SECURITY MANAGEMENT FOR CRITICAL INFRASTRUCTURE
Elysium Resort Paphos, Cyprus; 24th May – 11th June 2010

WHY NEEDED

The Security Management for Critical Infrastructure workshop is designed to instruct security personnel in a range of topics essential to protecting critical infrastructure sites and assets.

WORKSHOP DETAILS

• Duration: Fifteen Days, 24th May – 11th June 2010, 9:00 am – 4:00 pm;
• Fees: USD$ 10,575 (including workshop material, lunch & break at the venue);
• Venue: Elysium Resort Paphos, Cyprus (http://www.elysium-hotel.com);
• Presenters: Craig Gundry, CPS, ATO, CHS-III
  Robert Logan, ATO

CONTENTS

Students attending the Security Management for Critical Infrastructure course will acquire the following skills and competencies:

- Recognizing risks associated with critical infrastructure including an in-depth understanding of contemporary terrorist modus operandi and methods of covert sabotage used by state-directed adversaries
- Identifying security requirements essential to reducing security risk in critical infrastructure facilities
- Assessing facility risks and utilizing risk management principles in security planning, including:
  - Understand risk management principles and the function of risk assessment in security planning.

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
Recognize important characteristics of security related risk
Conduct security assessments by utilizing qualitative risk assessment methodology.
Design prioritized security countermeasures strategies by utilizing cost-benefit analysis techniques.

Implementing Operations Security (OPSEC) and protective counterintelligence principles to impair adversaries gathering target intelligence, including:
- Designing appropriate information security policies and procedures
- Detecting possible attempts to collect target intelligence
  - Surveillance and Reconnaissance Detection
  - Active Countersurveillance
- Documenting and cataloguing suspicious activity
- Investigating and analyzing trends of suspicious activity

Physical security design and analysis, including an in-depth understanding of:
- Physical security theory
- Performance-based physical security design
- Barrier technology
- Intrusion detection technology
- Response force integration

Screening and searching entrants at facility and building entry points, including:
- Designing facility access control procedures
- Questioning entrants and identifying behavioral signs of deception
- Recognizing indications of falsified or altered identity documents
- Procedures for search of hand-carried objects at access control points
- Procedures for search of vehicles at access control points
- Employment of technical aids for conducting search and screening

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

Recognizing indications of terrorist or sabotage attack or impending attack, including:
- Recognizing possible hazardous device deliveries
- Recognizing indications of chemical or biological attack.

Safely responding to terrorist and sabotage incidents and facility-level security response:
- Bomb threats
- Suspicious hand-carried objects
- Suspicious vehicles (Possible VBIED deliveries)
- Post-Blast Response
- Chemical/Biological/Radiological attack
- RFW/EMI Attack
- Armed assault (including tactical preparation of security forces)

Designing and implementing security force training programs.

Security force management and leadership.
THE WORKSHOP
WEEK ONE

Day 1
09:00 – 09:30  Program Orientation
09:30 – 12:00  Critical Infrastructure Threats
12:00 – 13:00  Lunch
13:00 – 16:00  Critical Infrastructure Threats (Cont.)

Day One provides a detailed analysis of potential adversaries to UAE critical infrastructure, threat scenarios, and threat modus operandi.

Instruction of Day One will be conducted by Craig Gundry.

Day 1 Outline:
- Program Orientation and Training Objectives
- Adversaries and Threats to Critical Infrastructure
  - Target Attractiveness and Critical Infrastructure
    - Potential Adversaries
      - Hostile Nations
        - Motives & Objectives
        - Adversary Characteristics
      - Terrorists / Ideologically-Motivated Non-State Actors
        - Strategic Objectives
        - Target Selection Criteria
        - Adversary Characteristics
    - Criminals
      - Motives & Objectives
      - Adversary Characteristics
  - Security Related Threat Scenarios
    - Explosive Attack
      - IED Attack Tactics and Threat MO
    - Physical Sabotage
    - Armed Assault
      - Armed Occupation

Day 2
09:00 – 12:00  Critical Infrastructure Threats (Cont.)
12:00 – 13:00  Lunch
13:00 – 16:00  Security Planning Concepts

Day Two concludes Day One’s detailed analysis of potential adversaries to UAE critical infrastructure and surveys security planning theory.

Instruction of Day Two will be conducted by Craig Gundry.

Day 2 Outline:
- Adversaries and Threats to Critical Infrastructure (Cont)
  - Civil Disturbance
  - Arson
  - Chemical/Biological/Radiological Contamination
  - Cyber Attack
Day 3

09:00 – 11:00 Principles of Risk Management
11:00 – 12:00 Risk Assessment Methodology
12:00 – 13:00 Lunch
13:00 – 16:00 Risk Assessment Methodology (Cont.)

Day Three introduces the principles of security risk management and explores methodology for conducting security risk assessments. Although the information in Day Three is presented in lecture format, several workshop exercises aimed at reinforcing important concepts will be conducted in the classroom and discussed as a group.

Instruction of Day Three will be conducted by Craig Gundry.

Day 3 Outline:

➢ Principles of Security Risk Management
  ✓ What is Risk?
    ✓ Risk Definitions
    ✓ Risk Elements
    ✓ Risk Expressions
  ✓ Fundamental Risk Management Concepts
  ✓ Risk Assessment Approaches
    ✓ Quantitative Risk Assessment
    ✓ Qualitative Risk Assessment
  ✓ Basic Qualitative Risk Assessment Model

➢ Risk Assessment Methodology for Critical Infrastructure
  ✓ Guidelines for Assessing Security Related Risk
  ✓ Step One: Identify and Profile Assets
    ✓ Asset Identification
    ✓ Sources of Asset Information
    ✓ Identification of Undesirable Events
    ✓ Exercise 1: Asset Inventory
  ✓ Asset Valuation
    ✓ Asset Valuation Considerations
    ✓ Establishing Asset Valuation Criteria
    ✓ Examples of Asset Valuation Scales
    ✓ Exercise 3: Develop a Criteria Scale for Rating Risk Criticality
Day Four continues exploring risk assessment methodology with a survey of threat assessment techniques and vulnerability assessment methods, assimilating risk data, and surveying several models for conducting risk assessments in critical infrastructure. During Day Four several in-class workshop exercises will be conducted to reinforce important concepts and aid students in applying risk management concepts in practical situations.

Instruction of Day Four will be conducted by Craig Gundry.

Day 4 Outline:
- Risk Assessment Methodology for Critical Infrastructure (Cont.)
  - Step Two: Identify and Profile Threats (a.k.a. “Threat Analysis”)
    - Categories of Threats
    - Identifying Potential Adversaries
    - Adversary Assessment
      - Sources of Adversary Information
      - Determination of INTENT and CAPABILITY
    - Analysis of Critical Threat Modus Operandi
      - Exercise 2: Assess Al-Qaeda as a Potential Adversary
    - Identification of Potential Risks Based on Threat M.O.
    - Development of Design Basis Threats (DBTs)
  - Development of Threat Scenarios
    - Exercise 3: Develop Several Threat Scenarios
  - Development of Threat Rating Criteria
- Step Three: Identify Asset Vulnerabilities
  - Vulnerability Assessment Principles
  - Areas of Vulnerability
  - Vulnerability Assessment Approaches
    - Compliance-Oriented Assessment Approaches
    - Performance-Oriented Assessment Approaches
    - Security Assessment Surveys
    - Quantitative Path Intrusion Analysis
    - Path Analysis Models and Software
    - Fault Tree Analysis
    - Practical Field Tests (a.k.a. “Red Team Exercises”)

Day Five concludes the risk assessment component with a module on assimilating risk data, and surveying several models for conducting risk assessments in critical infrastructure. In the afternoon of Day Five, the instructor explores the subject of pre-attack intelligence collection and countermeasures for detecting and impairing hostile intelligence collection against critical infrastructure facilities.

Instruction of Day Five will be conducted by Craig Gundry.
Day 5 Outline:
- Risk Assessment Methodology for Critical Infrastructure (Cont.)
  - Step Four: Evaluate Risk
    - Determining Risk Probability
    - Develop Probability/Criticality Pairing System for Risk Definition
    - Establish Level of Risk and Risk Acceptability
  - Step Five: Identify & Implement Countermeasures
    - Integrated Countermeasures Theory
      - Proactive Countermeasures
      - Reactive/Mitigative Countermeasures
    - Identifying Potential Countermeasures
      - Countermeasures Options
    - Countermeasures Cost-Benefit Analysis
      - Determining the Potential Effectiveness of Countermeasures
      - Determining the Cost of Countermeasures
      - Determining Risk Reduction Goals
  - Applied Cost-Benefit Analysis
- Operations Security (OPSEC) and Protective Counterintelligence
  - Adversary Intelligence Requirements
  - Adversary Intelligence Collection Methods
  - Complexity of Intelligence Requirements
  - Protective Counterintelligence/OPSEC
    - Information Security
    - Employee/Contractor Screening & Monitoring
      - Background Flags
      - HUMINT Indicators
    - Surveillance Detection & Countersurveillance
      - Surveillance Detection Guidelines
      - Countersurveillance Planning
    - Suspicious Activity Investigation
      - Suspicious Telephone Inquiries
      - Possible On-Site Reconnaissance
      - Possible Off-Site Surveillance
      - Possible Elicitation Contacts
      - Recruitment Approaches
      - Theft of ID Cards, Vehicle Stickers, etc.
      - Suspicious Activity Reporting, Investigation, & Analysis

WEEK TWO
Day 6
09:00 – 12:00  Physical Security & Access Control
12:00 – 13:00  Lunch
13:00 – 16:00  Physical Security & Access Control (Cont.)

Day Six surveys physical security theory, physical security design considerations, intrusion detection technology, surveillance and patrol employment, and security lighting concepts.

Instruction of Day Six will be conducted by Craig Gundry.
Day 6 Outline:
- **Physical Security & Access Control**
  - Physical Security Theory
    - Physical Security System Functions
    - Integrated Systems
    - Performance Definition
    - Common Design Flaws
    - System Design Guidelines
  - Physical Security Components
    - Intrusion Detection Systems
      - System Design Considerations
      - Intrusion Detection Sensor (IDS) Technology
      - IDS Signal Systems
      - ISD Monitoring Systems
  - Area Surveillance
    - CCTV
    - Intelligent CCTV Software Systems
    - Stationary Posts
    - Mobile Patrols
    - Intrusion Indicators
    - Bomb Delivery indicators
  - Security Lighting
    - Principles of Security Illumination
    - Illumination Design Considerations
    - Lighting Systems

Day 7

09:00 – 12:00 Physical Security & Access Control (Cont.)
12:00 – 13:00 Lunch
13:00 – 16:00 Physical Security & Access Control (Cont.)

Day Seven continues the examination of physical security with an exploration of barrier technology and access control design for critical infrastructure facilities.

Instruction of Day Seven will be conducted by Craig Gundry.

Day 7 Outline:
- **Physical Security & Access Control**
  - Barrier Technology
    - Conventional Barriers
      - Delay Time Calculation
      - Conventional Barrier Options
      - Barrier System Design
      - Barrier Employment Guidelines
    - Vehicle Barriers
      - Kinetic Energy Calculation
      - Passive Vehicle Barriers
      - Vehicle Barrier System Design
    - Vehicle Entry Points
      - Entry Point Design
      - Active Barriers
Day 8
09:00 – 12:00  Physical Security & Access Control (Cont.)
12:00 – 13:00  Lunch
13:00 – 16:00  Physical Security Analysis (Cont.)

Day Eight provides a survey of vehicle inspection techniques, tactical preparation and armed defense of critical infrastructure sites, and methods for analyzing the effectiveness of physical security design. Day Eight concludes with a physical security design evaluation exercise utilizing the techniques of Quantitative Intrusion Path Analysis.

Instruction of Day Eight will be conducted by Craig Gundry.

Day 8 Outline:
- **Physical Security & Access Control (Cont.)**
  - Vehicle Search Techniques for Entry Points
  - Hand Search at Entry Points
  - Tactical Readiness and Facility Defense
- **Physical Security Performance Analysis**
  - Performance Analysis Methods
  - Quantitative Intrusion Path Analysis
    - Basic Theory
    - Estimate of Adversary Sequence Interruption Model
    - Adversary Sequence Diagrams
    - Physical Security Analysis Exercises

Day 9
09:00 – 12:00  Blast Mitigation Design
12:00 – 13:00  Lunch
13:00 – 14:00  Blast Mitigation Design (Cont.)
14:00 – 16:00  Special Issues in Facility Security Design

Day Nine explores the subject of blast dynamics and facility design to reduce damage of critical assets to explosive attacks. In the afternoon of Day Nine, special security design issues such as minimized concealment areas, protection from projected charge weapons, and chemical and biological countermeasures are discussed in the context of critical infrastructure protection.

Instruction of Day Nine will be conducted by Craig Gundry.

Day 9 Outline:
- **Blast Mitigation Design**
  - Blast Assessment
Day Ten explores the types of major security incidents that should be prepared for as part of the contingency planning process and presents model procedures for use in critical infrastructure environments.

Instruction of Day Ten will be conducted by Craig Gundry.

Day 10 Outline:

- Response to Major Security Incidents
  - Incident Response Scenarios
  - Response Priorities
  - Responsibilities
- 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
    ▶ Suspicious Vehicle (Possible VBIEED) Response
      ▶ Initial Alert & Refuge
      ▶ Evacuation and Refuge Guidelines
      ▶ Refuge Procedures
      ▶ Evacuation Procedures
    ▶ Post-Blast Response
      ▶ Types of Post-Blast Scenarios
      ▶ Localized Bombings
        ▶ Characteristics of Localized Bombings
        ▶ Facility Damage
        ▶ Casualties and Injury Types
        ▶ Post-Blast Hazards
        ▶ Localized Response Procedures
    ▶ Conventional Weapon of Mass Destruction (CWMD) Incidents
      ▶ Characteristics of CWMD Incidents
      ▶ Facility Damage
      ▶ Casualties and Injury Types
      ▶ Post-Blast Hazards
      ▶ CWMD Public Safety Response
        ▶ CWMD Response Scenario
        ▶ Triage
      ▶ CWMD Facility Response Guidelines
        ▶ Important Safety Guidelines
        ▶ Post-Incident Recovery Issues

WEEK THREE
Day 11
09:00 – 12:00 Disaster Preparedness for Critical Infrastructure
12:00 – 13:00 Lunch
13:00 – 16:00 Disaster Preparedness for Critical Infrastructure

Day Eleven focuses exclusively on disaster preparedness for critical infrastructure organizations with emphasis on the security implications of disaster events.

Instruction of Day Eleven will be conducted by Robert Logan.

Day 11 Outline:
  ▶ Characteristics of Natural Disasters
    ▶ Case Studies
  ▶ Post-Disaster Security Concerns
  ▶ Disaster Response Planning
    ▶ Mission Requirements
    ▶ Personnel Deployment Organization and Readiness
Mutual Aid Planning & Pre-Disaster Assistance Agreements
Pre-Disaster Preferred Vendor Agreements
Interagency Coordination

Logistical Planning
Food, Lodging, Water, and Fuel
Communications
Transportation

Managing Post-Disaster Security Deployments
Information Management
  • EDICTS
Personnel Management Issues

Day 12
09:00 – 12:00 Security Force Organization and Training
12:00 – 13:00 Lunch
13:00 – 16:00 Security Force Organization and Training
Day Twelve surveys ideal organizational structures, Table of Equipment (TOE), and training for security personnel assigned to critical infrastructure protection.

Instruction of Day Twelve will be conducted by Robert Logan.

Day 12 Outline:
- Security Force Organizational Models
- Security Personnel Employment Criteria
- Security Personnel Training
  - Basic Training
  - Operational Training
  - Weapons and Tactical Training
  - Emergency Response Training
  - Site Specific Training
- Table of Equipment
  - Personal Equipment
  - Team Equipment
- Case Study: CIS Anti-Terrorism Officer Program

Day 13
09:00 – 12:00 Security Force Policies and Procedures
12:00 – 13:00 Lunch
13:00 – 15:00 Security Force Policies and Procedures

Day Thirteen provides a detailed examination of best practices in security force operations with focus on administrative and operational policies. Training on Day 13 also includes a presentation of model policies for various applications in critical infrastructure protection and several interactive exercises aimed at designing and writing policies.

Instruction of Day Thirteen will be conducted by Robert Logan.

Day 13 Outline:
- Standard Operating Procedures: The ‘Bible’ of Security Force Operations
- Organizational SOPs vs. Post Orders
- Universal Standard Operating Procedures
  - Model Policies and Best Practice Procedural Guidelines
- Policy and Procedure Writing Exercise
**Day 14**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 – 12:00</td>
<td>Security Force Leadership</td>
</tr>
<tr>
<td>12:00 – 13:00</td>
<td>Lunch</td>
</tr>
<tr>
<td>13:00 – 15:00</td>
<td>Security Force Leadership</td>
</tr>
</tbody>
</table>

Day Fourteen is the first day of a two-day interactive leadership workshop for security force leaders and supervisors. This is the same seminar used for professional leadership development for Critical Intervention Services and the Hillsborough County Sheriff’s Office. The principles of leadership as explored in this program are universal and applicable directly to any security or military organization.

Instruction of Day Fourteen will be conducted by Robert Logan.

**Day 15**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 – 12:00</td>
<td>Security Force Leadership</td>
</tr>
<tr>
<td>12:00 – 13:00</td>
<td>Lunch</td>
</tr>
<tr>
<td>13:00 – 15:00</td>
<td>Security Force Leadership</td>
</tr>
<tr>
<td>15:00</td>
<td>Graduation and Presentation of Certificates</td>
</tr>
</tbody>
</table>

Day Fifteen is the second day of a two-day interactive leadership workshop for security force leaders and supervisors. This is the same seminar used for professional leadership development for Critical Intervention Services and the Hillsborough County Sheriff’s Office. The principles of leadership as explored in this program are universal and applicable directly to any security or military organization.

Instruction of Day Fifteen will be conducted by Robert Logan.
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.

PRESENTERS’ PROFILES

*Craig S. Gundry, CPS, ATO, 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 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 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 on issues relating to terrorism and weapons of mass destruction and has provided expert commentary for numerous media organizations including Al-Jazeera, CNN, and Fox News Network.

As an instructor, Mr. Gundry has been training security, police, and emergency responders in terrorism-related issues for over 16 years. His previous students have included security professionals, facility managers, military personnel, police officers and federal officials from over 30 nations.
Robert Logan, ATO

Robert Logan is the S2 Institute’s lead instructor for disaster deployment operations and security force operations in hazardous environments. Mr. Logan is also an S2 instructor for advanced firearms and tactical operations.

Prior to joining the S2 training staff as a full-time instructor, Mr. Logan was the Commander of Hazardous Operations for Critical Intervention Services. As the Commander of Hazardous Operations at CIS, Mr. Logan was the senior operational commander of the Anti-Terrorism Officer division, responsible for protecting various critical infrastructure sites in the State of Florida. Mr. Logan was also the Field Commander for security operations during several major natural disasters including Hurricane Katrina, Hurricane Rita, and Hurricane Wilma. As part of these operations, Mr. Logan was responsible for supervising special security related deployments ranging from protecting field logistics facilities for power utilities to recovery of high value assets in afflicted zones.

Prior to joining CIS in 1995, Mr. Logan was a specialist in arctic warfare with the United States Army and mountaineering instructor for the 10th Mountain Division in Alaska. In addition to his duties as an S2 instructor, Mr. Logan is currently retained by several electrical power companies as a consultant on security force operations and NERC compliance.