Hotels: Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures

Bill Schweigart
Program Analyst, Commercial Facilities Sector
Office of Infrastructure Protection
U.S. Department of Homeland Security
(703) 235-2866
Bill.Schweigart@dhs.gov

The 2009 Hospitality Law Conference
February 9-11, 2009

Biography

Bill Schweigart
Commercial Facilities Sector

Mr. Bill Schweigart is a Program Analyst and Security Specialist for the Department of Homeland Security Office of Infrastructure Protection, Commercial Facilities Sector. The Commercial Facilities Sector is designated as a national key resource that includes prominent commercial centers, office buildings, shopping centers, arenas, stadiums, hotels, convention centers, and theme parks. Within the sector, Mr. Schweigart's focus is on the Lodging, Entertainment & Media, and Real Estate subsectors as well as cultural properties. He is a former U.S. Coast Guard officer with a background in Continuity of Operations (COOP) planning.

Prior to this assignment, Bill served at DHS Headquarters, working to reduce the Nation's vulnerability to disasters, including but not limited to influenza pandemics, hurricanes, and all-hazard contingencies, first with the National Preparedness Task Force, then with the Office of Risk Management & Analysis. Bill is one of the authors of the DHS Pandemic Influenza Contingency Plan, contributing the Continuity of Operations and National Incident Management annexes.

Prior to working for DHS Headquarters, Bill served as the Deputy COOP Program Manager for the Coast Guard, providing planning, implementation, exercise, and training support to USCG Headquarters. He developed and modified guidelines and procedures for the conduct of the Continuity of Operations and business continuity programs at Coast Guard Headquarters and field units.

During his active duty service with the Coast Guard as the Fifth Coast Guard District Contingency Planner, Bill developed, reviewed, and approved contingency plans focusing on severe weather and critical infrastructure protection for Coast Guard units in the mid-Atlantic states. He was the primary Business Continuity and Contingency Plan developer and consultant for the 75 units in his district and was awarded USCG Commendation Medal for outstanding achievement. Bill also served as a Coast Guard liaison to Department of Transportation and Federal Emergency Management Agency for domestic emergencies, and served as a Deck Watch Office aboard the Coast Guard Cutter BEAR.

Bill Schweigart
Program Analyst, Commercial Facilities Sector
Office of Infrastructure Protection
U.S. Department of Homeland Security
(703) 235-2866
bill.schweigart@dhs.gov

**"Hotels: Common Vulnerabilities,
Potential Indicators of Terrorist Activity, and
Protective Measures"**

**Bill Schweigart
U.S. Department of Homeland Security**

I. Scope of Presentation. This presentation will discuss common vulnerabilities in hotels, potential indicators of terrorist activity, and protective measures that can be implemented at facilities, and protective programs available through the U.S. Department of Homeland Security. The presentation will also discuss the ongoing effort to develop a Lodging Protective Measures Guide with the coordination of our Lodging Subsector partners.

II. The Commercial Facilities (CF) Sector

A. **CF Sector Vision Statement:** The Commercial Facilities Sector envisions a secure, resilient, and profitable sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security in the public and sustain favorable business environments conducive to attracting and retaining employees, tenants, and customers.

III. Principles of Protective Security

A. **Terrorist Targeting Objectives.** Primary objectives are to inflict casualties (fatalities, injuries, illnesses), to damage/destroy facilities (shut down facility, degrade facility operations, release hazardous material from facility), to disrupt facility operations (interfere with operations, contaminate facility products), and theft (materials, equipment, products, information).
B. **Specific Terrorist Threats**. Threats include explosives, arson, biological agents introduced into the facility, chemical agents introduced, radiological material introduced, hostage taking, automatic weapons or grenade attack, and theft of proprietary or sensitive information.
C. **Impacts and Effects of an Attack**. A high number of casualties could ensue not only from the attack itself but from structural collapse, smoke/dust inhalation, and stampeding crowds. Emergency response teams and law enforcement personnel could become monopolized. Facility owners, insurance companies, and local industries would face economic losses; the city/state would face lost jobs and incoming revenue; and Americans nationwide would face psychological impact.

IV. DHS Reports. DHS has developed three types of reports for each infrastructure and facility category in order to increase awareness and improve understanding. Integrated reports for each facility category are available for download at https://cvpipm.iac.anl.gov.

A. **Characteristics and Common Vulnerabilities.** This report focuses on common characteristics, components, and applicable standards for each infrastructure/facility category; consequences of events; and common vulnerabilities.
B. **Potential Indicators of Terrorist Activity.** This report focuses on terrorist targeting objectives and activity indicators for each infrastructure/facility category.
C. **Protective Measures.** This report focuses on increasing awareness, reducing vulnerabilities, and enhancing defense for each infrastructure/facility category.

V. Common Vulnerabilities

A. Definition. Common vulnerabilities to terrorist activity have *generally* been observed or are known to *generally* exist within an infrastructure category. Critical infrastructures and key assets vary in many characteristics and practices relevant to specifying vulnerabilities. There is no universal list of vulnerabilities that applies to all assets of a particular type within an infrastructure category. "Common" vulnerabilities should be interpreted as having a high likelihood of occurrence, but not as applying to each and every individual facility or asset.

B. Common Vulnerabilities: Hotels. Vulnerabilities for hotels include guest drop-off and pick-up points that may not distant enough to mitigate blasts from explosives in vehicles, parking garages that may have open access to the public with little to no screening, and a limited security force

VI. Potential Indicators of Terrorist Activity

A. Definition. Potential Indicators of surveillance may include: (1) persons discovered with a suspicious collection of casino/hotel maps, photos, or diagrams with facilities highlighted; (2) personnel being questioned off-site about practices pertaining to the facility or the facility's supporting infrastructure (e.g., electricity and natural gas lines); (3) theft of employee or contractor ID cards or uniforms; and (4) a noted pattern or series of false alarms requiring a response by law enforcement or emergency services. Observable anomalies or incidents that may be indicators of an imminent attack include: (1) persons in crowded areas wearing unusually bulky clothing; (2) unattended vehicles illegally parked near entrance, exit areas, or places where large numbers of patrons gather; (3) unattended packages (e.g., backpacks, briefcases, boxes or luggage); and (4) indications of unusual substances near air intakes.

VII. Protective Measures

A. Definition. Protective Measures include: (1) designating a security director and conducting threat analyses, vulnerability assessments, consequence analysis, risk assessments and security audits on a regular basis; (2) developing and implementing a security plan for computer hardware and software; (3) conducting background checks on employees and incorporating security awareness into employee training programs; (4) access control via photo identification badges for employees; (5) installing building perimeter barriers, such as flower pots, fences, bollards, shallow ditches, and high curbs; (6) installing and monitoring CCTV systems); (7) installing systems that provide communication with all people at the facility and can work in concert with law enforcement and emergency responders; and (8) identifying alternate rallying points for coordinated evacuations.

VIII. DHS Protective Programs

A. **Protective Security Advisors (PSAs).** PSAs are assigned to local communities throughout the U.S. They serve as DHS liaisons between the private sector and Federal, State, Territorial, local, and tribal governments. PSAs assist in identifying critical infrastructure and key resource assets. They coordinate requests by the private sector for DHS services and resources, including training requests, scheduling of Site Assistance Visits, and Buffer Zone Protection Program implementation.

B. **Site Assistance Visits (SAVs).** SAVs are visits to critical infrastructure facilities led by DHS protective security professionals, in conjunction with subject-matter experts and local law enforcement. SAVs are designed to facilitate vulnerability identification and mitigation discussions between DHS and the facility in the field. The focus of the SAV is evolving from vulnerability to a broader risk-based assessment by analyzing consequences and incorporating threat scenarios.

C. **FEMA 452.** The FEMA 452 risk assessment methodology is founded on conducting an asset value assessment, threat identification and rating, vulnerability assessment, and coming up with mitigation options to reduce the highest risk then making risk management decisions. The threat types currently addressed in FEMA 452 include explosive blast and CBR attacks. FEMA 452 is being updated to include floods, high winds, and earthquakes.

D. **Homeland Security Information Network (HSIN).** HSIN is a secure portal that provides a "peer to peer" collaboration space for members to engage in real-time. The eight subsectors each have their own subportal within the CF Sector portal. Resources available on HSIN include Joint Information Bulletins issued by DHS and the FBI.

E. **"Protect Your Workplace" Campaign.** "Protect Your Workplace" is a poster campaign designed to build security awareness among the American workforce. The four posters offer various physical and cyber security guidelines. Since 2006, more than 105,000 posters and brochures have been downloaded from the US-CERT Web site (www.us-cert.gov/reading_room/distributable.html), reaching more than 20,000 workplaces.

F. **Protective Measures Course.** The 2-day Protective Measures Course is offered to Executive Level and Employee Level Personnel in the private sector and is designed to provide students with the knowledge to identify vulnerabilities and select appropriate Protective Measures for their unique facility

G. **Surveillance Detection Course.** Surveillance Detection training is intended for security managers, security/safety staff, managers, supervisors and operators. Attendance is open for law enforcement personnel; however the majority of the students should represent personnel assigned to CI/KR. This 3-day Surveillance Detection (SD) course provides a guideline for mitigating risks to critical infrastructure through developing, applying, and employing SD protective measures by developing a SD plan. Instructors explain how this protective program can be applied to detect and deter potential threats to critical infrastructure and key resources (CI/KR) as well as the fundamentals for detecting surveillance activity. Students apply skills such as Vulnerability and Red Zone Analysis, Surveillance Detection and Observation and Reporting during practical exercises throughout the course.

H. Counterterrorism Awareness Workshop. This workshop is designed to improve the knowledge of Private Sector security professionals by providing exposure to key elements of soft target awareness, surveillance detection, and improvised explosive device (IED) recognition. The workshop training materials enhance and reinforce participants' knowledge, skills, and abilities related to preventing, protecting against, responding to, and recovering from terrorist threats and incidents. This workshop reviews the current development of strategies requiring collaboration of numerous agencies across multiple localities, disciplines and level of government. The workshop outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks.

I. Active Shooter Awareness Materials. The Commercial Facilities Sector produced a simple guide, a break-room poster, and wallet-sized business cards that have immediate actions to take in the event of an active shooter. The Materials have been developed with input from the Emergency Services Sector, the Office for Bombing Prevention, our Sector Coordinating Council, and the Sector Coordinating Council for the Emergency Services Sector.

J. Bomb Making Materials Program (BMAP) Suspicious Behavior Awareness Cards. Originally designed for the Retail Subsector, these joint FBI-DHS private sector advisory cards offer memorable and concise tips and images on how to identify and report home made explosive and IED precursor materials and suspicious behavior.

K. Safety Act. The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) was enacted as part of the Homeland Security Act of 2002. It is intended to facilitate the development and deployment of anti-terrorism technologies by creating systems of "risk management" and "litigation management." Protections apply only to claims arising out of, relating to, or resulting from an act of terrorism. Benefits of Safety Act designation include exclusive action in Federal court, no joint and several liability for non-economic damages, no punitive damages or prejudgment interest, and plaintiff recovery reduced by amounts from collateral sources. The SAFETY Act application kit with instructions and forms may be found and completed at **www.safetyact.gov**. This site also contains information on the SAFETY Act statute and other reference materials.

L. Protected Critical Infrastructure Information (PCII) Program. The PCII Program is designed to enhance information sharing between private sector and government. Info designated as PCII is protected throughout its lifecycle. Protection extends to drafts and copies of the PCII retained by the submitter(s) or person working with the submitter(s), as well as any discussions with DHS regarding the PCII. PCII Program safeguards ensure that PCII is: (1) accepted only by authorized and properly trained individuals; (2) used appropriately for analysis of threats, vulnerabilities, and other homeland security purposes; (3)protected from disclosure under FOIA and other similar State and local disclosure laws; and (4) not used directly in civil litigation nor as the basis for regulatory action. PCII is only shared directly through the PCII Program Office,

or through DHS field representatives and other Federal agencies that are designated to receive PCII by the PCII Program Manager.

IX. *Protective Measures Guide for the U.S. Lodging Industry*. Commercial Facilities has previously with members of the Sports Leagues and Public Assembly Subsectors to publish *Protective Measures Guide for U.S. Sports Leagues* in January 2008, which provides an overview of protective measures that can be implemented to assist sports teams and owners/operators of sporting event facilities in planning and managing security at their facilities. Now The Commercial Facilities Sector is working with its Lodging Subsector partners to develop *Protective Measures Guide for the U.S. Lodging Industry*.

The Lodging Guide would not only help us to become more familiar with the operating and security procedures of the lodging industry, it would ideally serve as a general reference guide by which lodging facilities without robust protective measures and/or emergency action plans in place may benefit from the expertise of their industry partners. Previously, for the Sports League Guide, Sports Leagues and Public Assembly Subsector members contributed their security guides and protective measure recommendations to the effort. The final publication was a compilation of those materials, intended for reference and guidance purposes only, labeled For Official Use Only and professionally printed by DHS as a resource exclusively for participating subsector members.

X. Conclusion.

A. Contact Information:

Bill Schweigart
Program Analyst, Commercial Facilities Sector
Office of Infrastructure Protection
U.S. Department of Homeland Security
(703) 235-2852
Bill.Schweigart@dhs.gov