday, 22 November 2019 (Day Five)

08:30 – 12:00	Response to Terrorist Attacks
12:00 – 13:00	Lunch
13:00 – 16:15	Response to Terrorist Attacks (cont.)
16:15 – 16:30	Graduation Presentation

Day Five Outline:

- Response to Terrorist Incidents
  - Incident Response Scenarios
  - Response Priorities
  - Responsibilities & Incident Command Systems
  - Communications Systems and Infrastructure
  - Weapons of Mass Destruction
    - WMD Response Authority
  - Active Shooter/Marauding Terrorist Firearms Attack (MTFA) Response
    - Organizational Response
    - Employee Response
  - Bomb Threat Response
    - Bomb Threat Motives
      - Malevolent Bomb Threat Strategies
    - Bomb Threat Planning Considerations
    - Search and Response Approaches
      - Security Team Search
      - Employee Work Area Search
      - Police Directed Search
    - Search Safety
    - Security Team Search Walk Through
      - Managing Bomb Threat Calls
      - Search Procedures
        - Room Search Techniques
    - Bomb Threat Response & The Real World
    - Response to Suspicious Objects
  - Suspicious Vehicle Response
    - Initial Alert & Refuge
    - TSWG Evacuation and Refuge Guidelines
    - Refuge Procedures
    - Evacuation Procedures
  - Post-Blast Response
    - Types of Post-Blast Scenarios
    - Localized Bombings
      - Characteristics of Localized Bombings
      - Localized Response Procedures
    - Conventional Weapon of Mass Destruction Incidents
      - Characteristics of CWMD Incidents
      - CWMD Public Safety Response
        - CWMD Response Scenario
        - Triage
      - CWMD Facility Response Guidelines
        - Important Safety Guidelines
      - Post-Incident Recovery Issues
  - Chemical & Biological Attack Response
    - Unique Response Issues
    - Key Players
    - Responsibilities
    - Public Safety Response Sequence

- Facility-Level Response
  - Attack Recognition
    - Chemical Attack Indicators
    - Biological Attack Indicators
  - Response to Indoor Aerosol/Vapor Attacks
    - Evacuation
    - Expedient Respiratory and Skin Protection
    - Emergency Decontamination
  - Response to Outdoor Aerosol/Vapor Attacks
    - Shelter-In-Place Procedures
    - Emergency Evacuation Procedures
  - Response to Covert CB Attacks

What Will You Receive?

In addition to 40-hours of instruction, all students attending the S2/IACSP Anti-Terrorism Officer Course will receive the following:

- Certificate of Completion suitable for framing
- Course notebook including over 250 pages of slides and reference material
- Digital library archive including security assessment tools and calculators and over 20,000 pages of reference documents related to course topics.
- 1-Year Membership in the International Association of Counterterrorism and Security Professionals (IACSP), including one-year subscription to Counterterrorism & Homeland Security International magazine. Existing IACSP members will receive one-year renewal of membership)
- Application Fee Waiver for the IACSP Certified Anti-Terrorism Officer (cATO) certification (US$30 value)
- S2 Institute Anti-Terrorism Officer Challenge Coin

Enrollment in the S2/IACSP Anti-Terrorism Officer Course also includes catered lunches and coffee breaks.

IACSP Certified Anti-Terrorism Officer (cATO™) Professional Certification

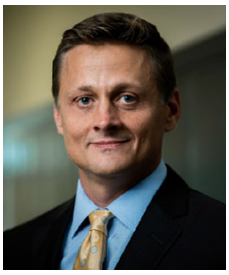
In addition to providing 40-hours of instruction on topics essential to protecting facilities against terrorist attack, the S2/IACSP Anti-Terrorism Officer (ATO) course is designed to prepare program participants for independent certification through the International Association for Counterterrorism and Security Professionals Certified Anti-Terrorism Officer (cATO™) Program. In order to be awarded with the IACSP cATO™ certification, eligible candidates are required to complete and successfully pass a 100-question examination based on content included in the IACSP/S2 Institute ATO course.

Information about the IACSP Certified Anti-Terrorism Officer application, examination, and certification process is available online: www.catocertification.org.

IMPORTANT NOTE: Attending the S2/IACSP Anti-Terrorism Officer course does not guarantee award of IACSP cATO™ certification. All course graduates pursuing certification after attending the

program must meet essential eligibility criteria and complete the independent application and certification process including successful completion of the cATO™ examination.

About the Instructor



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

Craig Gundry is the S2 Institute's lead instructor for anti-terrorism subjects and the Vice President of Special Projects for Critical Intervention Services (CIS). Mr. Gundry is responsible for directing CIS consulting and training projects pertaining to terrorism and critical infrastructure 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 and anti-terrorism with the United States Army.

Mr. Gundry is the author of the acclaimed Bomb Countermeasures for Security Professionals CD-ROM and numerous publications on terrorism-related topics. Mr. Gundry is also a court-qualified expert witness on physical security and risk management and provides frequent expert commentary on terrorism and weapons of mass destruction issues for news media organizations including Al-Jazeera, BBC, CNN, The Blaze, and Fox News Network.

As an instructor, Mr. Gundry has been training security and public safety professionals in terrorism-related issues for over 17 years. His previous students have included over 3,000 security professionals, facility managers, military personnel, police officers, and federal officials from over 50 nations.

Enrollment

Standard Tuition: USD $2,500 (*Group discounts available. Contact us for details.)*

To enroll in the S2 Anti-Terrorism Officer (ATO) Course, use our secure online registration and payment system:
http://www.s2institute.com/content/_pages_advanced/_courses/ato_vienna19.php

Students may also enroll by completing the attached enrollment form and returning it by fax to: +01-727-535-6666.

Questions regarding enrollment may be submitted to the S2 Institute by email:
info@s2institute.com

Lodging & Travel Information

The S2/IACSP ATO Course will be conducted on-site at the Fleming's Selection Hotel Wien-City:

Fleming's Selection Hotel Wien-City
Josefstädter Straße 10-12
A-1080 Wien
Austria
Tel. +43 1 205 99-0

https://www.flemings-hotels.com/selection-hotel-wien-city

Please note: Lodging is not included.