SPORT VENUE SECURITY: PLANNING AND PREPAREDNESS FOR TERRORIST-RELATED INCIDENTS

STACEY HALL, PHD, THE UNIVERSITY OF SOUTHERN MISSISSIPPI
LOU MARCIANI, EDD, THE UNIVERSITY OF SOUTHERN MISSISSIPPI
WALTER COOPER, EDD, THE UNIVERSITY OF SOUTHERN MISSISSIPPI

INTRODUCTION

American sports events are susceptible to various threats, such as terrorism, natural disasters, and fan violence (Fried, 2005; Lipton, 2005). Previous research indicates that terrorism is a concern for sport venue managers (Baker, Connaughton, Zhang, & Spengler, 2007). Researchers have reported that there is a lack of security personnel training at sport stadiums relative to guarding against terrorism (Baker et. al, 2007; Cunningham, 2007; Phillips, 2006; Phillips, Hall, Marciani, & Cunningham, 2006). With the uncertainty of terrorist actions and fan behavior, it is impossible to ensure a risk-free environment at sports venues. It is therefore a matter of how one prepares, responds, and recovers to mitigate the consequences of emergencies (Schwab, Eschelbach, & Brower, 2007). Terrorist activity indicators, common sport venue vulnerabilities, and protective facility security measures will be presented to aid sport venue managers in their operational planning and preparedness for emergency incidents.

TERRORISM

The Federal Bureau of Investigation (FBI) defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives" (WMD Threat and Risk Assessment Manual, 2005, p. 2-4). Organized terrorism has two distinct goals: inflicting the maximum amount of humiliation and publicizing the terrorists' cause to the widest possible audience (Spangler, 2001). Those involved in terrorist activity do so to achieve some type of objective such as gaining recognition, coercion, intimidation, and/or provocation (WMD Threat and Risk Assessment Manual, 2005). According to Arquilla, Ronfeldt, and Zanini (1999), the phenomenon of terrorism appeals to its perpetrators for three principal reasons: (1) to harm and defeat superior forces; (2) to assert identity and command attention; and (3) to achieve a new future order by trying to wreck the present. Motivations are a key factor when trying to determine whether a group or individual will commit an act of terrorism. The FBI identified five categories of threat motivations: (1) political, (2) religious, (3) racial, (4) environmental, and (5) special interest (WMD Threat and Risk Assessment Manual, 2005). Religiously-motivated terrorists are considered to be the most dangerous because of their fanaticism and willingness to die for their cause (Kennedy, 2006).

Terrorists tactics are only limited to the their imagination (Johnson, 2005). Conventional means such as knives, guns, and bombs are frequently used. However, the probability of terrorists using weapons of mass destruction (chemical, biological, radiological, nuclear, or explosives) has significantly increased in the past decade (National Strategy for Combating Terrorism, 2003). Recent worldwide events, like the October 2001 mailings of anthrax-tainted letters in the United States and the release of sarin gas in a Tokyo Subway in 1995, signify that weapons of mass destruction are now real-world risks (Sidell, Patrick, Dashiell, Alibek, & Layne, 2002). Suicide terrorism has also become an effective means for terrorists to achieve their goal of mass casualties and mass

humiliation. Suicide attacks accounted for 3% of all terrorist attacks from 1980 to 2003, but were responsible for 48% of all fatalities (Kennedy, 2006).

According to Johnson (2005), "perhaps no time in history has seen so much effort and so many resources dedicated to terrorism preparedness" (p. 6). On November 25, 2002, President George W. Bush signed the Homeland Security Act of 2002. The Act created the Nation's 15th cabinet-level Department of Homeland Security (DHS), consolidating 22 existing entities with homeland security missions (The National Strategy for Homeland Security, 2002). The administration "reorganized in a very dramatic fashion – called by many the largest federal reorganization in more than fifty years" (Cwiek, 2005, p. 9). For the first time in United States history, the reorganization established a single federal department whose primary mission is to protect the United States from terrorist threats.

THE TERRORIST THREAT TO SPORTS

Since terrorists follow the motto of mass casualties and mass exposure of humiliation, large scale sporting events provide a potential target for terrorist activity. In fact, "Al-Qaeda's Manual of Afghan Jihad proposed football stadiums as a possible terrorist attack site, and the FBI issued an alert in July [2002] warning that people with links to terrorist groups were downloading stadium images" (Estell, 2002, p. 8). In March 2005, the Department of Homeland Security identified a dozen possible strikes it viewed most devastating, "including detonation of a nuclear device in a major city, release of sarin nerve agent in office buildings and a truck bombing of a sports arena" (Lipton, 2005, p. A-1). Additionally, the Department of Homeland Security developed a National Planning Scenarios (2005) document to examine potential threat scenarios to the United States. The document specifically addressed the potential of a biological attack on a sports arena, stating that the spreading of pneumonic plague in the bathrooms of a sports arena would potentially kill 2,500 people.

The most notable sport-related terrorist incidents include the 1972 Munich Olympics and the Centennial Olympic Park bombing at the 1996 Atlanta Games. According to Spangler (2001), terrorists perceive the Olympics as a huge target because it is sponsored by international corporations that symbolize American capitalism and are attended by political leaders from other nations that support the American political agenda. There have been less serious incidents at U.S sport stadiums/arenas. Minutes after a bomb threat was made against Continental Airlines Arena in June 2003 during Game 5 of the NBA Finals, police found 10 cars on fire in the Arena parking lot (SI.com, 2003). More recently, an Oklahoma University student killed himself by prematurely detonating a bomb strapped to his body outside an 84,000 packed stadium in October 2005 (Hagmann, 2005). In October 2006, the National Football League received a dirty bomb threat indicating the use of radiological bombs at seven NFL stadiums (Associated Press, 2006).

POTENTIAL CONSEQUENCES

According to Michael Chertoff, Secretary of Homeland Security, "the consequence of another terrorist incident would far outweigh the cost of investing in back-up systems, alternative operating locations, and additional protective measures" (Philpott, 2007a). The consequences of an incident at a sports event could result in mass casualties and destruction of buildings and infrastructure. Targeting sports can negatively affect future attendance at sports events, subsequently decreasing ticket sales and the demand for airline, travel, tourism, lodging, dining, and recreation services, as experienced after 9/11 (Sauter & Carafano, 2005). Additionally, the target site faces the problem of reengineering sport programs and ensuring continuity of operations by relocating, rebuilding facilities, rescheduling games, and assisting with the displacement of players and employees. These recovery operations are similar to those implemented post Katrina for sport programs in the southern Mississippi and Louisiana region (Steinbach, 2006). The economic aftershock of an attack could have a ripple effect throughout the country ultimately halting a multi-billion dollar industry. Although sport is not

recognized as an official industry in the Census Bureau North American Classification System (Howard & Crompton, 2005), the total economic activity related to sport in the U.S was estimated at $213 billion (Sport Business Journal, 1999) at the beginning of 2000. The financial cost could be catastrophic to the sport organization and the U.S sports industry through the potential loss of revenue streams. The 9/11 attacks cost New York City economy $83 billion and the total U.S. economy in excess of $100 billion (Sauter & Carafano, 2005). Furthermore, the U.S. sporting industry may witness a paradigm shift towards security standards and regulations for sports events, as proposed by Hall (2006), and currently in practice in Britain. British sporting authorities established and published the *Guide to Safety at Sports Grounds* (1997), to which facilities must adhere for operational acceptance and inclusion in safety certificates.

To effectively secure a sport facility may be very cost-prohibitive. The average college athletic department budget would not lend itself to implementing extreme security measures, such as antiterrorism squads and bioterrorism detection equipment (Pantera, M.J. III, Accorsi, R., Winter, C., Gobeille, R., Griveas, S., Queen, D., Insalaco, J., & Domanoski, B., 2003). For example, security at the Utah Winter Olympics cost $300 million and the 2002 Super Bowl in New Orleans $6 million (Iwata, 2002). Even at the professional level, increased security has received some opposition. The mandatory pat-downs recently implemented by the National Football League have created some controversy for the Tampa Bay Buccaneers who requested that taxpayers absorb the extra $9,597 per game for security (Snel, 2005). Sport venue managers face the problem of financing security improvements and may find that the cost of implementing security initiatives diverts investment from more plausible areas, such as new facilities, better coaches, and athlete recruitment. However, it can be argued that good countermeasures and contingency planning can protect sports activities from disruption and financial burden, and ultimately enhance spectator confidence.

SPORT VENUE SECURITY

There are approximately 1,347 sport stadiums and arenas in the United States, excluding high school stadiums and other small venues (worldstadiums.com, 2006). These stadiums may be used for other functions besides sports events, such as graduations, concerts, or political events. Facility ownership and location also varies. Facilities may be privately or publicly owned and located in major cities, small towns, and on college campuses (DHS, 2007). The Department of Homeland Security has identified sport stadiums/arenas as a key asset in the critical infrastructure/key resource sector (Office of Domestic Preparedness Information Bulletin, 2003). Key assets are defined as individual targets whose destruction "could create local disaster or profoundly damage our Nation's morale or confidence" (CRS Report for Congress, 2004).

Sport venue managers and spectators perceive terrorism as a foreseeable threat to U.S. sport facilities and believe it is only a matter of time before they are attacked (Baker et. al, 2007; Phillips et al., 2006). However, it has been documented that some facilities are lacking in terms of staff training related to terrorism (Baker et al., 2007; Cunningham, 2007; Phillips, 2006). Since 9/11, sport venue managers realize their security policies and procedures need to be reviewed and have requested help regarding access to timely security information, assistance in conducting vulnerability assessments, and the provision of training for emergency response planning (Baker et. al, 2007; Phillips, 2006).

Security operations vary across facilities depending on location, ownership, and extent of use. Over 60% of the security personnel employed for game day operations at Division I-A and I-AA collegiate programs in the U.S. are outsourced (Phillips, 2006). Close to one-third of professional sport stadiums fail to perform background checks on part-time staff and less than 10% of those responsible for security at major university athletic facilities check all part-time staff. There was also a difference in screening of full-time staff. Eighty-eight percent of professional stadiums and arenas check all full-time staff compared to 27 percent at major college facilities (Gips, 2003).

TERRORIST INDICATORS

Specific terrorist threats, such as explosives, suicide bombers, arson, WMD agents, hostage taking, and active shooters, are a major concern to sport stadiums and arenas (Estell, 2002; Kennedy, 2006; Lipton, 2005; National Strategy for Combating Terrorism, 2003; National Planning Scenarios, 2005; Philpot, 2007a). According to Baker et al. (2007), designated security personnel should be trained to recognize potential terrorism threats and how to respond to such threats. It is therefore imperative that sport event managers are aware of the potential indicators of terrorist activity presented by Kennedy (2006). The seven signs of terrorist activity are: (1) surveillance, (2) elicitation, (3) tests of security, (4) acquiring supplies, (5) suspicious persons, (6) trial run, and (7) deploying assets. These signs are discussed below:

Surveillance: someone may observe the target area to determine the strengths and weaknesses, and number of personnel that might respond to an incident. It is therefore important to take note of anyone recording activities, taking notes, or using video/camera/observation devices.

Elicitation: involves individuals attempting to gain information about certain operations. For example, terrorists may acquire knowledge about a stadium structure and the location of security personnel during game time.

Test of Security: usually conducted to measure reaction times to breaches of security and to test physical security barriers for weaknesses. For example, individuals trying to access unauthorized areas of your facility.

Acquiring Supplies: someone has purchased or stolen explosives, weapons, or ammunition near your site; this may also include acquiring security passes or uniforms that make it easier for entrance to prohibited areas of your facility.

Suspicious People: this may be someone on your staff that does not fit in because of their unusual behavior, language usage, or unusual questions they are asking.

Trail Run: before the final attack, terrorist normally conduct a “dry run” to address any unanticipated problems. This may include recording emergency response times.

Deploying Assets: people and supplies are getting in position to commit the act. This is the final sign and last chance to thwart an attack.

COMMON VULNERABILITIES

Today’s terrorists can strike anywhere at anytime with a variety of weapons. Vulnerable facilities include government buildings, hospitals, restaurants, malls and sports arenas (Philpott, 2007b). In order for sport venue managers to effectively improve security measures at their respective sites they must first identify vulnerabilities in their security systems (National Infrastructure Protection Plan, 2006). A vulnerability is defined as an exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person (General Security Risk Assessment Guideline, 2003). In January, 2005, the Department of Homeland Security launched the first on-line Vulnerability Self-Assessment Tool (ViSAT) for large stadiums. The tool incorporates industry safety and security best practices for critical infrastructure to assist in establishing a security baseline for each facility. It focuses on key areas such as information security, physical assets, communication security, and personnel security (DHS.gov, 2005). Site-specific conditions to consider when assessing vulnerabilities are presented in Table 1 (U.S. Department of Homeland Security, 2004).

In the aftermath of 9/11, most leagues, teams, and venues conducted threat assessments and updated security practices (Hurst, Zoubek, & Pratsinakis, n.d.). Hall et al. (2007) identified common vulnerabilities at collegiate sport venues. These included:

- Lack of emergency and evacuation plans specific to sport venue;
- Inadequate searching of venue prior to event;
- Inadequate searches of fans and belongings;
- Concessions not properly secured;
- Dangerous chemicals stored inside the sport venue;
- No accountability for vendors and their vehicles; and
- Inadequate staff training in security awareness and response to Weapons of Mass Destruction (WMD) attacks.

PROTECTIVE MEASURES

Protective security measures include resources and procedures designed to protect a facility against threats and to mitigate the consequences of an attack. Protective measures are designed to promote the DHS strategy to effectively prevent, prepare, respond, and recover from terrorist attacks (National Strategy for Homeland Security, 2002). A number of associations and organizations are concerned with facility security, including the World Council for Venue Management, International Association of Assembly Managers, and sport league governing bodies such as the NFL, NBA, and NCAA. These entities issue security guidelines or "best practices" for their members. For example, NFL teams have planned and practiced various disaster scenarios (Pantera et. al, 2003); the National Hockey League conducts monthly security audits; and the National Basketball League follows strict bomb emergency procedures (Iwata, 2002). However, these guidelines are not always mandatory. The lack of mandatory guidelines results in varying degrees of security at each facility across the United States.

General protective security measures promoted by the Department of Homeland Security (Homeland Security Information Bulletin, 2003) can be categorized into four different areas: (1) Communication and Notification, (2) Planning and Preparedness, (3) Access Control, and (4) Surveillance and Inspection (see Table 2). Sport-specific security measures being shared as "best practices" by the Department of Homeland Security include: (1) conducting security assessments, (2) increasing perimeter security, (3) enhancing detection monitoring capabilities, (4) establishing access control, and (5) reinforcing employee procedures to ensure knowledge of emergency protocol (DHS.gov, 2004). Furthermore, Hall et al. (2007), during their research of college sport venue security, recommended the following countermeasure improvements: (1) identify a sports event security action team (SESAT) to organize and communicate security efforts on campus; (2) initiate a responsible vendor program with adequate identification, access control, and training; 3) encourage participation in an information sharing analysis center (ISAC); and 4) developing and exercising emergency and evacuation plans.

CONCLUSION

Catastrophic incidents, including 9/11, serve as constant reminders that sporting venues are vulnerable to man-made disasters, resulting in significant damage to property and loss of life. Sport organizations must act in a professionally and prudent manner by fulfilling their legal responsibility to provide a safe environment for spectators, officials, players, and surrounding community. According to Hurst, Zoubek, and Pratsinakis (n.d.), regardless of the analysis conducted after an incident, "the fundamental question will always be whether or not reasonable steps were taken to protect against an incident in light of the availability of security measures, the industry "standards' for security, and the potential threat of terrorism" (p. 5). Assessing risk, reducing vulnerabilities, and increasing the level of preparedness will help minimize potential threats to sport venues

nationwide. Sport venue managers must be familiar with terrorist activity indicators, common sport venue vulnerabilities, and possible protective security measure improvements.

REFERENCES

Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). Networks, netwar, and information-age terrorism. In Lesser, I.O., Hoffman, B., Arquilla, J., Ronfeldt, D., & Zanini, M. *Countering the new terrorism* (pp. 39-84). Santa Monica, CA: Rand Corporation.

ASIS International. (2003). *General security risk assessment guideline.* [On-line]. Available: http://www.asisonline.org/guidelines/guidelinesgsra.pdf.

ASIS International (2005). *Business continuity guideline.* [On-line]. Available: http://www.asisonline.org/guidelines/guidelinesbc.pdf.

Associated Press (2006, October 19). Homeland security: NFL stadiums threat not credible. *ESPN.com*. Retrieved from http://sports.espn.go.com/nfl/news/story?id=2631048.

Baker, T.A., Connaughton, D., Zhang, J.J., & Spengler, J.O. (2007, Winter). Perceived risk of terrorism and related risk management practices of NCAA Division IA Football Stadium Managers. *Journal of Legal Aspects of Sport, 13*(2), 145-179. Available: www.lexisnexis.com.

CRS Report for Congress. (2004, October 1). *Critical infrastructure and key Assets: Definition and identification.* [On-Line]. Available: http://www.fas.org/sgp/crs/RL32631.pdf.

Cunningham, G. (2007). *Security management capabilities in intercollegiate athletic departments.* Unpublished doctoral dissertation. The University of Southern Mississippi.

Cwiek, M.A. (2005). America after 9/11. In Ledlow, G.R., Johnson, J.A., & Jones, W.J. (Eds.), *Community preparedness and response to terrorism: Vol. 1. The terrorist threat and community response,* (pp. 7-21). Westport, CT: Praeger Perspectives.

Department of Homeland Security. (2004, July 23). *Department of Homeland Security hosts security forum for sports executives.* Office of the Press Secretary. Retrieved from http://dhs.gov/dhspublic/displaycontent=3863.

Department of Homeland Security. (2005, January 7). *Homelands Security launches first online tool assessing stadium vulnerabilities.* Office of the Press Secretary. Retrieved from http://www.dhs.gov/xnews/releasespress_release_0584.shtm.

Department of Homeland Security. (2007). *Homeland security planning for campus executives.* Morgantown, WV: VMC/Homeland Security Programs.

Estell, L. (2002). A banner year for stadiums? Security concerns could put an end to stadium fly-overs. *Incentive,* 176 (12), 8. Available: www.ebscohost.com.

Fried, G. (2005). *Managing sports facilities*. Champaign, IL: Human Kinetics.

Gips, M. (2003). Survey assesses sports facility security. *Security Management Online*. Available: www.securitymanagement.com.

Guide to Safety at Sports Grounds (1997). London: The Stationary Office.

Hagmann, D.J. (2005, October 30). Black hole in America's heartland. *Northeast Intelligence Network*. Retrieved from http://www.homelandsecurityus.com/site/modules/news/article.php?storyid=16.

Hall, S. (2006, Fall). Effective security management of university sport venues. The *Sport Journal, (9)* 4. Retrieved from http://www.thesportjournal.org/article/effective-security-management-university-sport-venues.

Hall, S., Marciani, L., & Cooper, W.E, & Rolen, R. (2007, August). Securing sport stadiums in the 21st century: Think security, enhance safety. *Homeland Security Institute: Journal of Homeland Security. Retrieved from http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=162.*

Homeland Security Information Bulletin. (May 15, 2003). *Potential indicators of threats involving vehicle borne improvised explosive devices*. [On-Line]. Available: http://www.esisac.com/publicdocs/Other_Advisories/DHS%20Bulletin%20VBIED1.pdf.

Howard, D.R., & Crompton, J.L. (2005). *Financing sport* (2nd ed.). Morgantown, WV: Fitness Information Technology, Inc.

Hurst, R., Zoubek, P., & Pratsinakis, C. (n.d.). *American sports as a target of terrorism: The duty of care after September 11th*. [On-Line]. Available: www.mmwr.com/_uploads/UploadDocs/publications/American%20Sports%20As%20A%20Target%20Of%20Terrorism.pdf.

Iwata, E. (2002, March 17). Stadium security gets serious. *USATODAY.com*. Retrieved from http://usatoday.com/money/general/2002/03/18/stadiums-security.htm.

Jane's Chem-Bio Handbook (2nd ed.). (2002). Texas Department of Public Safety. Jane's Information Group.

Johnson, J.A. (2005). A brief history of terrorism. In Ledlow, G.R., Johnson, J.A., & Jones, W.J. (Eds.), *Community preparedness and response to terrorism: Vol. 1. The terrorist threat and community response* (pp. 1-6). Westport, CT: Praeger Perspectives.

Kennedy, D.B. (2006). A précis of suicide terrorism. *Journal of Homeland Security and Emergency Management, (3)*4.

Lipton, E. (2005, March 16). U.S. report lists possibilities for terrorist attacks and likely toll. *New York Times, Section A, Page 1, Column 2.*

Office of Domestic Preparedness Information Bulletin (October 1, 2003). *Critical infrastructure protection funds*. [On-Line]. Available: http://ojp.usdoj.gov/odp/docs/info84.htm.

Pantera, M.J. III, Accorsi, R., Winter, C., Gobeille, R., Griveas, S., Queen, D., Insalaco, J., & Domanoski, B. (2003). Best practices for game day security at athletic & sport venues. *The Sport Journal*, *6* (4). [On-Line]. Available: http://www.thesportjournal.org/article/best-practices-game-day-security-athletic-amp-sport.

Phillips, D., Hall, S., Marciani, L., & Cunningham, G. (November, 2006). *Sport event security: How does it relate to customer satisfaction and marketing?* Paper presented at The Sports Marketing Association Annual Conference, Denver, CO.

Phillips, J. (2006). *An analysis of security outsourcing at NCAA DI A and DI AA collegiate football games.* Unpublished manuscript. The Center for Spectator Sports Security Management, Hattiesburg, MS.

Philpott, D. (2007a). Business resiliency handbook. *Journal of Homeland Defense: Special Report.* [On-Line]. Available: http://www.homelanddefensejournal.com/hdl/BusinessResiliency.htm

Philpott, D. (2007b). How your facility can avert a terrorist attack. *Journal of Homeland Defense: Special Report.* [On-Line]. Available: http://www.homelanddefensejournal.com/hdl/TerroristAttack.htm.

Sauter, M.A., & Carafano, J.J. (2005). *Homeland Security: A complete guide to understanding, preventing, and surviving terrorism*. New York: McGraw Hill.

Sidell, F.R., Patrick, W.C., Dashiell, T.R., Alibek, K., & Layne, S. (2002). *Jane's Chem-Bio Handbook (*2nd ed.). Alexandria, VA: Jane's Information Group.

SI.com (June 14, 2003). Arena targeted, cars aflame in parking lot after bomb threat at finals. Retrieved from http://sportsillustrated.cnn.com/basketball/nba/2003/playoffs/news/2003/06/13/arena_nets_ap/.

Snel, A. (2005, September 15). Sports authority, Bucs dispute cost of NFL rule; Most teams pay for security. *Tampa Tribune. Available*: www.ebscohost.com.

Spangler, J. (2001, September 30). Meeting the threat. *Deseretnews.com*. Retrieved from http://deseretnews.com/dn/sview/1,3329,320006966,00.html.

SportsBusiness Journal (1999, December 20-26). The making of the $213 billion sports business industry, 24-25.

Swab, A.K., Eschelbach, K., & Brower, D.J. (2007). *Hazard mitigation and preparedness.* Hoboken, NJ: John Wiley & Sons, Inc.

Steinbach, P. (2006, September). Storm: A year removed from the dark days of hurricane Katrina, college athletic departments are now being viewed in a new light – as disaster response specialists. *Athletic Business*, *30*(6), 38-46.

U.S. Department of Homeland Security. (2002, July). *National strategy for homeland security.* Washington D.C. [On-line]. Available: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

U.S. Department of Homeland Security. (2003, February). *National strategy for combating terrorism.* Washington D.C. [On-Line]. Available: http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/counter_terrorism_stratgey.pdf.

U.S. Department of Homeland Security. (2004). *Campus preparedness assessment manual*. Washington D.C.

U.S Department of Homeland Security. (April, 2005). *National planning scenarios executive summary*. [On-Line]. Available: http://cees.tamiu.edu/covertheborder/TOOLS/NationalPlanningSen.pdf.

U.S. Department of Homeland Security. (2006). *National infrastructure protection plan.* Washington D.C. [On-Line]. Available: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Worldstadiums.com. (2006). Stadiums in the United States. Retrieved from http://www.worldstadiums.com/north_america/countries/united_states.shtml.

WMD Threat and Risk Assessment (Local Jurisdiction). (2005, January) (3rd ed.). College Station, TX: Texas Engineering Extension Service (TEEX).

TABLE 1

SUMMARY OF CONDITIONS TO CONSIDER FOR ASSESSING VULNERABILITIES

Emergency Preparedness	External Environment	Parking
response plan response capabilities	surrounding areas lighting around property type of traffic in vicinity	controlled lots for visitors standoff from facility lighted areas
Access to Property/Buildings	**Building Systems**	**Hazards Present**
controlled security guards background checks number of entrances hours of access cameras/alarms delivery screening visitor management	HVAC intakes air, water, utility intakes emergency operations	CBRNE (chemical, biological, radiological, nuclear, explosive)

TABLE 2

PROTECTIVE MEASURES

Communication and Notification
Maintain situational awareness of world events and ongoing threats
Encourage personnel to be alert and report suspicious behavior, packages, or devices
Ensure all personnel are aware of protective measures and changes in threat conditions
Planning and Preparedness
Increase number of visible security personnel wherever possible
Develop or update emergency response and evacuation plans
Develop or update current contingency plans
Conduct internal training exercises with local emergency responders to ensure multi-agency collaboration in executing plans
Establish partnerships with local authorities to develop intelligence and information sharing relationships
Conduct vulnerability studies
Access Control
Arrange exterior vehicle barriers, traffic cones, and road blocks to control access
Limit the number of access points and control ingress and egress from the facility
Strictly enforce access control procedures for secured areas through photo identification
Conduct background checks
Surveillance/Inspection
Increase perimeter lighting
Provide video surveillance systems for facility
Implement mail and package screening procedures
Screen all patrons entering the facility