

The University of Southern Mississippi

STANDARDS FOR EFFECTIVE SECURITY MANAGEMENT OF UNIVERSITY

SPORT VENUES


by

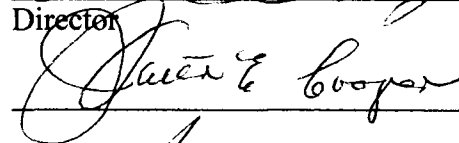
Stacey Ann Hall

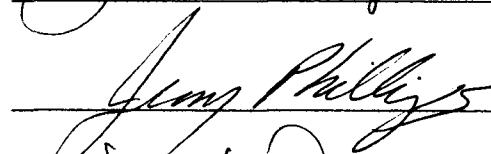
A Dissertation


Submitted to the Graduate Studies Office
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

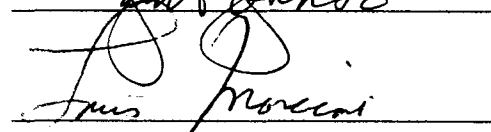
Approved:

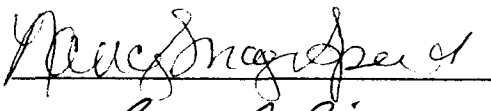

Director

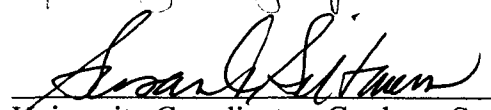












University Coordinator, Graduate Studies

August 2006

UMI Number: 3257011

Copyright 2006 by
Hall, Stacey Ann

All rights reserved.

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI[®]

UMI Microform 3257011

Copyright 2007 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

COPYRIGHT BY
STACEY ANN HALL
2006

The University of Southern Mississippi

STANDARDS FOR EFFECTIVE SECURITY MANAGEMENT OF UNIVERSITY

SPORT VENUES

by

Stacey Ann Hall

Abstract of a Dissertation
Submitted to the Graduate Studies Office
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

August 2006

ABSTRACT

STANDARDS FOR EFFECTIVE SECURITY MANAGEMENT OF UNIVERSITY SPORT VENUES

by Stacey Ann Hall

August 2006

The purpose of this study was to identify standards for effective security management of university sport venues. In March 2005, the Department of Homeland Security identified the truck bombing of a sports arena as a possible terrorist strike. It is imperative that universities take necessary steps to secure their stadiums and campuses against potential threats. Until now, there have been no documented research-based standards for university sport venue security.

The researcher developed standards through a series of interviews and a three-round Delphi study. Purposeful sampling was used to select participants for both the interviews and Delphi panel. Four sport security personnel participated in the interview process and an initial set of standards were developed and used for the Delphi study. The 28 member Delphi panel included the athletic facility manager, campus police chief, local sheriff, and local emergency management director responsible for game day security operations at seven state-supported universities in Mississippi. Importance ratings for developed standards were assessed on a 5-point Likert scale during Round 2 and 3.

The initial interview panel and Delphi panel produced 134 standards in eleven categories: Perimeter Control, Access Control, Credentialing, Physical Protection Systems, Risk Management, Emergency Management, Recovery Procedures,

Communications, Security Personnel, Training, Modeling, and Simulation, and WMD – Toxic Materials Protection. Twenty-two participants successfully completed all three rounds of the Delphi study (78.6%). Standards have now been identified to assist and support university sports event security teams in their quest to protect our most valuable assets – our people!

ACKNOWLEDGEMENTS

I wish to thank all of my committee members: Dr. Walter Cooper, Dr. J.T. Johnson, Dr. Dennis Phillips, Dr. Jerry Phillips, Dr. Lou Marciani, and Dr. Nancy Speed for their time and assistance throughout this research process. I would also like to thank Dr. Walter Cooper and Dr. Lou Marciani for their invaluable guidance and mentorship throughout this process and during my graduate studies at Southern Miss.

I express my sincere love and appreciation to my family at home in Northern Ireland for their continued love, support, and belief in all of my endeavors. Your commitment and encouragement has helped me to achieve more than I could have dreamed. I will continue to strive for excellence and make you proud.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	ii
LIST OF TABLES AND ILLUSTRATIONS	v
CHAPTERS	
I. INTRODUCTION	1
Purpose of the Study	
Research Questions	
Delimitations	
Limitations	
Assumptions	
Definition of Terms	
Justification	
II. REVIEW OF RELATED LITERATURE	13
Terrorism	
Securing the Homeland	
The Terrorist Threat to Sport	
Understanding Risk	
Sports Event Security Management	
Southern Miss Center for Sports Event Security Management	
Standards	
III. METHODS	46
Overview	
The Delphi Method	
Research Design	
Participants	
Instrument	
Procedures	
Data Analysis	
IV. RESULTS.....	53
Research Questions	
Hypothesis	
Interview Responses	
Delphi Study	
Delphi Round 1 Findings	

Delphi Round 2 Findings	
Delphi Round 3 Findings	
IV. SUMMARY OF FINDINGS.....	83
Discussion	
Limitations	
Recommendations for Future Research	
Recommendation for Practice	
Conclusions	
APPENDICES	97
A. IRB Approval	
B. Interview Questionnaire	
C. Letter Requesting Participation for Delphi Study	
D. Delphi Round 1 Survey	
E. Delphi Round 2 Survey	
F. Delphi Round 3 Survey	
G. Comparison of Means between Delphi Round 2 and 3	
H. Standards for Effective Security Management of University Sport Venues	
I. Comparison of Means between Participant Groups after Delphi Round 3	
REFERENCES	154

LIST OF TABLES

Table

1.	Terrorism Motivations	16
2.	Participation Rates for the Delphi Study	56
3.	Participation by Occupation for each Delphi Round	56
4.	Perimeter Control – Round 2 Delphi Responses	58
5.	Access Control – Round 2 Delphi Responses	59
6.	Credentialing – Round 2 Delphi Responses	61
7.	Physical Protection Systems –Round 2 Delphi Responses.....	62
8.	Risk Management – Round 2 Delphi Responses.....	63
9.	Emergency Management – Round 2 Delphi Responses.....	64
10.	Recovery Procedures – Round 2 Delphi Responses.....	66
11.	Communications – Round 2 Delphi Responses.....	66
12.	Security Personnel – Round 2 Delphi Responses.....	67
13.	Training, Modeling, and Simulation – Round 2 Delphi Responses	68
14.	WMD – Toxic Materials Protection – Round 2 Delphi Responses.....	69
15.	Perimeter Control – Round 3 Delphi Responses	70
16.	Access Control – Round 3 Delphi Responses	71
17.	Credentialing – Round 3 Delphi Responses	73
18.	Physical Protection Systems – Round 3 Delphi Responses.....	74
19.	Risk Management – Round 3 Delphi Responses.....	75
20.	Emergency Management – Round 3 Delphi Responses.....	76
21.	Recovery Procedures – Round 3 Delphi Responses.....	78

22.	Communications – Round 3 Delphi Responses.....	78
23.	Security Personnel – Round 3 Delphi Responses.....	79
24.	Training, Modeling, and Simulation – Round 3 Delphi Responses	80
25.	WMD – Toxic Materials Protection – Round 3 Delphi Responses.....	81
26.	Standards for Effective Security Management of University Sport Venues	85

LIST OF ILLUSTRATIONS

Figure

1.	International Terrorist Attacks, 1990 - 2004	19
2.	Anti-U.S. Attacks, 2003	20
3.	U.S. Targets Attacked, 2003	20
4.	Recreational Facilities – Potential Terrorist Targets	28

CHAPTER I

“The homeland is secure when the home town is secure”
(Former Secretary Tom Ridge, Department of Homeland Security)

INTRODUCTION

The tragic events of September 11, 2001, changed America forever. Feelings of fear, loss, shock, disbelief and anger overwhelmed the nation. How could terrorist insurgents easily attack the homeland? The horrific assault on the American people and their way of life stimulated a priority for homeland security and the protection of American values and ideals.

Since 9/11 the American sports industry has increased security at major sporting venues and high profile events such as the Super Bowl, World Series and Olympics. Large public gatherings, such as sports events, that celebrate American popular culture are potential targets of terrorism (Hurst, Zoubek, & Pratsinakis, n.d.). In March 2005, the Department of Homeland Security identified the truck bombing of a sports arena as a possible terrorist strike (Lipton, 2005). University sports venues are no exception to this terrorist threat. Collegiate sports stadiums host thousands of fans each weekend providing a perfect target for mass casualties and extensive media coverage. According to NCAA attendance records, approximately 46 million people attended collegiate football games during the 2003 season (Official NCAA Football Records Book, 2005). It is imperative that universities take necessary steps to secure their stadiums and campuses against potential threats. Assessing risk, reducing vulnerabilities, and increasing the level of preparedness will help minimize potential threats to university sport venues nationwide. Besides terrorism, other potential threats include drug/alcohol usage, fan violence, patron injuries, weather concerns, power failure, and sabotage (Fried, 2005).

American sports leagues, teams, and venue operators must realize the risk of complacency and continue to plan, test, and enhance security efforts. The National Football League (NFL) is an excellent example of a sporting organization that embraced security measures after 9/11 by providing security guidelines to their league members. The NFL “created a security task force and issued to teams a “best practices guide” of recommended security measures” (Hurst, Zoubek, Pratsinakis, n.d., p. 3). Collegiate sport programs need to develop and implement similar guidelines to ensure effective security management measures are in place. According to Goss, Jubenville, & MacBeth (n.d.), sport facility managers face two types of terror: organized terror and spontaneous terror. Organized acts of terror are planned over a long period of time and are usually rehearsed, versus spontaneous or unpredictable acts of terror such as fans attacking officials and players.

Unfortunately, the sporting world has already been victim to terrorist attacks. “In 1972, a Palestinian group seized Israeli athletes inside the Olympic village in Munich, leading to the death of 11 Israelis and some of the terrorists” (Bierbauer, 1996, ¶ 2). In 1996, a domestic terrorist bombed The Centennial Olympic Park at the Atlanta Games killing one person and injuring more than 100 (CNN.com, 1996). Sports venues are also faced with unexpected acts of violence. For example, in 2002, a father and son ran from the baseball stands to attack Kansas City Royal first base coach Tom Gamboa (Syken, 2002). More recently, in November 2004, basketball fans and players were involved in a scuffle at an Indian Pacers-Detroit Pistons game. This incident has been referred to as the worst brawl in NBA history (ESPN.com, 2004). Evidently, there is reason to allocate time, energy, and resources for the planning and prevention of such horrifying incidents.

One problem that sports venue managers face is the ability to determine the potential threat level, “causing leagues, teams and venues to prepare for a range of possible incidents at their facilities and to maintain close contact with federal, state and local law enforcement representatives regarding possible threats” (Hurst, Zoubek, Pratsinakis, n.d., p. 4). The risk assessment process is a way to determine risk and threat levels and identify vulnerabilities. “A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment.” (Decker, 2001, p. 1). These assessments provide vital information for the protection of critical assets against terrorist attacks and other possible threats. Sport venue managers are able to identify vulnerabilities and in turn harden the facility and improve physical protection systems. This may include implementing access controls, CCTV security cameras, lighting, background checks, credentialing, checking backpacks, enhancing communication networks, and developing or updating emergency response and evacuation plans.

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, 2005, p. 2-4). Terrorist objectives include coercion, intimidation, provocation, and recognition. “More often than not, there is extreme resentment of some government or leading group that does not fit within the terrorist’s worldview” (Johnson, 2005, p. 3). Terrorist tactics are only limited to their imaginations, common methods include: bombings, product contamination, hostage-taking, assassination and hijackings (WMD Threat and Risk Assessment, 2005). Recent

terrorist attacks, such as the 1995 sarin gas attack in Tokyo and the Anthrax mailings post 9/11, indicate the terrorists' preference to use chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons (2005).

The United States realized on September 11, 2001, that terrorism was a real threat and posed imminent danger to the American people. As a result, the U.S became a world leader in the global "war on terror" and President George W. Bush signed several critical pieces of legislation into law, including:

- Homeland Security Act of 2002
- USA PATRIOT Act of 2001
- Aviation and Transportation Security Act of 2001
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002
- Enhanced Border Security and Visa Entry Reform Act of 2002
- Maritime Transportation Security Act of 2002 (Progress Report on the Global War on Terrorism, 2003).

According to Johnson (2005), "perhaps no time in history has seen so much effort and so many resources dedicated to terrorism preparedness." (p. 6). The Homeland Security Act of 2002 created the Department of Homeland Security (DHS) to oversee the prevention, detection, deterrence, and recovery efforts from terrorist attacks (The Global War on Terrorism, n.d.). The creation of the DHS is considered the most extensive reorganization of government in over 50 years (Progress Report on the Global War on Terrorism, 2003). The DHS consists of 22 federal entities with a primary mission to protect the American homeland.

The University of Southern Mississippi Center for Sports Event Security Management
(SESM)

The Mississippi Department of Homeland Security (MDHS), in conjunction with the Mississippi Emergency Management Agency (MEMA), awarded The University of Southern Mississippi, School of Human Performance and Recreation, a \$568,000 research grant to create a research-based model for effective security of university sports events. According to Ed Worthington, Director of Mississippi Department of Homeland Security, “sporting events are perfect targets because of the number of people amassed in a relatively small space, and in any nation where sports are held in such high regard, an attack on any scale would likely grab national or even international attention.” (Doyle, 2005, ¶ 3). The grant included monies for vulnerability assessments on all state-supported university campuses in Mississippi, the creation of a Center for Sports Event Security Management (SESM), and the development of curriculum and training materials for certifications. The University of Southern Mississippi subcontracted Security Management Solutions (SMS), an Alabama security firm with expert credentials, to conduct the vulnerability assessments. The partnership assured quality sports stadium assessments in compliance with Homeland Security regulations. SMS identified key personnel at each campus location to include in the assessment team. The Sports Event Assessment Team (SESAT) included representatives from: 1) University Athletic Department, 2) Campus Police Department, 3) Emergency Management Agency, 4) Local Police Department, 5) Sheriff’s Department and, 6) Local Fire Department. A multi-disciplinary team approach is needed to effectively secure a potential terrorist target (WMD Threat and Risk Assessment, 2005). Results from the vulnerability

assessments were used by each institution to make necessary security improvements. The researcher utilized the Center resources, vulnerability assessment participants, and security experts in this study.

Purpose of the Study

The purpose of this study is to establish standards for effective security management of university sport venues. Recent terrorist attacks on U.S. soil and abroad have heightened the need for effective security at sporting venues within a 1 mile radius. Institutions have a responsibility to provide a safe environment for players, fans, officials, vendors, media personnel, and local community. Training personnel and improving physical protection systems will help detect, deter, prevent, and respond to potential threats on university campuses nationwide. Establishing standards will set a security level to be achieved by university sport venue security management teams. This will help provide consistency in security management practices among sport venues.

Research Questions

1. What standards are needed for effective security management of university sport venues?
2. What is the perceived level of importance for the security standards?

Hypothesis

1. Significant differences will exist in perceptions of importance for developed standards between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors.

Delimitations

- Five to seven security experts will be interviewed to gather a preliminary set of

standards.

- The Delphi study will be administered to athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors responsible for game-day security operations at The University of Southern Mississippi, Mississippi Valley State University, Alcorn State University, Delta State University, Jackson State University, The University of Mississippi, and Mississippi State University.
- Participation will be voluntary.
- Interviews and Delphi surveys will be conducted during the fall of 2005 and spring of 2006.
- Interviews and surveys will be delivered by email, mail, or fax.

Assumptions

- Participants will answer the interview and Delphi questions honestly.

Definition of Terms

Assets: any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value (General Security Risk Assessment Guideline, 2003).

Assessment: the evaluation and interpretation of measurements and other information to provide a basis for decision-making (WMD Threat and Risk Assessment, 2005).

Attack: to set upon with violent force – 1 (The American Heritage College Dictionary, 4th Ed., 2002)

Capability: provides the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be delivered with any

combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome (Universal Task List: Version 2.1, 2005).

CBRNE: common acronym pertaining to the five major categories of terrorism incidents: chemical, biological, radiological, nuclear, and explosive weapons or materials (WMD Threat and Risk Assessment).

Critical Asset: any facility, equipment, service or resource considered essential to Department of Defense (DOD) operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical assets may be DOD assets or other government or private assets, domestic or foreign (Department of Defense *Directive*: Number 5160.54, 2003).

Critical Infrastructure: are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private (Presidential Decision Directive 63, 1998)

Defend: to make or keep safe from danger, attack, or harm - 1 (The American Heritage Dictionary, 4th Ed., 2002)

Detect: identify, assess, investigate and communicate terrorist activities, intentions and capabilities in order to preempt and prevent attacks (Universal Task List: Version 2.1, 2005).

Deter: to prevent or discourage the occurrence of an action, as by means of fear or doubt (The American Heritage Dictionary, 4th Ed., 2002).

Emergency: a serious situation or occurrence that happens unexpectedly and demands immediate action - 1 (The American Heritage Dictionary, 4th Ed., 2002).

Emergency Management: organizations that are directed to coordinate preparedness, recovery, and mitigation for CBRNE terrorism incidents at the jurisdiction level (WMD Threat and Risk Assessment, 2005).

Event: something that happens; a noteworthy happening. In the security context, this usually represents an occurrence such as a security incident, alarm, medical emergency, or related episode or experience (General Security Risk Assessment Guideline, 2003).

Homeland Security: the preparation for prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards U.S. territory, sovereignty, domestic population, and infrastructure: as well as crisis management, consequence management, and other domestic civil support (Larsen, McIntyre, & DeMier, n.d.)

Incident: an occurrence or event that interrupts normal procedure or precipitates a crisis - 4 (The American Heritage Dictionary, 4th Ed., 2002).

Infrastructure: manmade physical systems, assets, projects, and structures, publicly and/or privately owned, that are used by or provide benefit to the public. Including utilities, bridges, levees, drinking water systems, electrical systems, communication systems, dams, sewage systems, and roads (National Response Plan, 2004).

Prevent: deter all potential terrorists from attacking America, detect terrorists before they strike, prevent them and their instruments of terror from entering our country, and take decisive action to eliminate the threat they pose (National Strategy for Homeland Security, 2002).

Preparedness: build, sustain and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents (Universal Task List: Version 2.1, 2005).

Protect: reduce the likelihood of attack on assets or systems and limit the impact should an attack occur (Universal Task List: Version 2.1, 2005).

Recover: the development, coordination, and execution of service-and site-restoration plans for impacted communities and the reconstitution of government operations through individual, private-sector, nongovernmental, and public assistance programs (National Response Plan, 2004).

Respond: implement immediate actions to save lives, protect property, and meet basic human needs (Universal Task List: Version 2.1, 2005).

Risk: the possibility of loss resulting from a threat, security incident, or event (General Security Risk Assessment Guideline, 2003).

Risk Analysis: a detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks (General Security Risk Assessment Guideline, 2003).

Risk Assessment: the process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel (General Security Risk Assessment Guideline, 2003).

Risk Management: is a systematic and analytical process to consider the likelihood that a

threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack (Decker, 2001)

Security: can include the process of safeguarding an item, person, or place (Fried, 2005).

Standards: a written, or visual measurable guideline describing expected behavior, performance, product or service (Thurber, 1993).

Terrorism: the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or a segment thereof, in furtherance of political or social objectives (FBI).

Threat: an intent of damage or injury; an indication of something impending (General Security Risk Assessment Guideline, 2003).

Threat Assessment: is used to evaluate the likelihood of terrorist activity against a given asset or location. It identifies and evaluates each threat on the basis of various factors, including capability, intention, and lethality of an attack (Decker, 2001).

Venue: college sports stadiums that host several thousand spectators.

Vulnerability: an exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person (General Security Risk Assessment Guideline, 2003).

Vulnerability Assessment: is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists and may suggest options to eliminate or mitigate those weaknesses (Decker, 2001).

Weapons of Mass Destruction (WMD): (A) any explosive, incendiary or poison gas, bomb, grenade or rocket having a propellant charge of more than four ounces, or a missile having an explosive or incendiary charge of more than one quarter ounce, or mine

or device similar to the above; (B) poison gas; (C) any weapon involving a disease organism; or (D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (WMD Threat and Risk Assessment, 2005).

Justification

Some sport organizations, such as the NCAA, have developed security checklists and standards but there are currently no documented research-based standards for effective security management of university sport venues. No one has conducted research utilizing Department of Homeland Security (Office of Domestic Preparedness) risk assessment methods directly related to sport event security management. Furthermore, there is little scholarly work in the area of sport event security management. The benefit of establishing standards is to create consistency in security policy and procedures at university sports venues, thereby minimizing risk and safeguarding a university's critical assets – the fans, players, officials, vendors, media personnel, local community, and stadium structure. Other projected benefits may include development of curriculum in sports event security management, development of training materials and certifications for key security staff, and improving communication networks for dissemination of standards or “best practices”. Improving security management awareness through identification of standards, developing training/certification materials, conducting vulnerability assessments and game day audits will most certainly harden potential targets and hopefully deter potential threats to sports event venues.

CHAPTER II

REVIEW OF RELATED LITERATURE

This chapter includes an overview of terrorism, actions taken to secure the homeland, the terrorist threat to sport, understanding risk, sports event security management, a description of the Center for Research and Education: Sports Event Security Management, and discussion of standards.

Terrorism

Terrorism is not something new, its roots can be traced back at least 2,000 years (Burgess, 2003). “The word *terrorism* originated in Europe after becoming a known tactic during the “Reign of Terror” that followed the French Revolution of 1789” (Johnson, 2005, p. 1). It is probably safe to say that every civilization in the history of humankind has been exposed to terrorism (Johnson, 2005). Prehistoric village dwellers used kidnapping and rape as a means to intimidate competing tribes. Roman soldiers contaminated water supplies by throwing dead bodies into water wells, poisoning many people. In the sieges of Crimea during the mid-1300’s, the Tatar army launched corpses of plague victims over city walls causing an epidemic and eventual surrender to their forces. There has also been state-sponsored terrorism throughout history. In 1478, Pope Sixtus IV ordered the Spanish Inquisition; in 1918, the soviet secret police (the Cheka) was founded by Vladimir Lenin to restrain opposition; and in the 1930’s and 40’s the Nazi Gestapo supported Adolph Hitler’s control by fear (2005).

Terrorism has been prevalent in the United States for centuries. According to Johnson (2005), “during the British Colonization of America in the 1700’s, soldiers intentionally distributed small-pox infected blankets to Native Americans to take back

their villages” (p. 1) resulting in thousands of innocent deaths. After the American Civil War (1861-1865), segregationists formed the Klu Klux Klan to oppose supporters of reconstruction. In September, 1920, anarchists exploded a horse cart filled with dynamite on the corner of Wall Street, causing 40 deaths and injuring 300 others (National Strategy for Combating Terrorism, 2003). President William McKinley was assassinated in 1901. In 1984, the Rajneeshee cult in Oregon contaminated salad bars with salmonella to incapacitate voters in order to influence a local election (Johnson, 2005). A Muslim extremist group bombed the World Trade Center in New York City in 1993 and in 1995 a domestic terrorist named Timothy McVeigh bombed a federal building in Oklahoma City (2005). The attacks on the World Trade Center and Pentagon in 2001 were an indication of things to come in the twenty-first century. “Our Nation learned a terrible lesson on September 11. American soil is not immune to evil or cold-blooded enemies capable of mass murder and terror.” (The National Strategy for Homeland Security, 2002, p. 1).

There are two primary categories of terrorism: domestic terrorism and international terrorism. WMD Threat and Risk Assessment (2005):

Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States and its territories without foreign direction, and whose acts are directed at elements of the U.S. Government or its population, in furtherance of political or social goals.

International terrorism is the unlawful use of force or violence against persons or property committed by a group or individual who has some connection to a foreign power or whose activities transcend national boundaries (p. 2-4).

According to George Eisen, an expert in international terrorism, “organized

terrorism has two distinct goals: inflicting the maximum amount of humiliation and publicizing the terrorists' cause to the widest possible audience" (Spangler, 2001).

Terrorists tend to be outside the mainstream of society and take pride in not being part of the majority (Johnson, 2005). Those involved in terrorist activity do so to achieve some type of objective. These include gaining recognition, coercion, intimidation, and/or provocation (WMD Threat and Risk Assessment, 2005). According to Arquilla, Ronfeldt, & Zanini (1999), the phenomenon of terrorism appeals to its perpetrators for three principal reasons:

1. It appeals as a weapon of the weak – waging war to harm and defeat superior forces (p. 39).
2. It appeals as a way to assert identity and command attention (p. 40).
3. It appeals as a way to achieve a new future order by trying to wreck the present (p. 40).

Spangler (2001) explains that "modern terrorism comes in many shapes and forms, from organized groups with meticulous planning to a single individual acting on his or her own political agenda." 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, including: political, religious, racial, environmental, and special interest. Table 1 highlights the five different threat motivations, likely targets, and existing groups identified in WMD Threat and Risk Assessment (2005).

Terrorists run the full political and religious spectrum, from left to right wing extremists, and from religious to secular (Johnson, 2005). "The only term that seems to apply universally is *radical*. Terrorists are radical in both perspective and in chosen

actions” (p. 3). For example, religiously motivated terrorism has resulted in bombings by

Table 1: Terrorism Motivations

Threat Motivation	Likely Targets	Existing Groups
1. Political	<ul style="list-style-type: none"> • Government institutions • Government/National leadership/ authority figures • Icons and symbols of government (historical facilities) 	<ul style="list-style-type: none"> • Anarchists • Armed Forces of National Liberation Front (FALN) • Mountaineer Militia • Sons of the Gestapo • Patriots Council
2. Religious	<ul style="list-style-type: none"> • Financial institutions • Media • Large public venues • Churches, synagogues, etc • Women’s health facilities 	<ul style="list-style-type: none"> • Pro-life/Right-to-life extremist groups • Branch Davidians • Fundamentalists/Extremists
3. Racial	<ul style="list-style-type: none"> • Minority churches • Facilities and symbols of racial groups or organizations 	<ul style="list-style-type: none"> • National Black United Front • Aryan Nations • National Alliance
4. Environmental	<ul style="list-style-type: none"> • Construction projects • Mining • Logging or exploration sites • Potential sources of pollution of air or water 	<ul style="list-style-type: none"> • Earth First • Earth Liberation Front (ELF)
5. Special-Interest	<ul style="list-style-type: none"> • Women’s health facilities • Animal research laboratories • Technology companies • University research facilities 	<ul style="list-style-type: none"> • Animal Liberation Front (ALF) • Anti-abortion • Anti-technology

extremist Christians opposed to abortion (2005). Political motivated terrorism, such as the Al Qaeda network and Islamic movement have a goal to impose their “own beliefs upon society and in turn reshape the culture” (p. 3).

Despite the terrorists’ diversity in motive or means of attack, terrorist organizations share a basic structure of *underlying conditions, international environment, states, organization, and leadership* (National Strategy for Combating Terrorism, 2003). Underlying conditions include poverty, religious conflict, corruption and ethnic strife, which terrorists use to justify their actions and gain support (2003). The international environment influences how terrorist strategies evolve. Open borders provide access to

support, such as safe havens and capabilities. States around the world, intentionally and unintentionally, offer physical (training grounds) and virtual (communication networks) havens for terrorists to plan, train and organize their operations (2003). Organization determines membership, resources, and capabilities. The leadership provides direction and is the catalyst for terrorist action. Some organizations today have decentralized command with autonomous cells (2003).

“The means used by modern day terrorists run from the simple to the elaborate.” (Johnson, 2005, p. 3). Conventional means such as knives, guns, and bombs are frequently used but the probability of terrorists using weapons of mass destruction (chemical, biological, radiological, nuclear, or high-yield explosives) have significantly increased in the past decade (National Strategy for Combating Terrorism, 2003). Recent events worldwide, including the October 2001 mailings of anthrax-tainted letters in the United States, the release of sarin gas in a Tokyo Subway in 1995 and suspected plans by terrorists to use a crop duster as a means to disperse chemical or biological weapons emphasize that chemical and biological attacks, once thought of as only a remote possibility, are now real-world risks (Jane’s Chem-Bio Handbook, 2002, p. 3). The knowledge, technology, and materials needed to build weapons of mass destruction are more accessible and widespread than ever before (The National Strategy for Homeland Security, 2002). Chemical weapons are extremely lethal and capable of producing mass casualties. Unfortunately, they are easily manufactured as needed materials normally have legitimate dual purposes (2002). Biological weapons release large quantities of disease-causing microorganisms and can be extremely dangerous (2002). One does not know immediately that they are being attacked allowing the biological agent time to

spread and cause serious harm. They are also easy to manufacture and can serve as a means of attack against humans, livestock, and crops (2002). Bio-terrorism is now a buzz word in most governmental documents in the fight against terrorism. According to President Bush, the U.S. has “to be prepared for the threat of biological terrorism – the deliberate use of disease as a weapon.” (Securing the Homeland Strengthening the Nation, n.d., p. 12). The President’s Budget for 2003 proposed \$5.9 billion in new funding to defend against biological terrorism, focusing on 1) infrastructure: strengthening the state and local health systems, 2) response: improve specialized Federal capabilities to respond in coordination with state, local, and private capabilities, and 3) science: developing new vaccines, medicines, and tests through research and development (p. 12). Radiological weapons combine radioactive material with conventional explosives and can cause widespread panic in densely populated areas (National Strategy for Homeland Security, 2002). Nuclear weapons can cause enormous destruction and devastation. Nuclear weapons are not as easy to acquire and to work such a weapon requires a high degree of technical ability (2002). Explosives have been the weapon of choice as the materials for manufacturing explosives are readily available.

Other ‘new’ forms of terrorism may include cyber attacks on electronic and computer networks which are linked to critical infrastructures such as energy, financial, and security networks (The National Strategy for Homeland Security, 2002). Terrorist enemies are constantly looking for new ways to attack by finding areas of vulnerability. America provides an infinite number of potential targets (2002). “Our population is large, diverse, and highly mobile, allowing terrorists to hide within our midst. Americans congregate at schools, sporting arenas, malls, concert halls, office buildings, high-rise

residences, and places of worship, presenting targets with the potential for many casualties” (p. 8).

In April, 2004, the U.S. Department of State, Office of the Coordinator for Counterterrorism, released a report on the patterns of global terrorism. The following line graph illustrates the total number of international terrorist attacks from 1990-2004. Statistics were retrieved from the Patterns of Global Terrorism (2003) and ArizonaDailyStar.com (2005).

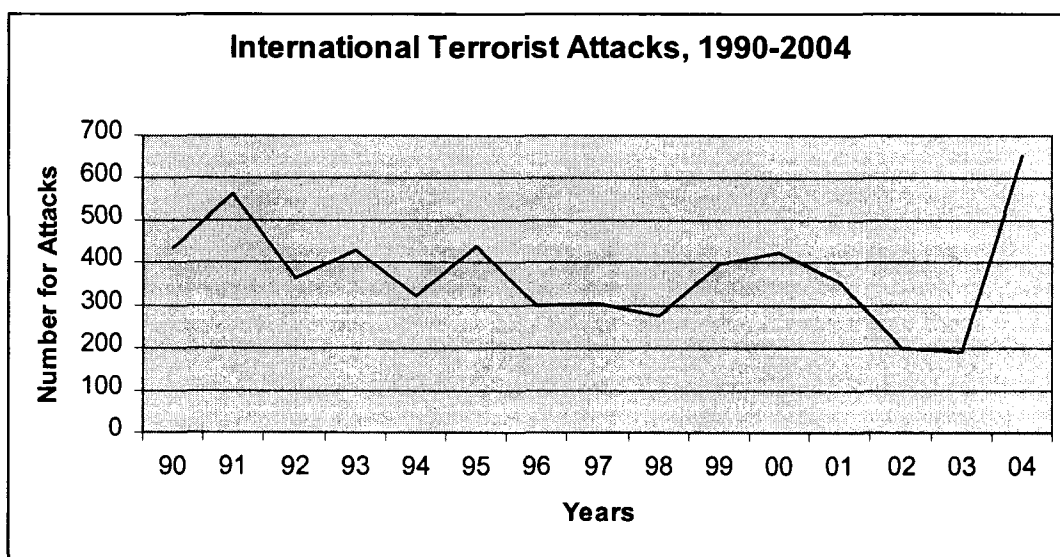


Figure 1. International Terrorist Attacks, 1990-2004

The graph clearly indicates terrorist activity sharply increased in 2004. The Associated Press (2005a) reported statistics released from the counterterrorism center. International attacks in 2004 more than tripled to 651 (ArizonaDailyStar.com, 2005).

The following bar charts depict the total anti-U.S. attacks in 2003 by region (Figure 2) and targets attacked (Figure 3) (Patterns of Global Terrorism, 2004, p. 181). Methods of attack included kidnapping, firebombing, arson, armed attack, and bombing (2004).

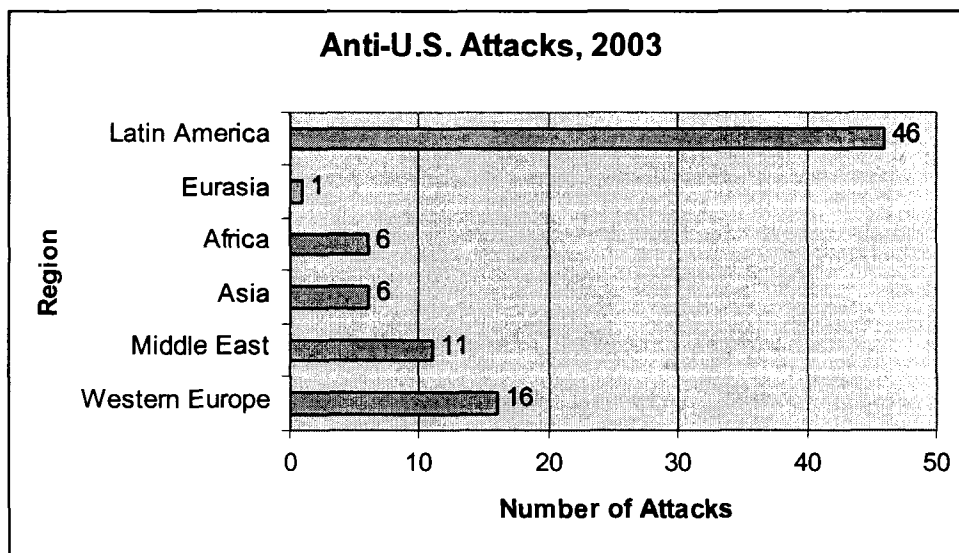


Figure 2. Anti-US Attacks, 2003

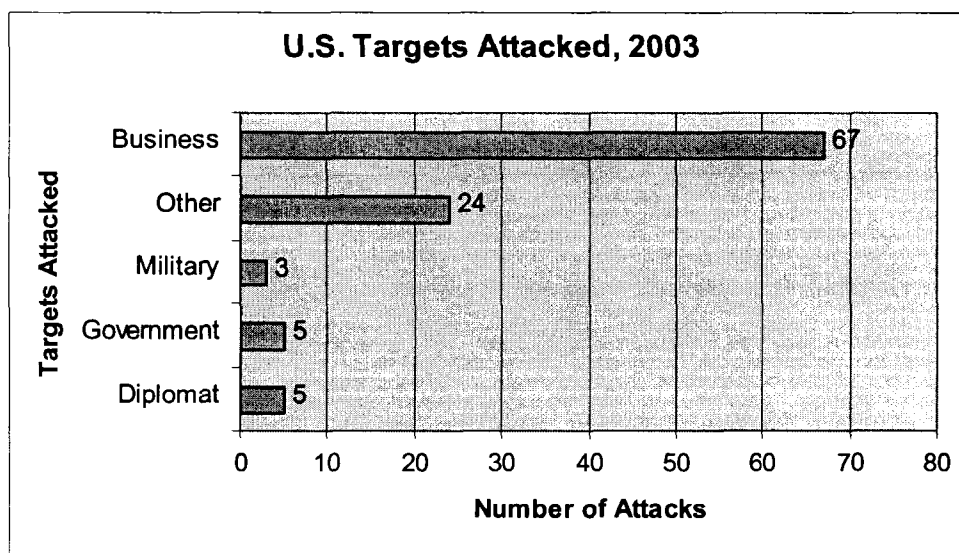


Figure 3. U.S. Targets Attacked, 2003

“Today’s terrorists can strike at any place, at any time, and with a wide variety of weapons”(Securing the Homeland Strengthening the Nation, n.d., p. 2).

Johnson (2005) describes some recent examples of terrorist attacks:

Rajneeshee Cult

In 1984 in Oregon, salad bars were contaminated with salmonella prior to Election Day in an effort to influence local elections. Over 750 people were seriously ill (p. 3).

World Trade Center

In 1993, Islamic terrorist groups attacked the World Trade Center in New York City. The terrorists placed a 1,500-pound urea-nitrate bomb in a van and parked it in the basement of one of the buildings and set the timer. The bomb exploded killing six people and injuring over a thousand innocent victims (p. 4).

Tokyo Subway

In 1995, a terrorist group released the nerve agent sarin in the Tokyo subways, killing twelve and sickening thousands (p. 4).

Oklahoma City Bombing

In 1995, domestic terrorist Timothy McVeigh parked a truck loaded with explosives outside the Alfred P. Murrah government building in Oklahoma City. This attack killed 168 people and wounded over 500 others (p. 4).

U.S. Embassies, Africa

In 1998, a coordinated attack was executed on two U.S. embassies in Kenya and Tanzania. A total of 224 people were killed and over 5,000 injured. Osama Bin Laden is held responsible for these attacks (p. 4).

U.S.S. Cole

In 2000 in Yemen, a group of suicide bombers used a skiff to pull alongside the U.S.S. Cole. They detonated a bomb killing seventeen and wounding thirty-nine. This attack was also attributed to Osama Bin Laden (p. 5).

World Trade Center and Pentagon

On September 11, 2001, terrorists hijacked 4 commercial airplanes to use as weapons of mass destruction. One plane crashed into Trade Center Tower One and another crashed into Trade Center Tower Two. Both towers eventually collapsed resulting in approximately 3,000 deaths of men, women, and children (p. 5).

Anthrax Mailings

In October, 2001, there were several incidents of anthrax mailings to individuals and entities in the U.S. Targets included the NBC television station and U.S. Congress. One person died from contracting anthrax from a letter sent to American Media in Florida (p. 5).

Madrid Subway

In 2004, subways in Madrid, Spain, were attacked using explosives killing 191 people. This incident is believed to have changed the course of presidential elections in Spain (p. 5).

The synchronized bombings in London on July 7, 2005, “will stifle any creeping complacency about the risks of terrorist attacks” (Andrews, 2005, ¶ 1). The attack on Britain, a U.S. ally in the war on terror, reinforced the need for planning and preparedness to prevent, detect, respond, and mitigate the risks and consequences of terrorist activity. “There is not a single community today that is completely immune and there is no individual who is not responsible for remaining informed and vigilant” (Johnson, 2005, p. 6).

Securing the Homeland

President George W. Bush signed several critical pieces of legislation into law after 9/11 in an effort to defeat terrorism. These included the Homeland Security Act of 2002; USA Patriot Act of 2001; Aviation and Transportation Security Act of 2001; Public Health Security and Bioterrorism Preparedness and Response Act of 2002; Enhanced Border Security and Visa Entry Reform Act of 2002; and Maritime Transportation Security Act of 2002 (Progress Report on the Global War on Terrorism, 2003).

On November 25, 2002, President Bush signed the Homeland Security Act of 2002. The Act established 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). This provided for the first time a single federal department whose primary mission is to protect the United States from terrorist threats (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). The Department's strategic goals include:

1. Awareness: identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and American public.
2. Prevention: Detect, deter and mitigate threats to our homeland.
3. Protection: Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.

4. Protection: Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.
5. Response: Lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.
6. Recovery: Lead national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.
7. Service: Serve the public effectively by facilitating lawful trade, travel and immigration.
8. Organizational excellence: Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness and operational synergies (Securing Our Homeland, 2004, p. 9).

The Department consists of many major components and subcomponents. An organizational chart can be found in Appendix A. The Office of Domestic Preparedness (ODP) is a principal component of the DHS responsible for preparing the U.S. for acts of terrorism (OJP.USDOJ.gov, 2005). ODP helps prepare state and local jurisdictions by providing training, funding for new equipment, support for planning exercises, and technical assistance (2005). In 2003, ODP consolidated with numerous other grant programs and functions under a new DHS agency, the Office of State and Local Government Coordination and Preparedness (SLGCP) (2005).

Four key subcomponents of the Department include Border and Transportation Security, Emergency Preparedness and Response, Information Analysis and Infrastructure Protection, and Science and Technology. Border and Transportation Security (BTS) secures the nation's borders and transportation systems and enforces U.S. immigration laws (DHS.gov, 2005). Emergency Preparedness and Response (EP&R), headed by FEMA (Federal Emergency Management Agency), ensures the nation is prepared for incidents and oversees the government's national response and recovery strategy (2005). Information Analysis and Infrastructure Protection (IAIP) helps deter, prevent, and respond to terrorist attacks by assessing vulnerabilities (2005). "It disseminates timely accurate information to federal, state, local, private, and international partners" (2005). The Science and Technology (S&T) directorate serves as the primary research arm of Homeland Security. It provides the nation with the necessary scientific and technological resources with capabilities to protect America (2005). The U.S. Department of Homeland Security in conjunction with the Office of State and Local Government Coordination and Preparedness released a Target Capabilities List (TCL) needed to perform homeland security tasks related to the four key mission areas: prevent, protect, respond to, and recover from acts of terrorism, natural disasters, and other emergencies (Target Capabilities List: Version 1.1, 2005).

According to the Progress Report on the Global War on Terrorism (2003) the American homeland is more secure today due to some important initiatives. The creation of "Smart Borders" to track the flow of people and commerce into the U.S while detecting terrorists (2003). The establishment of the Terrorist Threat Integration Center (TTIC), analyzing terrorism-related information and ensuring intelligence and law

enforcement are working together (2003). “One of the most significant law enforcement tools in the war on terrorism is the USA Patriot Act” (p. 8):

The Act strengthened the nation’s ability to prevent, investigate, and prosecute acts of terror by providing enhanced tools to detect and disrupt terrorist cells. The Act removed barriers that inhibited coordination between law enforcement, intelligence, and national defense communities. The Act also accommodated for new technology and new threats, allowing forces to fight a digital-age battle with modern tools (2003).

The Terrorist Threat to Sport

Sport lost its innocence on September 5, 1972, at the Olympic Games in Munich, Germany (CNN.com, 2002). A Palestinian group, known as Black September, sneaked into the Olympic Village and took nine members of the Israeli team hostage. The captors demanded a safe exit out of Germany and the release of Palestinian prisoners held in Israeli jails (2002). Unfortunately, a failed rescue attempt led to the death of all nine Israeli hostages, five terrorists, and one German policeman (2002). “For the first time world sport had become a victim of terrorism, bringing with it a brutal reminder of the world’s harsher realities” (¶ 2).

Terrorism struck again in 1996. This time a ‘domestic terrorist’ was responsible for the Centennial Olympic Park bombing at the Atlanta Games. This incident killed one person and injured more than 100 (CNN.com, 1996). Regardless of the motives for these attacks, terrorists chose to act on a world stage that offered global exposure for their cause, unlike the ancient Greeks who put aside their weapons and political differences for the duration of the games (1996).

In preparation for the Salt Lake Winter Games in 2002, Spangler (2001) discussed why terrorists may perceive the Games as a huge target. “The Games are sponsored by international corporations that symbolize American capitalism, companies such as Coca-Cola and McDonald’s. And they will be attended by political leaders from dozens of nations that support the American political agenda” (2001). The security cost for this event was estimated to be more than \$300 million (Grossman, Owens-Liston, & Shannon, 2002). Lisa Delpy Neirota, professor of sports management at George Washington University, believes the Super Bowl is a greater target than the Games because it is such an American icon (2001). High profile sporting events in the U.S. are a celebration of American culture and therefore considered potential terrorist targets (Hurst, Zoubek, & Pratsinakis, n.d).

Sport is a multibillion dollar industry in the United States and plays a critical role in the lives of many Americans. Since terrorists follow the motto of mass casualties and mass exposure of humiliation, large sporting events such as the Super Bowl, NASCAR, or Collegiate Football Bowls, could provide an attractive stage to communicate their message of evil and hatred for society. “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). The WMD Threat and Risk Assessment (2005) classified sports arenas/stadiums as a potential target in the recreational facility category (Figure 4).

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). The National Planning Scenarios document developed by the DHS also examines the potential of a biological attack on a sports arena (2005). The

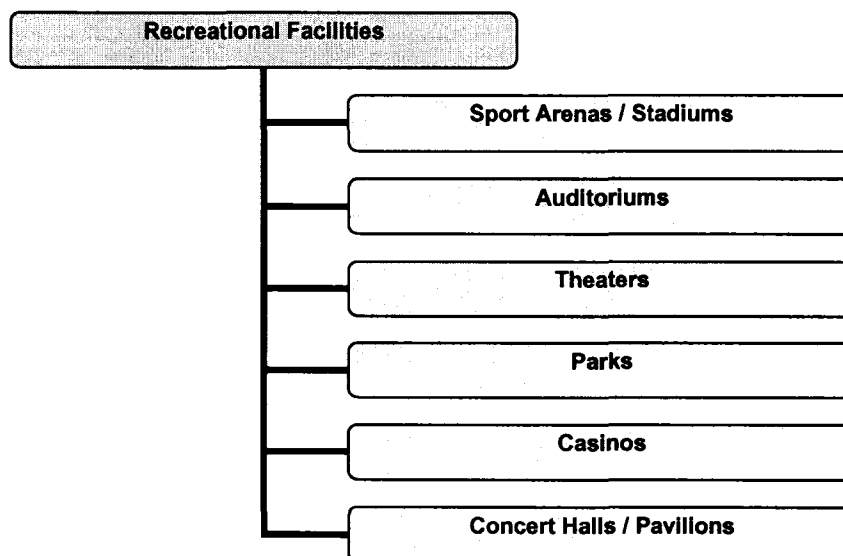


Figure 4. Recreational Facilities - Potential Terrorist Targets

spreading of pneumonic plague in the bathrooms of an airport, sports arena and train station, would potentially kill 2,500 and sicken 8,000 worldwide (2005). International terrorism expert, George Eisen, understands the difficulty in protecting all venues, events, athletes, and sports enthusiasts gathered in large crowds at an internationally televised event (Spangler, 2001). There will always be a threat and not every risk can be eliminated. The realization that sports events are at risk to terrorist activity has stimulated the need for security planning at sports venues. On July 23, 2004, the Department of Homeland Security hosted representatives from professional and collegiate sport associations and venues, and security personnel, to discuss security planning for high profile sports events. Homeland Security “Best Practices” for sporting venues was shared at the one-day seminar (DHS.gov, 2004). “American sporting venues must continue to be

viewed as “American signature properties” subject to the real and present threat of a terrorist attack” (Hurst, Zoubek, & Pratsinakis, n.d., p. 2).

In particular, collegiate sports events can be considered a potential target for terrorists. Approximately 46 million attended Division I Football games during the 2003 season (Official NCAA Football Records Book, 2005). The intercollegiate game-day environment meets the criteria for a perfect strike with high consequences. There are a large number of people in one place with mass media coverage. Most Division I college stadiums in America have large capacity stadiums. A few programs, such as the University of Michigan and the University of Tennessee, have a 100,000 plus capacity stadium. Whether a bomb explodes or a biological agent is released, fatalities will result, injuries will occur, and widespread panic will ensue. It is vital for collegiate athletic programs to acknowledge this risk and plan for worst case scenarios. Some athletic programs may not have an effective security structure in place but should take necessary steps in developing and executing security management game-day protocol.

One important issue that sport venue security must plan for is the unpredictable or unexpected acts of fan violence. “The frequency and intensity of spectator violence is increasing” (Farmer, Mulrooney, & Ammon, 1996, p. 137). The Monica Seles stabbing incident in Hamburg, Germany, soccer riots in England and Italy, and post-game victory riots after super bowls, are examples of violent fan behavior (1996). Fan violence and unruly behavior have been a problem for both professional and collegiate sports associations in recent years. In September, 2005, LSU Tiger fans pelted beer bottles at a University of Tennessee bus after the Volunteers came from behind to defeat the Tigers 30-27 in overtime (Associated Press, 2005b). In 2004, “a street reveler was killed at a

Boston Red Sox celebration when she was hit in the eye by a projectile filled with pepper spray” (Fried, 2005, p. 294). In September, 2002, a father and son attacked Kansas City Royals first base coach Tom Gamboa at Comiskey Park (Syken, 2002). Mayhem broke out at an Indiana-Pacers game in November, 2004, when fans and players exchanged punches in the stands (ESPN.com, 2004). The September 16, 2002 game between the Philadelphia Eagles and Washington Redskins “was stopped for eight minutes when pepper spray that police used to break up a fight drifted towards the Philadelphia bench” (Syken, 2002). In 1995, Chicago Cubs pitcher Randy Myers had to fend off a Wrigley fan who charged the field (2002). The British Football (soccer) Association has been dealing with fan violence or hooliganism at their soccer matches for years. The Association had to rethink all aspects of their security plans to prohibit dangerous fan behavior.

With the unknown certainty of terrorist actions and fan behavior, it is impossible to ensure a risk-free environment at America’s sporting venues. Incidents will happen and emergencies will arise. It is therefore a matter of how one prepares, responds, and recovers to mitigate the consequences of emergencies at a sporting venue. Sport venue managers need to be aware of risk assessment methodologies to detect threats, identify vulnerabilities, and reduce consequences. Information gathered through this process is extremely valuable to enhance security measures and harden the venue.

Understanding Risk

“Risk is the possibility of loss resulting from a threat, security incident, or event” (General Security Risk Assessment Guideline, 2003, p. 5). Risk is inherent in almost all aspects of life. Sport venue managers must continually attempt to minimize risk at their facilities. Risk can not be totally eliminated from the environment, but with careful

planning it can be managed. “Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack” (Decker, 2001, p. 1).

Risk is best understood as the product of the consequence of an event and the probability of the event occurring: Risk = Consequence x Probability (“Risk 101”, n.d). Risk increases as the consequences and probability of occurrence increases (n.d.). “In order to manage risk, it must first be identified, measured, and evaluated” (§ 4). The Vulnerability Assessment Report (2003) issued by the Office for Domestic Preparedness, Department of Homeland Security, identified three types of risk: mission or function risks, asset risks, and security risks. Mission risks prevent an organization from accomplishing its mission (2003). Asset risks may harm an organization’s physical assets and security risks have the potential to cripple actual data and people (2003).

Sport facility managers identify risks through various means. They can conduct surveys of attendees, conduct inspections of the facility, interview present employees, or ask experts in the field (Ammon, Southall, & Blair, 2004). Sport facility managers must address primary and secondary factors in order to reduce risk (2004). Primary factors are identified in the standard operating procedures. Facility staff is included among these factors (2004). An unsupervised or improperly trained ticket taker, usher, or cashier can become a risk for the facility manager (2004). “A well-trained staff, educated about proper risk management procedures, can help the risk manager to identify potential risks” (p. 108). Secondary factors of risk faced by most sport facilities include weather, type of event, patron demographics, and facility location (2004).

The essence of risk is dependent on the potential of threats. “A threat is a product of intention and capability of an adversary, both manmade and natural, to undertake an action which would be detrimental to an asset” (Vulnerability Assessment Report, 2003, p. 11). Vulnerabilities expose the asset to a threat and eventual loss. The General Security Risk Assessment Guideline (2003) defines vulnerability as “an exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person” (p. 5). A risk analysis evaluating the potential of loss from a threat will determine whether risk should be reduced, re-assigned, transferred, or accepted (Vulnerability Assessment Report, 2003). . “An acceptable risk is the risk level that an individual or group considers reasonable for the perceived benefit of an activity” (“Risk 101”, n.d., Acceptable Risk ¶ 1). An acceptable level of risk is usually determined by the asset manager or owner (2003). Risks that are severe, cause a high degree of loss, and occur frequently should be avoided (Ammon, Southall, & Blair, 2004). Average frequency and moderate severity risks can be transferred to someone who is willing to assume the risk. The facility manager may decide to pay an insurance company to cover physical and financial damages (2004). Some facility managers may decide keep or retain the risk and in doing so become financially responsible (2004). Facility managers can reduce risk through staff training, preventative maintenance, and development of a risk management plan to be included in the standard operating procedure (SOP) (2004). “The SOP is a set of instructions giving detailed directions and appropriate courses of action for given situations. SOP’s should be developed for all risks,” (Farmer, Mulrooney, & Ammon, 1996, p. 81).

In order to determine threats and vulnerabilities an organization must undergo a

risk assessment. The Department of Homeland Security issued a ten-step risk assessment methodology criterion:

- Clearly identify the infrastructure sector being assessed
- Specify the type of security discipline addressed, e.g. physical, information, operations
- Collect specific data pertaining to each asset
- Identify critical/key assets to be protected
- Determine the mission impact of the loss or damage of that asset
- Conduct a threat analysis and perform assessment for specific assets
- Perform a vulnerability analysis and assessment to specific threats
- Conduct analytical risk assessment and determine priorities for each asset
- Be relatively low cost to train and conduct
- Make specific, concrete recommendations concerning countermeasures (Vulnerability Assessment Report, 2003).

This criterion is general in nature and may be adapted to meet the needs of a specific organization. Several risk assessment models exist today, for example Sandia National Laboratories developed the RAM-Chemical to assess chemical facilities in the United States. Sports facilities in the U.S. must embrace risk management processes. Identifying the greatest threats and eliminating or reducing vulnerabilities will help minimize risk at sports events. “A sports arena is always critical as a high value terrorist target because of the potentially high casualty rate” (Durling, Price, & Spero, 2005, p. 8). Whether it is a terrorist attack, natural disaster, or unruly fan behavior sport venue managers must pursue an effective risk management approach to protect the facility and

human lives.

Sports Event Security Management

“On September 11th, it became abundantly clear that stadium and arena operators needed to incorporate security safeguards at America’s sporting venues.” (Pantera et al., 2003, ¶ 1). Imagine thousands of panicky sports fans trapped in a stadium, “bloodied and dying from explosions, gunfire or a bioterrorist attack” (Iwata, 2002, ¶ 1). Simple security upgrades were made at professional and college sports stadiums after 9/11 but venue managers have made more significant changes since then, including: staying alert for bioterrorist attacks by posting cameras and guards near air ducts and water pipes that could spread a poisonous gas; thinking like cops and military intelligence through working closely with law enforcement; using stronger permanent barriers; and using more guards and security devices such as surveillance cameras, alarm systems and x-ray devices (2002).

In the aftermath of 9/11, most leagues, teams, and venues conducted threat assessments and updated security practices (Hurst, Zoubek, & Pratsinakis, n.d.). By way of example, the National Football League developed a “best practices guide” of recommended security measures for NFL teams (n.d.). According to the Associate Press (2001) the “NFL has implemented the tightest security measures since the 1991 playoffs and Super Bowl during the Gulf War” (¶ 1). Recommended security measures included: 24 hour security, use of hand-held metal detectors, the search of bags and personal items, parking prohibitions, limited vehicle access near the stadium pre-game and game-day, use of barricades, increased security personnel, additional surveillance equipment, and the banning of backpacks, large purses, coolers, etc. (n.d.). The NFL also made a request to the Federal Aviation Administration to restrict airspace above all NFL stadiums (Mason,

2001). In this heightened environment for terrorist attacks it is important for sports organizations to “institutionalize security measures in policy and procedure guidelines, train personnel on the guidelines and stage exercises to drill and test incident response plans” (Hurst, Zoubek, & Pratsinakis, n.d., p. 4). Several 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).

Hurst, Zoubek, & Pratsinakis (n.d.) also indicated the necessity to educate players, fans, and employees about new practices, the importance of adherence to the new practices, the inconveniences possibly caused, and finally, the costs generated from the new practices. Several colleges have posted their stadium security policies on their websites to inform fans. Americans may not be happy about policy changes or invasion of privacy but they must understand the urgent demand for effective security in today’s terrorist environment.

Collegiate athletic programs in particular stepped up security on many levels. For example, the Federal Aviation Administration accepted a request from the University of Michigan to declare a no-fly zone over the Wolverines stadium for their game against Western Michigan in September, 2001 (Bagnato, 2001). Michigan also locked down their stadium several days before game day and used bomb sniffing dogs to sweep the premises the morning before kick-off (2001). The Penn State Nittany Lions no longer allowed re-entry to the stadium and illegally parked cars were towed. The Mississippi State Bulldogs officially banned backpacks, and like many other college stadiums in the country, Nebraska’s Memorial stadium had a greater security presence inside and outside the grounds (2001).

Pantera et al. (2003) conducted a nationwide investigation on game-day security operations at Division I college football and basketball venues. After an extensive review of literature and key correspondence with sports security experts they developed a 38 item "Game Day Security Operations Checklist" (2003). Some items included venue lockdown, restricted areas, employee IDs, pre-event training, risk management plans, coordination with state police, evacuation plans, undercover surveillance, and broadcasts regarding security factors (2003). One hundred and twenty-one (38%) of Division I schools, representing all 31 conferences, were surveyed. Results from this study indicated that there were a few superior athletic conferences (2003). Eight conferences participating in Division I Football (SEC, Big East, Pac-10, Big 12, Big 10, ACC, WAC, and Mountain West) complied with the security measures 75% of the time versus only six basketball playing conferences (Big East, SEC, Big 12, Big 10, West Coast Conference, and Horizon League) (2003). The research study indicates there is much room for needed improvement of security measures at college sporting venues.

So why is security not as effective in the collegiate arena? Pantera et al. (2003) presented reasons for such conditions. Cost may be a factor as the average college athletic department budget would not lend itself to implementing extreme security measures, like antiterrorism squads and bioterrorism detection equipment (2003). Football stadiums are normally located off-campus, host a limited number of events, and are normally catered to the corporate client meaning they would probably have more stringent security measures in place (2003). Basketball arenas tend to be located on-campus and host several other university activities (2003). To effectively secure such a facility may be very cost-prohibitive. Colleges must look for the most cost-efficient methods for securing their

venues. Milton Alherich, Vice President for NFL security, suggested purchasing concrete bollards coupled with low-cost strategies like no re-entry, no carry-ins, and no deliveries 90 minutes prior to kick-off, can help secure sporting venues (2003). According to Iwata (2002) "Security is costly". Security at the Utah Winter Olympics cost \$300 million, the 2002 Super Bowl in New Orleans cost \$6 million, and the cost for security at the 2006 World Cup in Germany is yet to be confirmed. The mandatory pat-downs recently implemented by the NFL have created some controversy for the Tampa Bay Buccaneers. The Buccaneers wanted the taxpayers to pay for the extra \$9,597 per game for security (Snel, 2005). However, it is important to overcome these obstacles as one can not put a price on saving lives.

Future implications discussed by Pantera et al., (2003) included the necessity for effective communication and scrutinization of game plans well in advance of game time. Coordinated communications such as disaster/emergency responses need to be planned and practiced (2003). Collegiate sport venue managers should develop and practice responses to disaster scenarios with support of local, state, and federal first responders (2003). Furthermore, all game-day staff must be familiar with their roles and responsibilities (2003). According to Goss, Jubenville, & MacBeth (n.d., "Training: our best kept secret"), "To be ready to preempt or react to terror strikes, venue workers at entry level must receive timely security training." Training must be a continuous element to facility worker's duties (n.d.). Outsourcing security personnel just to present a security presence is no longer adequate (n.d.). Many venues have chosen to develop and maintain their own in-house security response teams that are familiar with the venue (n.d.). Facility managers should also communicate to local law enforcement the exact role they play during game-

day operations and in the event of an emergency (n.d.)

Security Management Online conducted a survey in November, 2002, to assess sport facility security in the U.S. and Canada (Gips, 2003). Forty-seven professional and collegiate facility managers responded to the survey regarding their current security posture (2003). Similar to Pantera et al. (2003) findings, the majority of facilities have tightened restrictions on bags, coolers, and other items. Gips (2003) reports that close to one-third of professional sport stadiums fail to perform background checks on part-time staff and less than 10 percent 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 (2003). The professional ranks have increased standoff distance around their facilities, 81 percent of stadiums and 60 percent of arenas, versus only half of the college stadiums surveyed (2003). Facilities that serve alcohol are reluctant to reduce or eliminate sales (2003). Only 19 percent of respondents pursue criminal charges against violent or unruly fans and only 28 percent of facilities have instituted a stricter expulsion policy for unruly fans (2003). More than two-thirds of all respondents increased electronic surveillance (2003).

Pantera (2003) reported a list of pre-event, game time, and post-event considerations for sport venue managers:

Pre-Event Considerations

1. write a formal risk management plan
2. implement a pre-event training program for all event staff
3. be aware of nearby dangerous/explosive sites

4. be aware of the quantities of antidotes within the region
5. coordinate your plans with the local and state police
6. conduct background checks on all employees including students and seasonal employees
7. verify that first responders have a small stockpile of drugs and medications for rapid response use should a biological weapon be released
8. utilize 24 hour live security teams in concert with a sophisticated surveillance system
9. lockdown the venue prior to the event
10. prohibit all concessions deliveries 90 minutes prior to the event
11. utilize bomb-sniffing dogs
12. test air quality prior to the event
13. issue holographic personal identification cards for all media
14. purchase and install clear refuse bags and receptacles
15. escort all cleaning crews

Game Time Considerations

1. secure no-fly zones over the venue
2. patrol air space above the venue, parking lots, and adjacent access roads
3. secure the services of a mobile emergency room to be on site
4. utilize portable biological detection equipment
5. use undercover surveillance teams/individuals
6. utilize 1 crowd observer for every 250 spectators

7. utilize radio equipped security personnel in parking lots and key access points
8. utilize radio equipped security personnel in parking lots and key access points
9. have key personnel wear inexpensive hazmat smart strips that detect the presence of nerve agents, cyanide, and other chemicals
10. invoke periodic broadcasts detailing security practices and restricted areas within the facility
11. implement electronic scanning of all tickets and match these records with detailed records of all your season ticket holders
12. frisk/wand every spectator
13. ban all carry-ins and backpacks
14. prohibit re-entry by spectators

Post-Event and General Considerations

1. implement a formal post-event debriefing of all personnel
2. vary your security practices so as not to create a pattern in your system

In July, 2004, the Department of Homeland Security held a one-day seminar for professional and collegiate sport association representatives, and security personnel. The focus of the seminar was security planning for high profile sporting events. This provided a unique opportunity for sports and security representatives to share important information that would help sport facility operators better prevent, detect and respond to terrorist threats (DHS.gov, 2004). Specific security measures being shared as “best practices” by the DHS include:

- Conducting comprehensive security assessments of event venues;
- Increasing perimeter security and safety patrols during an event;
- Installing surveillance cameras and other equipment to enhance detection monitoring capabilities;
- Establishing restricted areas of access for essential personnel only; and
- Reinforcing employee procedures to ensure knowledge of emergency protocol (2004).

In February, 2005, the Department of Homeland Security developed an on-line Vulnerability Self-Assessment Tool (VSAT) for large stadiums (McHale, 2005). “The tool incorporates industry safety and security best practices for critical infrastructure to assist in establishing a security baseline for each stadium” (Chabrow, 2005, p. 71). It is user-friendly and designed for stadiums that seat more than 30,000 people (2005). It focuses on key areas such as information security, physical assets, communication security, and personnel security (2005). Users are provided a report on the effectiveness of their facility security plan and provided strategies for implementing future improvements (2005).

Preventing terrorism at sporting venues is not the only battle venue manager’s face. One of the recent problems facing sports events is fan violence, whether directed at players and officials, or each other. Sport venue managers must plan and prepare to counter unruly fan behavior. Goss, Jubenville, & MacBeth (n.d.), examined the various methods utilized by British soccer stadium authorities “to curb hooliganism before, during, and after soccer matches” (n.d.). Efforts centered around three key areas: stadium accessibility, provisions and monitoring of hospitality, and mastery of cutting-edge technology (n.d.). Authorities conducted audits on operating procedures, including risk management planning. The

analysis led to several new security measures to prevent future incidents. Hooligans were banned from matches in Britain and abroad, and their passports confiscated prior to international matches (n.d). Undercover agents were assigned to particular football clubs to identify and monitor hooligans (n.d). New stadium construction controlled access by restricting the size of the grounds around the stadium, and bench-like bleacher seating systems were replaced with all-seated stadiums (n.d.) Authorities established better organization of ticket sales and distribution, controlling fan placement and allocating empty sections as buffer zones between fan sections (n.d). Ushers were trained in crowd control methods and spectator safety (n.d.). Technology, such as closed-circuit television (CCTV), Photophone, and FaceTrac are used to identify fans, run database searches, and send images to security personnel on the ground (n.d.). “By conducting threat/vulnerability assessments, by establishing clear guidelines and procedures, by training personnel, and by conducting incident drills, leagues, teams, and venue operators can take significant and effective measures to prevent and prepare for a terrorist incident” (Hurst, Zoubek, & Pratsinakis, n.d., p. 4), natural disaster, fan violence, and other emergencies.

Center for Sports Event Security Management (SESM)

The University of Southern Mississippi Center for Sports Event Security Management (SESM) was established in May, 2005, through a research grant awarded by the Mississippi Department of Homeland Security (MDHS) and the Mississippi Emergency Management Agency (MEMA). The specific purpose of the research grant was to create a research-based model for effective security management of university sport venues.

The Center, in partnership with Security Management Solutions (SMS), conducted vulnerability assessments at seven of the state-supported universities in Mississippi. SMS

provided security expertise and experience and ensured the vulnerability assessments were conducted according to Homeland Security/Office of Domestic Preparedness guidelines. SMS created a Sports Event Security Assessment Team (SESAT) at each campus site to aid with the assessments. The SESAT included a representative from the athletic department, campus police, local law enforcement, university physical plant, and local county emergency management agency. The vulnerability assessment process helped gather relevant data and information to develop a Sports Event Security Risk Assessment Model that was aligned with Homeland Security/ODP criteria. The Southern Miss Center, in cooperation with Security Management Solutions, created a risk assessment model specific to sports event security management.

The objective of the Center for SESM is to develop organizational, technical, and educational tools required to prevent, prepare for, respond to, and recover from sports events emergencies (including terrorist attacks, natural disasters, and/or fan violence). The Center will develop a consortium with other universities, corporate partners, and professional organizations. Research areas to be addressed include: planning, prevention and deterrence, preparedness, decision-making, effective response networks, recovery efforts, communication systems, modeling and simulation, and best practices. The Center will develop academic courses, certification programs, training, and consulting services. An annual sports event security management conference will also be established.

Standards

Standards are defined by Marshall Thurber (1993) as “a written, or visual measurable guideline describing expected behavior, performance, product or service.” Standards are used by many organizations to ensure effectiveness and efficiency in

programs and processes. The sports event security management standards developed by the researcher will guarantee that an acceptable level of security is attained and a degree of safety is provided by college athletic programs. The standards will ensure college sports venues are taking the necessary precautions to secure the venue and safeguard their critical assets – the people. Standards to be developed by the researcher will assist the development of the Sports Event Security Assessment Model (SESAM). By meeting or exceeding the proposed standards, collegiate athletic programs will dramatically enhance security levels, providing a safer environment for players, fans, media and game-day personnel. According to Hurst, Zoubek, & 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). Since no research-based standards exist for university sport venue security in America, policies, procedures, and guidelines vary between institutions. Developing standards for intercollegiate sport venues will help the industry establish a security level to be achieved by all athletic programs. If collegiate sport associations, such as the NCAA and NAIA, endorse industry standards they are forcing awareness among members and letting sport consumers know reasonable measures are in place for their safety. The NCAA has issued a “best practices” planning options guide for institutions to review and the International Association of Assembly Managers (IAAM) have also identified key security practices. The Department of Homeland Security issued a Target Capabilities List (TCL) on April 6, 2005, identifying key security areas to be addressed. These documents were an excellent starting point in researching common

security themes to be used in the research study.

The review of literature presented common themes or categories of security measures. These security measures will serve as the basis for the researcher's proposed standards. Categories include: perimeter control, access control, credentialing, physical protection systems, risk management, emergency management, communications, recovery procedures, security personnel, training, modeling and simulation, and WMD – toxic materials protection.

CHAPTER III

METHODS

This chapter provides an overview of the research process, including an overview of the Delphi technique, research design, participants, instrument, procedures, and data analysis.

Overview

Through an interview process and Delphi study with a panel of experts, new knowledge in the sports event security management field was discovered. Six security experts were interviewed first to obtain a preliminary set of standards critical to the effectiveness of university sports event security management. The Delphi technique was utilized to gain feedback on the pre-established list of standards and to reach consensus among sports event security management experts (n=28). A level of importance for agreed upon standards was established through a likert-scale in rounds two and three of the Delphi study.

The Delphi Method

The Delphi technique was developed in the 1950's at RAND, the Santa Monica, California "think tank" by Olaf Helmer and Norman Dalkey (Dalkey, n.d). The Delphi method was initially used for technological and scientific forecasting. Today, businesses and governmental agencies use the Delphi process to predict or forecast future events (Ludwig, 1997). 'Delphi' refers to the classical city of Greece and was home to the Priestess Oracle that made predictions about the future that were always true (Dennington, 2004).

The primary function of the Delphi Technique in research "is to seek predictions,

interpretations, or recommendations” (Dennington, 2004, ¶ 1) from a group of experts in the area under investigation. “Delphi may be characterized as a method for structuring a group communication process, so the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem” (Linstone & Turoff, 1975, p. 3). The Delphi process aims to reach consensus among panel experts through a series of Delphi rounds. “This technique, if used effectively, can be highly efficient and generate new knowledge” (“Delphi method”, n.d., ¶ 1).

The Delphi Technique begins with the development of a set of open-ended questions on a specific issue. These questions are then distributed to various ‘experts’. The responses to these questions are summarized and a second set of questions that seek to clarify areas of agreement and disagreement is formulated and distributed to the same group of ‘experts’. The cycle of formulating further questions based on the answers given in the first set of questions is termed an ‘iteration’. Often the Delphi Technique repeats this process of iteration until consensus is reached (Dennington, 2004, p. 1).

“The key to a successful Delphi study lies in the selection of participants” (Gordon, 1994, p. 6). It is extremely important to include knowledgeable persons in the research area who are likely to cooperate and contribute valuable ideas (1994). Gordon states that most studies use expert panels of 15-35 people and one should anticipate an acceptance rate between 35 and 75 percent. Selected experts should be notified of the study and receive an official invitation to participate in the Delphi research process. A description of the project, its objectives, number of rounds, and promise of anonymity should be conveyed to potential participants (1994).

An advantage of the Delphi process is experts do not have to be in close proximity (Ludwig, 1997). The exchange of information can take place via mail, email, or FAX (Dunham, 1998). This tends to avoid the negative aspects of face-to-face panel discussions and group dynamics (“Delphi Method”, n.d.). Participant anonymity is an important aspect of the process (1997). The Delphi method “was designed to encourage true debate, independent of personalities” (Gordon, 1994).

The Delphi technique can be very time-consuming and requires skill in written communication (Dennington, 2004). Although, according to Pollard & Pollard (2004), “the writing process enables participants to thoroughly deliberate and reflect upon all aspects of the problem. The result is participants’ submission of precise, distinctive ideas” (p. 147). A disadvantage of Delphi is the information comes from a selected group and may not be representative (Dennington, 2004). The researcher may also eliminate extreme positions to force a middle-of-the-road consensus (2004).

Research Design

The purpose of this study is to develop standards for effective security management of university sport venues and assess the level of importance for those standards according to individuals responsible for sport venue security. The researcher chose a qualitative study in nature due to the desire for new knowledge from key security personnel that possessed the necessary expertise and knowledge. Email interviews were conducted and a Delphi study utilized to discover new knowledge in the field of sports event security management through a relatively small, non-random, purposeful sample.

Preliminary information was obtained through interviews. All information was recorded and used for the Delphi study. Data was gathered using a three-round Delphi

technique. Data was analyzed after each round to identify common themes or trends towards consensus for university sport venue security standards. An Analysis of Variance was used to find differences between groups in their perception of importance.

Participants

Approval for this study was obtained from the Institutional Review Board at The University of Southern Mississippi (see Appendix A). Participants in this study were qualified experts in the field of security and/or sports event security. There were two sets of participants - interview participants and Delphi study participants.

The researcher interviewed six experts in the field of sports event security management. These experts worked in various disciplines and offered their unique perspective on security management. They included: 1) a FBI agent with extensive experience in conducting vulnerability assessments of sport venues; 2) a Homeland Security Officer who oversees the implementation of ODP practices and ensuring local agencies are trained and prepared; 3) an Emergency Management Director; 4) a professional sports security officer; 5) a professional sport management officer, and 6) a NCAA Division I collegiate athletic administrator responsible for game-day security planning and operations.

Delphi study participants included the athletic facility manager, local sheriff, campus police chief, and local county emergency management director at The University of Southern Mississippi, Alcorn State University, Delta State University, Jackson State University, Mississippi Valley State University, Mississippi State University, and The University of Mississippi. These individuals were involved in the Homeland Security (ODP)/MEMA funded sports event security management research at The University of

Southern Mississippi. This sample population reflects NCAA Division I, Division I AA, and Division II, and four different Athletic Conferences.

Instrumentation

An interview process was utilized first. Interview questions were the same for each identified expert. The panel of experts were asked to list standards they perceive to be critical in effectively securing university sports events. The preliminary list of standards was used for round one Delphi. Round one Delphi asked the panel to review the pre-established list of standards and add any new standards. Round two and three Delphi questionnaires were developed from responses to the first questionnaire. Round two and three Delphi questionnaires included a 5-point likert scale requesting experts to rate each standard's level of importance. Each questionnaire was reviewed by two to three other researchers to ensure accuracy.

Procedures

A phone call was made to all interviewees explaining the research study and requesting their voluntary participation. All interviews were delivered via email. Interview participants receiving the questionnaire were asked to generate responses to the question, "What standards, under the following categories, do you perceive to be important in effectively securing sport venues? Categories included: Perimeter Control, Access Control, Credentialing, Physical Protection Systems, Risk Management, Emergency Management, Recovery Procedures, Communications, Security Personnel, Training, Modeling, and Simulation, and WMD –Toxic Materials Protection. All interview responses remained confidential and stored in a locked file cabinet in the researcher's office.

A letter and email was sent to the Delphi study participants (n=28) explaining the nature of the study and the Delphi process. They were assured complete confidentiality. To participate in the study the experts had to consent and identify their preferred choice of correspondence. Once participants were confirmed, round one Delphi was emailed or faxed according to their choice of correspondence. Participants were asked to review the standards compiled through the interview process and add, edit, or comment accordingly. A return date was stated and follow-up emails and phone calls were conducted after five days. Round one responses were summarized and common standards identified. These common standards were used to formulate round two Delphi. Round two Delphi was sent to those who responded to the first round (n=26). Participants were asked to rate the importance of each standard on a 5-point Likert Scale. Follow-up emails and phone calls were made after five days. Once returned, descriptive statistics (mean, median, and standard deviation) for the group ratings were calculated. Round two results were compiled and reformulated for round three Delphi. Round three Delphi was sent to participants with a return date and follow-up emails and phone calls made after five days. Round three again asked participants to rate the importance of each standard. They were provided descriptive information on how the group responded and were asked to consider the group response and then re-rate the items. All Delphi responses remained confidential and stored in a locked file cabinet in the researcher's office.

Data Analysis

Upon interview completion, responses were analyzed to identify a preliminary set of standards to be used for the Delphi Study. Round one Delphi questionnaires were analyzed through summarization and identification of new standards suggested by the

Delphi panel. This process ensured a consensus of university sport venue security standards by key personnel responsible for intercollegiate game day security operations. “The equivalent terms for *reliability* and *validity* for qualitative data are credibility, dependability, and confirmability. With the Delphi study, credibility is directly related to the selection of the panel of experts who must fit the area of inquiry” (Doerries & Foster, 2005, p. 260) as did the selected panel in this study. Athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors are key players in the planning and preparation for security operations of intercollegiate sports events. These experts provided valuable insights into the coordination of security protocol on game day. To further enhance credibility, transferability, dependability, and confirmability, of this study the researcher utilized triangulation, peer debriefing, and member checks. The mode of analysis was inductive by the researcher as opposed to deductive by statistical methods. With this type of study the researcher was able to reach more comprehensive findings and conclusions.

Round two and three Delphi questionnaire results were analyzed by SPSS in relation to importance ratings. Descriptive statistics (mean, median, and standard deviation) were provided for each standard. An ANOVA was conducted after round three Delphi to test for significant differences in perception of importance between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors. A level of significance was set at $\leq .0004$.

CHAPTER IV

RESULTS

This chapter includes an overview of the interview responses and Delphi study conducted to gain new knowledge in the field of university sports event security management. Results are provided for the initial interviews and each round of the Delphi study.

The purpose of this study was to establish standards for effective security management of university sport venues. Recent terrorist attacks on U.S. soil and abroad heightened the need for effective security at major sporting venues. Determining standards for effective security management of university sport venues will help provide consistency in security management practices at intercollegiate sports events. The remainder of this chapter presents findings for the interviews and Delphi study conducted to answer the research questions and hypothesis stated in chapter one.

Research Questions

1. What standards are needed for effective security management of university sport venues?
2. What is the perceived level of importance for the security standards?

Hypothesis

1. Significant differences will exist in perceptions of importance for developed standards between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors.

Interview Responses

A pre-selected group of security management experts (N = 6) were invited to

participate in a focused email interview to develop a preliminary set of standards. They included: 1) an FBI agent with extensive experience in conducting vulnerability assessments of sport venues; 2) a Homeland Security Officer who oversees the implementation of Office of Domestic Preparedness (ODP) practices and ensures that local agencies are trained and prepared; 3) an Emergency Management Director; 4) a professional sports security officer; 5) a professional sport management officer, and 6) a NCAA Division I collegiate athletic administrator responsible for game-day security planning and operations.

Interview participants received a phone call discussing the research study and requesting their participation. Six experts agreed to participate and received the interview questionnaire by email which provided a definition and example of a standard. Participants were asked, “What standards, under the following categories, do you perceive to be important in effectively securing sport venues?” Category headings determined by the researcher through the review of literature were provided, and included: Perimeter Control, Access Control, Credentialing, Physical Protection Systems, Risk Management, Emergency Management, Recovery Procedures, Communications, Security Personnel, Training, Modeling & Simulation, and WMD – Toxic Materials Protection. A copy of this interview questionnaire can be found in Appendix B. Four of the six participants responded and their feedback was used to create a preliminary list of standards. The researcher contacted interview participants by phone and email to confirm their responses and eliminate any misinterpretations. A total number of 206 standards were suggested from all four participants. The standards were consolidated under each category and as much as possible of the participants’ original wording was retained.

Some standards were suggested by more than one participant, but were only listed once to avoid duplication. The words “should be” were removed from respondents’ answers to make each standard consistent as a formal statement. A total number of 141 standards were used for Round 1 of the Delphi survey.

A peer examination enhanced the researcher’s analysis and provided a “devil’s advocate” point of view to enhance credibility. The peer examiner can attest to the conclusions and recommendations, ensuring dependability and confirmability. The researcher chose to conduct interviews and a Delphi study because new knowledge from different sources via different methods (triangulation) would strengthen the validity of the study and help the researcher gain a better understanding of the phenomena.

Delphi Study

The three-round Delphi study was conducted over a two month period and involved the athletic facility manager, campus police chief, local sheriff, and local emergency management director from seven state-supported universities in Mississippi. These included: Alcorn State University, Delta State University, Jackson State University, Mississippi Valley State University, Mississippi State University, The University of Mississippi, and The University of Southern Mississippi. Twenty-two (22) of the 28 participants successfully completed all three rounds of the Delphi (78.6%). Table 2 highlights the overall participation rates for the Delphi Study by each round and Table 3 provides participation rates by occupation for each Delphi round.

Delphi Round 1 Findings

The researcher compiled interview responses under each category heading to create the first Delphi survey. An invitational letter was sent to the Delphi panel by email

requesting their participation. A copy of this letter can be found in Appendix C. The first

Table 2: Participation Rates for the Delphi Study

Round	Main Purpose	# of Experts Asked to Participate	Number of Complete Returns	% Completed
1	Feedback on standards created through interviews	28	26	92.6
2	Rating of importance	26	23	82.1
3	Updating of previous ratings	23	22	78.6

Table 3: Participation by Occupation for each Delphi Round

Occupation	RI	RII	RIII
Campus Police Chief	6	6	5
Athletic Facility Manager	7	7	7
Local Sheriff	7	6	6
Emergency Management Director	6	4	4
TOTAL	26 (92.6%)	23 (82.1%)	22 (78.6%)

round Delphi survey was sent to a 28-member panel of experts who agreed to participate: the athletic facility manager, campus police chief, local sheriff, and local emergency management director responsible for game day security operations at seven state-supported universities in Mississippi. A copy of this survey can be found in Appendix D. Participants were asked to review the list of 141 standards and to add/edit/comment accordingly. Twenty-six (26) participants responded with a return rate of 92.6%. Eleven

(11) responded with no feedback and concurred with the researchers compiled list of standards. Fifteen (15) of the participants provided at least one or more editions to the currently listed standards. For example, in the *Communications* category it was suggested that each agency radio also be independent in case there is a breach of security. In the *Perimeter Control* category it was suggested that lock down of the stadium be 24 hours prior to the sport event and not 12 hours as previously stated, and establish a 500 feet secure outer perimeter around the stadium as opposed to 100 feet as previously stated. In the *Access Control* category it was suggested to utilize tables outside entry gates for bag inspections. Some standards were moved from one category to another as they pertained to that area more effectively. For example, ticket taker responsibilities separate from security responsibilities was moved from the *Access Control* category to *Training, Modeling, and Simulation*. The inclusion of emergency management personnel in policy development and training was moved from *Emergency Management* to *Training, Modeling, and Simulation*. Most of the feedback was directed toward wording and elimination of some listed standards due to overlap. Several participants commented on how costly it would be to implement and maintain the standards. As one panel member wrote, "Most of our small universities and local governments are operating on a tight budget and minimal personnel, how do we comply with these standards? Who will pay for all of this, and who will pay for the continuation of it?" After Delphi round 1 analysis, 134 standards were listed in Round 2.

Delphi Round 2 Findings

The 26 participants who responded to Delphi 1 received Delphi 2. Delphi 2 was distributed by email, fax, and in-person. Participants received a list of 134 standards and

were asked to rate each standard on a 5-point Likert scale as to the degree of importance (1 = very low; 2 = moderately low; 3 = average; 4 = moderately high; 5 = very high). A copy of Delphi survey 2 can be found in Appendix E. Twenty-three (23) of the 27 participants successfully completed the survey (82.1%). High mean scores indicated a high level of importance and low standard deviations (low variance) indicated a high level of consensus.

Table 4 presents a descriptive statistical summary for each standard listed under *Perimeter Control* in Delphi Round 2. The panel of experts indicated that Standard #2 - locking down the stadium (4.36), Standard #3 - police patrolling before and after events (4.41), and Standard #6 - securing vulnerable systems with locks and seals (4.41) were moderately to highly important. However, the panel clearly felt that Standard #4 - the use of bomb dog teams for inspection (3.38) was not as important.

Table 4: Perimeter Control – Round 2 Delphi Responses

Perimeter Control	Mean	SD	Mdn
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.	4.18	.85	4.00
2. Lock down stadium 24 hours prior to an event and allow only controlled access.	4.36	.79	4.50
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.	4.41	.73	5.00
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.	3.38	1.07	3.00
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.	3.64	1.17	4.00
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.	4.41	.91	5.00
7. Security assigned to guard vulnerable systems, including air takes.	3.77	.81	4.00

8. Check and empty dumpsters and trash receptacles regularly.	3.90	1.00	4.00
9. Do not place dumpsters under structural supports when and where possible.	4.23	.92	4.00
10. Establish a 500-foot secure outer perimeter around the stadium.	4.05	.87	4.00
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.	3.52	1.17	3.00
12. All campus buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	3.52	.93	4.00
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	3.81	.93	4.00

Scale (1-Low; 5-High)

Table 5 presents a descriptive statistical summary for each standard listed under *Access Control* in Delphi Round 2. The Delphi panel highlighted the prohibition of certain items such as coolers, large backpacks, weapons, etc. as highly important with a rating of 4.76 (Standard #14). Several other standards in this category proved to be important including: Standard #15 - publicize inspections and prohibited items (4.68), Standard #17 - security personnel at each entry point (4.59), Standard #23 - law enforcement at each entry point (4.55), Standard #25 - identification of coaches and players entering locker rooms and restricted areas (4.59), and Standard #35 - the right to inspect any deliveries to event area (4.59). The least important to the panel was Standard #28 - the electronic scanning of tickets (3.64).

Table 5: Access Control – Round 2 Delphi Responses

Access Control	Mean	SD	Mdn
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.	4.76	.44	5.00

15. Publicize the policy concerning inspections and identify prohibited items.	4.68	.72	5.00
16. No re-entry except for medical emergency.	4.50	.86	5.00
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	4.59	.59	5.00
18. Utilize tables outside entry gates for bag inspections.	4.41	.85	5.00
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	4.10	.89	4.00
20. Portable metal detectors at stadium entry gates.	3.82	1.10	4.00
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	4.36	.90	5.00
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	4.05	1.09	4.00
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	4.55	.60	5.00
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	4.23	.87	4.00
25. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted team areas.	4.59	.59	5.00
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	4.41	.59	4.00
27. All tickets contain a hologram for ticket validation.	3.76	.94	4.00
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	3.64	.90	4.00
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	4.36	.79	5.00
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	3.86	.99	4.00
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	3.76	.77	4.00

32. Open all main entry gates at the same time.	4.00	.87	4.00
33. Schedule limited daily or weekly delivery times for vendors.	4.00	.87	4.00
34. Accept vendor deliveries by appointment only and Authorization by the appropriate stadium supervisor.	4.19	.75	4.00
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	4.59	.73	5.00
36. No vendor deliveries should be allowed within 90 minutes of the game.	4.14	1.04	4.00
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	4.33	.80	4.00

Scale (1-Low; 5-High)

Table 6 presents a descriptive statistical summary for each standard listed under *Credentialing* in Delphi Round 2. This category ranged from 3.95 (Standard #38 - background checks) to 4.52 (Standard #45 - wearing credentials at all times). Credentialing appears to be important with only one standard with a rating below 4.00.

Table 6: Credentialing – Round 2 Delphi Responses

Credentialing	Mean	SD	Mdn
38. Background checks required for all vendors, employees, contractors, students and volunteers.	3.95	.97	4.00
39. Simplify credential systems indicating zone access and color code by game function.	4.29	.85	4.00
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	4.38	.67	4.00
41. Credentials are substantially different from those used in prior seasons.	4.43	.81	5.00
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	4.24	.83	4.00
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	4.19	.75	4.00
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	4.24	.70	4.00

45. Require all credentials to be worn at all times and clearly displayed.	4.52	.75	5.00
46. Require all team bench staff, except players in uniform, to wear a game credential.	4.38	.97	5.00
47. To assist with access control, display credential boards at all access control points.	4.48	.81	5.00

Scale (1-Low; 5-High)

Table 7 presents a descriptive statistical summary for each standard listed under *Physical Protection Systems* in Delphi Round 2. Having bomb removal equipment on site was the least important to the panel with a mean importance rating of 3.62 (Standard #50). Standard #48 - establishing a 100 ft inner perimeter (4.48), Standard #57 - having a digital security management system located in stadium and press box (4.14) with Standard #58 - monitoring capabilities in the command center (4.43), and Standard #60 - lighting in gate areas for searching purposes (4.48) were highly rated.

Table 7: Physical Protection Systems – Round 2 Delphi Responses

Physical Protection Systems	Mean	SD	Mdn
48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	4.48	.75	5.00
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	4.14	.91	4.00
50. Bomb removal equipment is on site.	3.62	1.20	4.00
51. Annual structural inspection of entire facility is required and documented.	4.18	.91	4.00
52. All utility areas alarmed and contain card access entry points.	4.14	1.01	4.00
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	3.62	.97	4.00
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	4.05	1.13	4.00
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	4.14	1.17	5.00

56. 24-hour camera surveillance of perimeter and playing field.	4.09	1.15	4.50
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	4.14	1.21	5.00
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	4.43	1.12	5.00
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	4.14	1.11	4.00
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	4.48	.87	5.00
61. Portable Hazmat Smart Stripes and detection equipment is on site.	3.95	1.02	4.00

Scale (1-Low; 5-High)

Table 8 presents a descriptive statistical summary for each standard listed under *Risk Management* in Delphi Round 2. All standards in this category received a rating higher than 4.00. The Delphi panel recognized the importance of developing and reviewing risk management plans for athletic department events with a mean score of 4.38 (Standard #62). Standard #65 - conducting weekly game management meetings including risk management issues was closely rated with a mean score of 4.35.

Table 8: Risk Management – Round 2 Delphi Responses

Risk Management (threat/risk assessment)	Mean	SD	Mdn
62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	4.38	1.02	5.00
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	4.14	.91	4.00
64. Complete plans in conjunction with local law enforcement anti-terror task force.	4.10	.89	4.00
65. Conduct weekly game management meetings (include risk management issues).	4.35	.86	5.00

Scale (1-Low; 5-High)

Table 9 presents a descriptive statistical summary for each standard listed under *Emergency Management* in Delphi Round 2. Fourteen (14) of the twenty-three (23) standards received an importance rating of 4.52 or higher. No standard in this category received an average importance rating below 4.20. Emergency management appears to be a critical area in the security management of university sport venues, especially the development of an Emergency Response Plan (Standard #66), Evacuation Plan Standard #67), Disaster Plan (Standard #79), and an Emergency Medical Plan (Standard #81).

Table 9: Emergency Management – Round 2 Delphi Responses

Emergency Management (response & evacuation)	Mean	SD	Mdn
66. Develop, maintain, and practice Emergency Response Plan.	4.52	.68	5.00
67. Develop, maintain, and practice Emergency Evacuation Plan.	4.48	.75	5.00
68. Coordinate emergency plan with local, state and federal emergency management authorities.	4.38	.87	5.00
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	4.57	.68	5.00
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	4.52	.68	5.00
71. Establish a security command and control center (primary and secondary location).	4.57	.75	5.00
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	4.33	.91	5.00
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	4.24	.89	5.00
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	4.29	.78	4.00
75. The Command Center has a view of the playing field to facilitate decision making.	4.38	.87	5.00
76. Provide a secure incident room designated for decision makers.	4.33	.91	5.00

77. Identification of management teams for response to command and control.	4.35	.93	5.00
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	4.57	.68	5.00
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	4.52	.60	5.00
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.	4.52	.75	5.00
81. Develop Emergency Medical Plan.	4.68	.65	5.00
82. Designate primary and secondary triage and transport sites.	4.45	.91	5.00
83. Identify and secure emergency routes in and out of the stadium facility.	4.57	.75	5.00
84. All emergency routes remain clear throughout the event on campus.	4.57	.60	5.00
85. Emergency Management response and evacuation personnel on site throughout event.	4.38	.67	4.00
86. More than one ambulance and at least two Certified EMT's onsite.	4.52	.60	5.00
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	4.59	.67	5.00
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	4.55	.74	5.00

Scale (1-Low; 5-High)

Table 10 presents a descriptive statistical summary for each standard listed under *Recovery Procedures* in Delphi Round 2. Standard #89 - identifying security needs received the highest mean importance rating of 4.57, closely followed by Standard #94 - the need to have written contracts or mutual aid agreements in effect with local and out of state emergency responders (4.29). Identifying insurance needs (Standard #92) was least

important in this category with a mean score of 3.81.

Table 10: Recovery Procedures – Round 2 Delphi Responses

Recovery Procedures	Mean	SD	Mdn
89. Identify security needs.	4.57	.68	5.00
90. Contracts in place for immediate restoration.	4.24	.77	4.00
91. Identify secondary locations to hold event bookings.	4.00	.71	4.00
92. Identify insurance needs.	3.81	.81	4.00
93. Campus setting with class cancellations addressed.	4.00	.78	4.00
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	4.29	.78	4.00

Scale (1-Low; 5-High)

Table 11 presents a descriptive statistical summary for each standard listed under *Communications* in Delphi Round 2. Standard #98 - megaphones for crowd control received the lowest mean importance score of 4.00. All other standards received a score of 4.10 or higher. Some of the highest importance scores were assigned to Standard #103 - identifying a chain of command (4.57) and Standard #104 - providing sequence of notification (4.67), Standard #99 - access to hand held radios (4.52) and Standard #107 - reliable communication systems with backups in place (4.62).

Table 11: Communications – Round 2 Delphi Responses

Communications	Mean	SD	Mdn
95. Communications cross jurisdictional, reporting, and management lines.	4.38	.81	5.00
96. Command Center should have direct access to emergency communication system.	4.52	.81	5.00
97. In house loop tapes for immediate communications.	4.10	1.00	4.00
98. Megaphones for crowd control.	4.00	1.05	4.00
99. Hand held radios with minimum 10 channels.	4.52	.87	5.00
100. Each agency radio channel is also independent in case there is a breach of security.	4.48	.87	5.00

101.	Signal enhancement (repeater) of emergency responder's communications for in-house use.	4.48	.87	5.00
102.	Wireless cell service with phone to phone and group talk communication capability.	4.33	.73	4.00
103.	Identify a chain of command (decision makers).	4.57	.68	5.00
104.	Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.	4.67	.48	5.00
105.	Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	4.38	.74	5.00
106.	Communications established and checked with all emergency responders prior to the game.	4.62	.67	5.00
107.	Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	4.62	.50	5.00
108.	Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	4.67	.48	5.00

Scale (1-Low; 5-High)

Table 12 presents a descriptive statistical summary for each standard listed under *Security Personnel* in Delphi Round 2. From the data gathered it is important for security personnel to be included in all training and planning activities to ensure they are aware of their duties and responsibilities (Standard #109 - 4.57). An interesting finding was the panel's importance rating for background checks on personnel (Standard #113) was one of the lowest in the category (4.29) but still rated highly.

Table 12: Security Personnel – Round 2 Delphi Responses

Security Personnel	Mean	SD	Mdn
109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	4.57	.68	5.00
110. Security personnel are provided by licensed and certified	4.48	.60	5.00

providers.

111. Physical plant security personnel mandatory with full time staff under the direction of Security Director.	4.57	.60	5.00
112. Game Day Event Security Director in-house or vendor hire.	4.29	.78	4.00
113. All personnel must have background check.	4.29	1.01	4.50

Scale (1-Low; 5-High)

Table 13 presents a descriptive statistical summary for each standard listed under *Training, Modeling, and Simulation* in Delphi Round 2. The average importance ratings in this category ranged from 4.00 to 4.62. Standard #124 - campus police and safety officers trained in bomb threat response was of most importance with a mean score of 4.62. Standard #117 - conducting evacuation simulations (4.23), Standard #121 - practicing emergency drills (4.48), Standard #120 - conducting table top exercises (4.35), and Standard #125 - training of all vendors, ushers, and volunteers in security awareness (4.55) were important to the Delphi panel.

Table 13: Training, Modeling, and Simulation – Round 2 Delphi Responses

Training, Modeling, and Simulation	Mean	SD	Mdn
114. Initial training in guest relations, problem solving and basic security procedures.	4.14	.96	4.00
115. Crowd control and crowd behavior techniques.	4.38	.87	5.00
116. International Association of Assembly Managers “best practices” awareness.	4.00	.82	4.00
117. Conduct annual evacuation simulations.	4.23	.81	4.00
118. Provide detailed training on inspection procedures to all security staff.	4.57	.60	5.00
119. Train access control personnel in credential recognition and access.	4.48	.75	5.00
120. Conduct table top exercises regarding all plans, practices, and procedures.	4.35	.813	5.00
121. Conduct at least one annual emergency drill prior to or early in the season.	4.48	.60	5.00

122.	During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	4.57	.60	5.00
123.	Include Emergency Management personnel in policy development and training.	4.52	.60	5.00
124.	All Campus Police and Safety Officers are trained in bomb threat response.	4.62	.59	5.00
125.	All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.	4.55	1.01	5.00
126.	Ticket taker responsibilities separate and distinct from those having security responsibilities.	4.45	.67	5.00

Scale (1-Low; 5-High)

Table 14 presents a descriptive statistical summary for each standard listed under *WMD – Toxic Materials Protection* in Delphi Round 2. The Delphi panel assigned the highest importance rating (4.55) to Standard #133 - remove all potentially dangerous chemicals or materials from the stadium. This category did not receive any mean scores lower than 4.10.

Table 14: WMD – Toxic Materials Protection – Round 2 Delphi Responses

WMD – Toxic Materials Protection		Mean	SD	Mdn
127.	Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.	4.45	.74	5.00
128.	On site decontamination locations identified.	4.18	1.05	4.50
129.	Banner planes identified, inspected, monitored, and restricted.	4.25	.91	4.50
130.	For any WMD, the scene is under the control of the Emergency Management Director.	4.10	1.00	4.00
131.	All Campus Police and Safety Officers trained to the WMD/ CBRNE/Hazmat awareness level.	4.14	.99	4.00
132.	A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.	4.27	.94	5.00
133.	All potentially dangerous chemicals or materials are permanently removed from the stadium.	4.55	.74	5.00

134. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.	4.41	.73	5.00
--	------	-----	------

Scale (1-Low; 5-High)

Delphi Round 3 Findings

The 23 participants who responded to Delphi 2 received Delphi 3. Delphi 3 was distributed by email and fax. Participants received a list of 134 standards and again were asked to rate each standard on a 5-point Likert scale as to the degree of importance (1 = very low; 2 = moderately low; 3 = average; 4 = moderately high; 5 = very high).

Participants also received descriptive information about how the group responded and asked to consider the group response before re-rating each item. Twenty-two of the 23 participants successfully completed the survey (78.6%). A copy of Delphi survey 3 can be found in Appendix E. High mean scores indicated a high level of importance and low standard deviations (low variance) indicated a high level of consensus. Table 15 presents a descriptive statistical summary for each standard listed under *Perimeter Control* in Delphi Round 3. Standard #1 – Establish a secure perimeter, Standard #2 – lock down 24 hours prior to event, Standard #3 – police patrol, and Standard #6 – secure and protect HVAC, mechanical, gas, and fuel systems received the highest mean score of 4.36. Standard #4 - bomb dog teams inspect facilities after lock down was rated the lowest at 3.62, consistent with Round 2 findings.

Table 15: Perimeter Control – Round 3 Delphi Responses

Perimeter Control	Mean	SD	Mdn
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.	4.36	.79	5.00
2. Lock down stadium 24 hours prior to an event and allow only controlled access.	4.36	.90	5.00

3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.	4.36	.73	4.50
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.	3.62	.92	4.00
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.	3.64	1.10	4.00
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.	4.36	.79	4.50
7. Security assigned to guard vulnerable systems, including air takes.	3.73	.70	4.00
8. Check and empty dumpsters and trash receptacles regularly.	4.00	.82	4.00
9. Do not place dumpsters under structural supports when and where possible.	4.18	.85	4.00
10. Establish a 500-foot secure outer perimeter around the stadium.	4.09	.81	4.00
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.	3.68	1.00	3.50
12. All campus buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	3.75	.85	4.00
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	3.75	.91	4.00

Scale (1-Low; 5-High)

Table 16 presents a descriptive statistical summary for each standard listed under *Access Control* in Delphi Round 3. Standard #15 - publicize policies concerning inspections (4.73) and Standard #17 - locating security personnel at each entry point (4.64) were among the highest rated standards in this category. Tickets containing a hologram (Standard #27) and electronic scanning of tickets (Standard #28) were among the lowest rated in this category with mean scores of 3.77 and 3.64 respectively.

Table 16: Access Control – Round 3 Delphi Responses

Access Control	Mean	SD	Mdn
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.	4.50	.69	5.00
15. Publicize the policy concerning inspections and identify prohibited items.	4.73	.55	5.00
16. No re-entry except for medical emergency.	4.14	1.17	4.50
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	4.64	.58	5.00
18. Utilize tables outside entry gates for bag inspections.	4.36	.90	5.00
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	4.10	.64	4.00
20. Portable metal detectors at stadium entry gates.	4.14	.83	4.00
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	4.50	.86	5.00
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	4.23	.75	4.00
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	4.45	.86	5.00
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	4.32	.72	4.00
25. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted team areas.	4.50	.51	4.50
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	4.18	.80	4.00
27. All tickets contain a hologram for ticket validation.	3.77	.75	4.00
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	3.64	.85	4.00
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	4.32	.90	5.00

30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	3.95	.95	4.00
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	3.77	.87	4.00
32. Open all main entry gates at the same time.	3.95	.90	4.00
33. Schedule limited daily or weekly delivery times for vendors.	3.68	.89	3.50
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	3.91	.92	4.00
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	4.45	.80	5.00
36. No vendor deliveries should be allowed within 90 minutes of the game.	4.18	.85	4.00
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	4.55	.51	5.00

Scale (1-Low; 5-High)

Table 17 presents a descriptive statistical summary for each standard listed under *Credentialing* in Delphi Round 3. Only one of the *Credentialing* standards received a mean score lower than 4.36. Standard #38 - requiring background checks for vendors, employees, contractors, students and volunteers (3.91) had the lowest mean score. Standard #45 - require credentials to be worn at all times was highly rated at 4.50.

Table 17: Credentialing – Round 3 Delphi Responses

Credentialing	Mean	SD	Mdn
38. Background checks required for all vendors, employees, contractors, students and volunteers.	3.91	.87	4.00
39. Simplify credential systems indicating zone access and color code by game function.	4.41	.85	5.00
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	4.36	.79	5.00
41. Credentials are substantially different from those used in prior seasons.	4.45	.67	5.00
42. Use a hologram or other protection on the credential to reduce	4.36	.79	5.00

the potential for counterfeiting.

43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	4.41	.80	5.00
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	4.14	.89	4.00
45. Require all credentials to be worn at all times and clearly displayed.	4.50	.74	5.00
46. Require all team bench staff, except players in uniform, to wear a game credential.	4.36	.85	5.00
47. To assist with access control, display credential boards at all access control points.	4.45	.74	5.00

Scale (1-Low; 5-High)

Table 18 presents a descriptive statistical summary for each standard listed under *Physical Protection Systems* in Delphi Round 3. Standards in this category were assigned mean scores ranging from 3.86 (Standard #50 - bomb removal equipment on site) to 4.59 (Standard #60 - enhanced lighting of gated areas and digital security system monitored by command center). Establishing an inner perimeter (Standard #48), utilizing barriers (Standard #49), and having digital camera monitoring capabilities (Standard #58) were highly rated. Having portable hazmat smart stripes and detection equipment on site (Standard #61) received one of the lowest mean scores of 3.91.

Table 18: Physical Protection Systems – Round 3 Delphi Responses

Physical Protection Systems	Mean	SD	Mdn
48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	4.41	.80	5.00
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	4.27	.70	4.00
50. Bomb removal equipment is on site.	3.86	.99	4.00
51. Annual structural inspection of entire facility is required and documented.	4.27	.70	4.00
52. All utility areas alarmed and contain card access entry points.	4.09	.92	4.00

53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	3.86	.94	4.00
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	4.27	.96	5.00
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	4.36	.90	5.00
56. 24-hour camera surveillance of perimeter and playing field.	4.27	.94	4.50
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	4.41	.80	5.00
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	4.59	.80	5.00
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	4.23	.81	4.00
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	4.59	.80	5.00
61. Portable Hazmat Smart Stripes and detection equipment is on site.	3.91	.92	4.00

Scale (1-Low; 5-High)

Table 19 presents a descriptive statistical summary for each standard listed under *Risk Management* in Delphi Round 3. Standards 62 – 65 were all rated moderately to highly important. Developing risk management plans for athletic department events (Standard #62) and completing these plans in conjunction with local law enforcement (Standard #64) were assigned mean scores of 4.45 and 4.48 respectively.

Table 19: Risk Management – Round 3 Delphi Responses

Risk Management (threat/risk assessment)	Mean	SD	Mdn
62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	4.45	1.01	5.00
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	4.36	.90	5.00
64. Complete plans in conjunction with local law enforcement	4.48	.75	5.00

anti-terror task force.

65. Conduct weekly game management meetings (include risk management issues).	4.25	.97	5.00
--	------	-----	------

Scale (1-Low; 5-High)

Table 20 presents a descriptive statistical summary for each standard listed under *Emergency Management* in Delphi Round 3. No standard in this category received a mean importance rating lower than 4.33. Standards in this category were assigned means scores ranging from 4.33 to 4.73. Develop, maintain, and practice Emergency Response Plans (Standard #66 - 4.73) and Emergency Evacuation Plans (Standard #67 - 4.68), and keeping all emergency routes clear throughout the event on campus (Standard #84 - 4.73) were among the highest rated standards.

Table 20: Emergency Management – round 3 Delphi Responses

Emergency Management (response & evacuation)	Mean	SD	Mdn
66. Develop, maintain, and practice Emergency Response Plan.	4.73	.55	5.00
67. Develop, maintain, and practice Emergency Evacuation Plan.	4.68	.57	5.00
68. Coordinate emergency plan with local, state and federal emergency management authorities.	4.68	.57	5.00
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	4.68	.65	5.00
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	4.62	.67	5.00
71. Establish a security command and control center (primary and secondary location).	4.55	.74	5.00
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	4.50	.74	5.00
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	4.55	.74	5.00
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	4.50	.80	5.00

75. The Command Center has a view of the playing field to facilitate decision making.	4.36	.79	5.00
76. Provide a secure incident room designated for decision makers.	4.33	.86	5.00
77. Identification of management teams for response to command and control.	4.41	.73	5.00
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	4.59	.73	5.00
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	4.64	.66	5.00
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.	4.55	.67	5.00
81. Develop Emergency Medical Plan.	4.55	.74	5.00
82. Designate primary and secondary triage and transport sites.	4.45	.80	5.00
83. Identify and secure emergency routes in and out of the stadium facility.	4.59	.73	5.00
84. All emergency routes remain clear throughout the event on campus.	4.73	.55	5.00
85. Emergency Management response and evacuation personnel on site throughout event.	4.55	.74	5.00
86. More than one ambulance and at least two Certified EMT's onsite.	4.55	.74	5.00
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	4.64	.66	5.00
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	4.68	.65	5.00

Scale (1-Low; 5-High)

Table 21 presents a descriptive statistical summary for each standard listed under *Recovery Procedures* in Delphi Round 3. Standard #89 - identify security needs (4.67) and Standard #94 - having written contracts or mutual aid agreements in effect (4.43)

were assigned the highest mean importance ratings by the panel of experts.

Table 21: Recovery Procedures – Round 3 Delphi Responses

Recovery Procedures	Mean	SD	Mdn
89. Identify security needs.	4.67	.73	5.00
90. Contracts in place for immediate restoration.	4.24	.83	4.00
91. Identify secondary locations to hold event bookings.	3.95	.74	4.00
92. Identify insurance needs.	3.90	.70	4.00
93. Campus setting with class cancellations addressed.	4.05	.81	4.00
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	4.43	.81	5.00

Scale (1-Low; 5-High)

Table 22 presents a descriptive statistical summary for each standard listed under *Communications* in Delphi Round 3. Standards 95 – 108 were assigned mean scores ranging from 4.14 to 4.76. Standard #103 - identifying a chain of command was of most importance to the panel of experts with a mean score of 4.76.

Table 22: Communications – Round 3 Delphi Responses

Communications	Mean	SD	Mdn
95. Communications cross jurisdictional, reporting, and management lines.	4.57	.75	5.00
96. Command Center should have direct access to emergency communication system.	4.57	.75	5.00
97. In house loop tapes for immediate communications.	4.33	.86	5.00
98. Megaphones for crowd control.	4.14	.91	4.00
99. Hand held radios with minimum 10 channels.	4.67	.58	5.00
100. Each agency radio channel is also independent in case there is a breach of security.	4.62	.67	5.00
101. Signal enhancement (repeater) of emergency responder's communications for in-house use.	4.55	.86	5.00
102. Wireless cell service with phone to phone and group talk communication capability.	4.41	.73	5.00

103. Identify a chain of command (decision makers).	4.76	.44	5.00
104. Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.	4.59	.80	5.00
105. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	4.50	.80	5.00
106. Communications established and checked with all emergency responders prior to the game.	4.64	.73	5.00
107. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	4.59	.73	5.00
108. Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	4.68	.73	4.50

Scale (1-Low; 5-High)

Table 23 presents a descriptive statistical summary for each standard listed under *Security Personnel* in Delphi Round 3. Standards 109 – 113 were rated between 4.41 and 4.64. The panel of experts believe security personnel should be included in all training and planning activities (Standard #109) to be of most importance with the highest mean score of 4.64.

Table 23: Security Personnel – Round 3 Delphi Responses

Security Personnel	Mean	SD	Mdn
109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	4.64	.58	5.00
110. Security personnel are provided by licensed and certified providers.	4.55	.60	5.00
111. Physical plant security personnel mandatory with full time staff under the direction of Security Director.	4.41	.80	5.00
112. Game Day Event Security Director in-house or vendor hire.	4.50	.60	5.00
113. All personnel must have background check.	4.45	.74	5.00

Scale (1-Low; 5-High)

Table 24 presents a descriptive statistical summary for each standard listed under *Training, Modeling, and Simulation* in Delphi Round 3. Providing training on inspection procedures to security staff (Standard #118), credential recognition to access control personnel (Standard #119), and security awareness to ushers, vendors, and volunteers (Standard #125), were assigned the highest importance rating of 4.59.

Table 24: Training, Modeling, and Simulation – Round 3 Delphi Responses

Training, Modeling, and Simulation	Mean	SD	Mdn
114. Initial training in guest relations, problem solving and basic security procedures.	4.36	.73	4.50
115. Crowd control and crowd behavior techniques.	4.55	.60	5.00
116. International Association of Assembly Managers “best practices” awareness.	3.91	.69	4.00
117. Conduct annual evacuation simulations.	4.14	.64	4.00
118. Provide detailed training on inspection procedures to all security staff.	4.59	.59	5.00
119. Train access control personnel in credential recognition and access.	4.59	.67	5.00
120. Conduct table top exercises regarding all plans, practices, and procedures.	4.41	.73	5.00
121. Conduct at least one annual emergency drill prior to or early in the season.	4.55	.60	5.00
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	4.55	.60	5.00
123. Include Emergency Management personnel in policy development and training.	4.59	.59	5.00
124. All Campus Police and Safety Officers are trained in bomb threat response.	4.55	.67	5.00
125. All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.	4.59	.67	5.00
126. Ticket taker responsibilities separate and distinct from those having security responsibilities.	4.41	.73	5.00

Scale (1-Low; 5-High)

Table 25 presents a descriptive statistical summary for each standard listed under *WMD – Toxic Materials Protection* in Delphi Round 3. The panel of experts indicated with the highest mean score of 4.59 that all potentially dangerous chemicals or materials be permanently removed from the sport stadium (Standard #133). All standards in this category were rated between 4.23 and 4.59.

Table 25: WMD – Toxic Materials Protection – Round 3 Delphi Responses

WMD – Toxic Materials Protection	Mean	SD	Mdn
127. Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.	4.45	.67	5.00
128. On site decontamination locations identified.	4.23	.92	5.00
129. Banner planes identified, inspected, monitored, and restricted.	4.36	.73	4.50
130. For any WMD, the scene is under the control of the Emergency Management Director.	4.27	.94	5.00
131. All Campus Police and Safety Officers trained to the WMD/ CBRNE/Hazmat awareness level.	4.32	.95	5.00
132. A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.	4.32	.90	4.50
133. All potentially dangerous chemicals or materials are permanently removed from the stadium.	4.59	.80	5.00
134. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.	4.50	.80	5.00

Scale (1-Low; 5-High)

Appendix G provides a comparison of means for each standard between Round 2 and 3 of the Delphi study. Eighty-six of the 134 standards were assigned a positive net change between Round 2 and 3, 41 of the standards were assigned a negative net change, and 7 standards were assigned the same mean importance scores. Appendix H provides an overview of the 134 identified standards, including their importance means and

standard deviations after the third and final Delphi round. A one-way ANOVA was conducted after Delphi Round 3 to test Hypothesis 1.

Hypothesis

1. Significant differences will exist in perceptions of importance for developed standards between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management director's.

A level of significance was set at $\leq .0004$ to correct for Type I error. No significant differences existed in perception of importance for each standard between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors. Hypothesis 1 was rejected. Appendix I highlights the means for athletic facility managers, campus police chiefs, local sheriffs, and local emergency management directors after Delphi Round three for the 134 identified standards.

Through a series of interviews and a three round Delphi study a consensus was reached among four key groups involved in intercollegiate game day security operations. A total of 134 standards were identified and agreed upon through an open-ended Delphi Round 1 questionnaire and importance ratings gathered in Delphi Rounds 2 and 3. Importance means gathered highlighted some critical areas of security to be addressed by university sport security teams. Credentialing, Emergency Management, Risk Management, Communications, Security Personnel, and Training, Modeling, and Simulation received some of the highest rated importance means for standards listed in that category.

CHAPTER V

SUMMARY OF FINDINGS

This chapter presents a summary of findings, a table of finalized standards developed through the research process, discussion of findings, recommendations for future research and practice, and conclusions.

The purpose of this study was to establish standards for effective security management of university sport venues. The benefit of establishing standards is to create consistency in security policy and procedures at university sports venues, thereby minimizing risk and safeguarding a university's critical assets – the fans, players, officials, vendors, media personnel, local community, and stadium structure. In order to develop standards for effective security management of university sport venues an email interview process and Delphi study was employed to gather new knowledge in the sport security field. Four security experts were interviewed and a preliminary list of 141 standards identified for Round 1 of the Delphi Study. Twenty-eight (28) sport security experts participated in Delphi Round 1. Twenty-seven (27) participants responded with a return rate of 96.4%. Through Round 1 analysis 134 standards were retained for Round 2. Twenty-six (26) participants received Round 2 and were asked to rate the level of importance for each standard on a 5-point Likert scale (1 = very low; 2 = moderately low; 3 = average; 4 = moderately high; 5 = very high). Twenty-three (23) participant's responded (82.1%) and descriptive statistics for importance ratings were calculated. Of the 134 standards listed, mean importance ratings ranged from 3.38 to 4.76 indicating a moderate to high degree of importance. Delphi 3 was distributed to the 23 participants who completed Round 2. Participants received descriptive

information about how the group responded in the previous round and asked to consider the group response before re-rating each item. Twenty-two participant's responded (78.6%) and descriptive statistics for importance ratings were calculated. Of the 134 standards listed, mean importance ratings in Round 3 ranged from 3.62 to 4.76.

Standard #4 - bomb dog teams and bomb removal teams inspect the facility after lock down and four hours prior to opening received the lowest mean importance score in Round 2 (3.38) and Round 3 (3.62) of the Delphi study. Standard #14 - prohibit coolers, bags, backpacks, containers, explosives, weapons, and outside food and beverages received the highest mean importance score (4.76) in Round 2 but not in Round 3. Standard #103 - identify a chain of command (decision makers) received the highest mean importance score (4.76) in Round 3. Standard #15 - publicize policy concerning inspections and prohibited items, Standard #66 - develop, maintain, and practice Emergency Response Plan, and Standard #84 - emergency routes remain clear throughout the event closely followed with mean importance scores of 4.73. The researcher set an elimination level at a mean score of 3 or below indicating average to low importance. No standard was assigned a mean importance score low enough to warrant elimination.

A one-way ANOVA was conducted after round three Delphi to determine if significant differences existed in perception of importance for each standard (134) between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors. A level of significance was set at $\leq .0004$ to correct for Type I error. No significant (NS) differences existed in perception of importance for developed standards between athletic facility managers, local sheriffs, campus police chiefs, and local county emergency management directors. Hypothesis 1 was rejected

indicating a high level of agreement among practicing professionals.

Table 26 presents the research-based standards for effective security management of university sport venues.

Table 26: Standards for Effective Security Management of University Sport Venues
Perimeter Control

1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.
2. Lock down stadium 24 hours prior to an event and allow only controlled access.
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.
7. Security assigned to guard vulnerable systems, including air takes.
8. Check and empty dumpsters and trash receptacles regularly.
9. Do not place dumpsters under structural supports when and where possible.
10. Establish a 500-foot secure outer perimeter around the stadium.
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.
12. All buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.

Access Control

14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.
15. Publicize the policy concerning inspections and identify prohibited items.
16. No re-entry except for medical emergency.
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.

18. Utilize tables outside entry gates for bag inspections.
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.
20. Portable metal detectors at stadium entry gates.
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.
25. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted team areas.
26. Each entry point has a ticket taker equipped with access management equipment and scanners.
27. All tickets contain a hologram for ticket validation.
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.
32. Open all main entry gates at the same time.
33. Schedule limited daily or weekly delivery times for vendors.
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.
36. No vendor deliveries should be allowed within 90 minutes of the game.
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.

Credentialing

38. Background checks required for all vendors, employees, contractors, students and volunteers.
39. Simplify credential systems indicating zone access and color code by game function.
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.
41. Credentials are substantially different from those used in prior seasons.
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.
45. Require all credentials to be worn at all times and clearly displayed.
46. Require all team bench staff, except players in uniform, to wear a game credential.
47. To assist with access control, display credential boards at all access control points.

Physical Protection Systems

48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.
50. Bomb removal equipment is on site.
51. Annual structural inspection of entire facility is required and documented.
52. All utility areas alarmed and contain card access entry points.
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.
54. Install internal and external cameras (digital) with pan, tilt, and zoom.
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.
56. 24-hour camera surveillance of perimeter and playing field.
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.

59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.
61. Portable Hazmat Smart Stripes and detection equipment is on site.

Risk Management

62. Develop risk management plans for Athletic Department events and review on an ongoing basis.
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.
64. Complete plans in conjunction with local law enforcement anti-terror task force.
65. Conduct weekly game management meetings (include risk management issues).

Emergency Management

66. Develop, maintain, and practice Emergency Response Plan.
67. Develop, maintain, and practice Emergency Evacuation Plan.
68. Coordinate emergency plan with local, state and federal emergency management authorities.
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.
71. Establish a security command and control center (primary and secondary location).
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).
75. The Command Center has a view of the playing field to facilitate decision making.
76. Provide a secure incident room designated for decision makers.
77. Identification of management teams for response to command and control.

78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.
81. Develop Emergency Medical Plan.
82. Designate primary and secondary triage and transport sites.
83. Identify and secure emergency routes in and out of the stadium facility.
84. All emergency routes remain clear throughout the event on campus.
85. Emergency Management response and evacuation personnel on site throughout event.
86. More than one ambulance and at least two Certified EMT's onsite.
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.

Recovery Procedures

89. Identify security needs.
90. Contracts in place for immediate restoration.
91. Identify secondary locations to hold event bookings.
92. Identify insurance needs.
93. Campus setting with class cancellations addressed.
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.

Communications

95. Communications cross jurisdictional, reporting, and management lines.
96. Command Center should have direct access to emergency communication system.
97. In house loop tapes for immediate communications.
98. Megaphones for crowd control.
99. Hand held radios with minimum 10 channels.
100. Each agency radio channel is also independent in case there is a breach of security.

101. Signal enhancement (repeater) of emergency responder's communications for in-house use.
102. Wireless cell service with phone to phone and group talk communication capability.
103. Identify a chain of command (decision makers).
104. Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.
105. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.
106. Communications established and checked with all emergency responders prior to the game.
107. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.
108. Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.

Security Personnel

109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.
110. Security personnel are provided by licensed and certified providers.
111. Physical plant security personnel mandatory with full time staff, under the direction of Security Director.
112. Game Day Event Security Director in-house or vendor hire.
113. All personnel must have background check.

Training, Modeling, and Simulation

114. Initial training in guest relations, problem solving and basic security procedures.
115. Crowd control and crowd behavior techniques.
116. International Association of Assembly Managers "best practices" awareness.
117. Conduct annual evacuation simulations.
118. Provide detailed training on inspection procedures to all security staff.
119. Train access control personnel in credential recognition and access.
120. Conduct table top exercises regarding all plans, practices, and procedures.

121. Conduct at least one annual emergency drill prior to or early in the season.
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.
123. Include Emergency Management personnel in policy development and training.
124. All Campus Police and Safety Officers are trained in bomb threat response.
125. All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.
126. Ticket taker responsibilities separate and distinct from those having security responsibilities.

WMD – Toxic Materials Protection

127. Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.
128. On site decontamination locations identified.
129. Banner planes identified, inspected, monitored, and restricted.
130. For any WMD, the scene is under the control of the Emergency Management Director.
131. All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level.
132. A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.
133. All potentially dangerous chemicals or materials are permanently removed from the stadium.
134. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.

Discussion

Established standards will assist university sport security management teams and provide consistency in security management practices among sport venues. Some sport organizations have developed security checklists and guidelines. For example, the NCAA have issued “planning options” for athletic department events, but there are currently no documented research-based standards for effective security management of university sport venues. The research study provided a final product of 134 standards in eleven

separate categories developed and adapted through a series of surveys with a panel of experts (field-based practitioners). The panel of experts was chosen based on their security expertise and knowledge in the sport event security management field.

Therefore, the outcome of this study has been a unified decision of best security practices by key personnel responsible for security operations at university sports events in the state of Mississippi. In addition, there were no significant differences in perceptions of importance for each standard reinforcing the thought that these groups are on the same page when planning and preparing security initiatives for sports events. With recent events, such as Hurricane Katrina, a lot of the media attention and review of recovery efforts was focused on the lack of communication and coordination efforts between various agencies.

In an ideal world, if all of the 134 standards can be implemented at university sports events the organization in question has taken necessary steps to protect its assets. Ultimately, the implementation and long term adherence to these standards should enhance security operations at university sports events. These standards can be used as a basis for key personnel to refer to when deciding what security measures are critical or should be made a priority when hardening their facility, especially if organizations have limited funding and can not implement all security initiatives.

Standards in the *Communication, Credentialing, and Training, Modeling, and Simulation* categories were assigned some of the highest mean importance scores. This finding was consistent with highlighted areas in the review of literature. Practitioners and researchers identified these areas as critical to effectively secure a sport venue. Therefore, university sport programs need to ensure these areas are addressed. It is extremely critical

for security staff to work as a team in the coordination of security operations during university sports events and to have in place effective communication systems. Training, Modeling, and Simulation was another key area identified by the panel of experts. Athletic department staff, hired security staff, and all other game day staff (ushers, vendors, ticket takers, etc.) must be properly trained and aware of security policies and practices. They must understand their role and responsibility during game day operations.

In the qualitative feedback part of this study several of the panel experts expressed concern about the cost of implementing the established security standards and maintaining them over the long term. Also included in the feedback was the concern of liability issues and whether university sport programs will be held accountable to these standards even if they did not have the resources to enforce. Assessing the cost or perception of cost on achieving standards was beyond the scope of this study but the researcher will acknowledge such comments for future research initiatives and practical implications. For example, if an event was to occur what would be the potential economic impact? This provides data for organizations to consider their return on investment in security measures.

With increasing pressure to enhance security efforts at university sports events there may be some concern about the adverse affect on the sport consumer's experience. Implementing new security policies may agitate or disgruntle fans who have been accustomed to attending and enjoying their sport experience in a more lax environment. Intercollegiate sport marketing departments will be faced with this challenge. Collegiate marketing departments must overcome these barriers to retain customers and continue to provide a positive fun experience for spectators. The athletic marketing director will have

to work closely with security personnel to ensure security policies and practices do not infringe upon the consumer experience.

The researcher identified some limitations during the research study. Twenty-two (22) of the 28 Delphi panel successfully completed all three rounds (78.6%). Even though this is a high return rate for a Delphi study, the groups (athletic facility manager, campus police chief, sheriff, and emergency management director) varied in size when calculating descriptive statistics for Round 2 and 3 of the Delphi analysis. Also, the Delphi survey was very extensive with 134 security standard items which may have contributed to only 22 participants completing all three rounds.

The research study and findings have provided several recommendations for future research initiatives and practical implications:

Recommendations for Future Research

1. Replicate study on a national basis to ensure transferability so researchers can infer findings beyond the scope of this study.
2. Determine the degree to which other universities/athletic conferences are implementing the research-based standards.
3. Assess importance perceptions of key personnel from other universities/athletic conferences regionally and/or nationally.
4. Determine whether universities have the necessary financial means, resources, manpower, training, or equipment to implement research-based standards.
5. Determine possible implications of new security standards on sport consumers, sport marketers, sport financial officers, and potential legality issues for intercollegiate athletic departments and universities.

6. Assess potential economic impact of disasters to justify adherence to identified standards and identify further benefits to implementing and maintaining security standards for university sports events.
7. Conduct a factor analysis (of the 134 standards) to determine clusters or factors to reduce the number of standards to a more manageable list.

Recommendations for Practice

1. Plan, add, or implement university curriculums and certification programs in the area of sports event security management.
2. Establish an annual sports event security management conference for academics and professionals to serve as a networking arena and hub for dissemination of new knowledge.
3. Develop training seminars for key personnel involved in game day security operations of intercollegiate sports events. All staff members and hired security personnel must be aware of their role and responsibility on game day.
4. Conduct grant writing workshops for intercollegiate security teams to enhance knowledge regarding proposal development and grant opportunities available through the Department of Homeland Security and FEMA, filtered through local county emergency management agencies.
5. Conduct external audits to evaluate the degree to which these research-based standards are in place and being implemented.
6. Nation-wide research results in this area would provide evidence to the NCAA that there is a justified need for consistent security standards and grounds to seek endorsement.

7. University sports event security personnel may utilize these standards to prioritize security measures according to importance due to availability of limited funds and need to harden their facility.

Conclusions

Complacency may be overwhelming the nation today as 9/11 appears so long ago and some of us forget the threat that exists in our ever changing world. It is no longer acceptable to have the attitude “it will never happen to us”. Planning and preparation are an integral component of any security directive to detect, deter, respond, and mitigate incidents, whether it is a terrorist event, natural disaster, or crowd management issue. American sports leagues, teams, and venue operators must realize the risk of complacency and continue to plan, test, and enhance security efforts. According to Hurst, Zoubek, & 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). This study has identified standards to assist and support university sports event security teams in their quest to protect our most valuable assets – our people!

APPENDIX A



The University of
Southern Mississippi

Institutional Review Board

118 College Drive #5147
Hattiesburg, MS 39406-0001
Tel: 601.266.6820
Fax: 601.266.5509
www.usm.edu/irb

HUMAN SUBJECTS PROTECTION REVIEW COMMITTEE NOTICE OF COMMITTEE ACTION

The project has been reviewed by The University of Southern Mississippi Human Subjects Protection Review Committee in accordance with Federal Drug Administration regulations (21 CFR 26, 111), Department of Health and Human Services (45 CFR Part 46), and university guidelines to ensure adherence to the following criteria:

- The risks to subjects are minimized.
- The risks to subjects are reasonable in relation to the anticipated benefits.
- The selection of subjects is equitable.
- Informed consent is adequate and appropriately documented.
- Where appropriate, the research plan makes adequate provisions for monitoring the data collected to ensure the safety of the subjects.
- Where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of all data.
- Appropriate additional safeguards have been included to protect vulnerable subjects.
- Any unanticipated, serious, or continuing problems encountered regarding risks to subjects must be reported immediately, but not later than 10 days following the event. This should be reported to the IRB Office via the "Adverse Effect Report Form".
- If approved, the maximum period of approval is limited to twelve months. Projects that exceed this period must submit an application for renewal or continuation.

PROTOCOL NUMBER: **25102502**

PROJECT TITLE: **Standards for Effective Security of University Sports Venues**

PROPOSED PROJECT DATES: **09/01/05 to 05/01/06**

PROJECT TYPE: **Dissertation or Thesis**

PRINCIPAL INVESTIGATORS: **Stacey Hall**

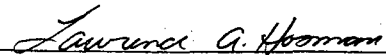
COLLEGE/DIVISION: **College of Health**

DEPARTMENT: **Human Performance & Recreation**

FUNDING AGENCY: **N/A**

HSPRC COMMITTEE ACTION: **Expedited Review Approval**

PERIOD OF APPROVAL: **11/03/05 to 11/02/06**



Lawrence A. Hosman, Ph.D.
HSPRC Chair

11-05-05

Date

APPENDIX B
Standards for Effective Security Management of University Sport Venues
A Doctoral Dissertation Study
By
Stacey A. Hall

The purpose of my study is to establish standards for effective security management of university sport venues. Establishing standards will provide consistency in security management practices among sport venues in America.

Due to your expertise and knowledge in security management you have been selected to serve on a panel of experts. The researcher hopes to gain new knowledge in the field of sports event security management. Feedback provided will be utilized in developing a list of standards or “best practices” for sport event venues. These standards will then be used in a Delphi study to reach consensus among sports event security professionals.

“Standards” defined: a written or visual measurable guideline describing an expected behavior, performance, product or service.

Examples of standards:

Perimeter Control

1. The stadium/arena is locked down 36 hours prior to kick-off.

Risk Management

1. A written risk management plan has been developed and is updated annually.

Emergency Management

1. An emergency response plan has been developed, updated, and practiced at least once a year.

What standards, under the following categories, do you perceive to be important in effectively securing sport venues? **Please feel free to add or modify categories.**

1. Perimeter Control
2. Access Control
3. Credentialing
4. Physical Protection Systems
5. Risk Management (threat/risk assessment)
6. Emergency Management (response and evacuation)
7. Recovery Procedures
8. Communications
9. Security Personnel
10. Training, Modeling, and Simulation
11. WMD – Toxic materials protection
12. Other:

Please respond by Friday, December 9, 2005. You can email your responses to Stacey.A.Hall@usm.edu or fax to 601-266-4445. If you have any questions please call 601-266-6183. Thank you for your participation. It is greatly appreciated.

APPENDIX C

January 20, 2006

Stacey Hall, MBA
Operations Coordinator
Center for Sports Event Security Management
The University of Southern Mississippi
118 College Drive #5142
Hattiesburg, MS 39406-0001

RE: Standards for effective security management of university sport venues

I am currently working on a doctoral dissertation in the area of sports event security management. The purpose of my study is to establish standards for effective security management of university sport venues. Establishing standards will provide consistency in security management practices among sport venues in America.

Due to your expertise and knowledge in security management you have been selected to serve on a panel of experts. The researcher hopes to gain new knowledge in the field of sports event security management. Feedback provided will be utilized in developing a list of standards or "best practices" for sport event venues.

I am asking for your participation in a three-round survey that will take no more than 10-15 minutes of your time for each of the three surveys. The survey distribution will begin in February, 2006. I understand you are extremely busy but would greatly appreciate your assistance.

Please respond to the following email Stacey.A.Hall@usm.edu or call 601-266-6183 with your intent to participate. Please identify the best method of contact i.e., email/ fax. Thank you for your time and consideration.

Yours Sincerely,

Stacey Hall

APPENDIX D

Standards for Effective Security Management of University Sport Venues A Doctoral Dissertation Study

By
Stacey A. Hall

Dear Participants:

The purpose of my study is to establish standards for effective security management of university sport venues. Establishing standards will provide consistency in security management practices among university sport venues in the U.S.A.

Interviews have been conducted with several sports event security experts in order to develop a set of standards or “best practices”. I am now asking each of you to review these standards and make necessary additions. Please add any new standards you believe to be critical in effectively securing a university sport venue. It is my goal to reach a consensus among key personnel involved in college game day operations regarding security management.

“Standards” defined: a written or visual measurable guideline describing an expected behavior, performance, product or service.

This is the first of three surveys that you will receive over the next four weeks. Each survey should take no longer than 15 minutes. Please complete and return via email Stacey.A.Hall@usm.edu or fax 601-266-4445.

A. Please check which of the following categories you are presently employed:

Dept. of Intercollegiate Athletics _____
 Campus Police _____
 Sheriff's Office _____
 Emergency Management Agency _____

B. Please review the following standards and add any new standards you believe critical in effectively securing a university sports event venue (you are also encouraged to comment/edit currently listed standards):

A. Perimeter Control

1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and people access points twelve (12) hours prior to the event.
2. Lock down stadium 12 hours prior to an event.
3. Only people with tickets, credentials/badges/passes/wristbands or coaches/players are allowed in the inner perimeter.
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and one (1) hour prior to opening.
5. The same teams remain on site throughout the event to regularly patrol the perimeter and facility and/or to react to reports.
6. K-9 bomb search of truck ramp and vehicles parked immediately adjacent to stadium.
7. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.
8. Police patrol one (1) hour before parking lots open.
9. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems. Test backup systems annually or in compliance with local codes to ensure they are properly maintained and functional.
10. Store flammables and combustibles in a secure area.
11. Security assigned to guard vulnerable systems, including air takes.
12. Install a central emergency shut-off switch for the HVAC system.
13. Keep facility clear of clutter and debris. Check and empty dumpsters and trash receptacles regularly.
14. Do not place dumpsters under structural supports when and where possible.
15. Establish a 100-foot secure outer perimeter around the stadium to the maximum extent possible.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

B. Access Control

1. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and no outside food or beverages, except as required for medical or family needs.

2. Baby bags allowed with baby in tow, tagged after search.
3. Publicize the policy concerning inspections and identify prohibited items.
4. No re-entry except for medical emergency.
5. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.
6. Ticket entry areas identified with standard pat down and /or hand metal detector usage.
7. Portable metal detectors at stadium entry gates.
8. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.
9. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.
10. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.
11. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.
12. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted team areas.
13. Each entry point has a ticket taker equipped with access management equipment and scanners.
14. All tickets contain a hologram for ticket validation.
15. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.
16. Ticket taker responsibilities separate and distinct from those having security responsibilities.
17. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.
18. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.
19. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors into and out of facility with appropriate department staff.
20. Open all main entry gates at the same time.
21. Schedule limited daily or weekly delivery times for vendors.
22. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.
23. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.
24. No vendor deliveries should be allowed within 90 minutes of the game unless the delivery is inspected and escorted by a security person.
25. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-

-
-

C. Credentialing

1. Background checks required for all vendors, employees, contractors, students and volunteers participating in stadium activities.
2. Simplify credential systems indicating zone access and color code by game function.
3. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.
4. Credentials are substantially different from those used in prior seasons.
5. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.
6. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.
7. Require those designated to pick up their credentials to do so in person, using government issued photo identification.
8. Require all credentials to be worn at all times and clearly displayed.
9. Require all team bench staff, except players in uniform, to wear a game credential.
10. To assist with access control, display credential boards at all access control points.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

D. Physical Protection Systems

1. Establish an inner perimeter (100 ft) with permanent and movable barricades and operationalized with law enforcement personnel.
2. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses. Configure the barriers in such a manner as to prevent any type of forced vehicle entry.
3. Bomb removal equipment is on site.
4. Annual structural inspection of entire facility is required and documented.
5. Stadium area gated for identifiable security area.
6. Parking lots unopened and sealed off except for business guests and employees.
7. Mag locks used and tied into fire alarm system.
8. All utility areas alarmed and contain card access entry points.
9. Intake vents hidden from view and alarmed for weighed objects/ biohazards.
10. Install internal and external cameras (digital) with pan, tilt, zoom and monitoring capability covering all vulnerable areas.
11. Cameras monitor all areas of the stadium and arena including the perimeter, surrounding exterior areas, concourses, seating bowl, and concession areas.
12. 24-hour camera surveillance of perimeter and inside bowl area.

13. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.
14. The system is digital and capable of being monitored at the Command Center and the Campus Police Department.
15. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.
16. The lighting of the gate areas enhanced to allow for searching of bags, and persons outside the gates with no flashlights.
17. Portable Hazmat Smart Stripes and detection equipment is on site.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

E. Risk Management (threat/risk assessment)

1. Develop risk management plans for Athletic Department events and University in general and review on an ongoing basis.
2. Training regarding risk management plans and polices is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.
3. Complete plans in conjunction with local law enforcement anti-terror task force.
4. Weekly game management meetings are conducted which include all of the above groups to review the previous event and prepare for the upcoming event. Risk management is assessed and addressed at each meeting.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

F. Emergency Management (response and evacuation)

1. Develop, maintain, and practice Emergency Management Plan.
2. Develop, maintain, and practice Emergency Evacuation Plan.
3. Include Emergency Management personnel in policy development and training.
4. Coordinate emergency plan with local, state and federal emergency management authorities.
5. Document in-house procedures for emergency response to local weather conditions, fire emergency, electrical and mechanical emergencies.
6. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.

7. Establish a security command and control center (primary and secondary location).
8. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).
9. Designate a backup Command Center in the event primary Command Center has to be evacuated.
10. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center. A mobile police command vehicle may be considered.
11. The Command Center has a view of the bowl and playing field to facilitate decision making.
12. Provide a secure incident room designated for decision makers. Monitors in the Command Center with feeds to monitors in the incident room may be beneficial.
13. Identification of management teams for response to command and control.
14. Copies of the Emergency Evacuation Plan along with a map indicating evacuation routes and identifying pre-determined security officer locations are maintained at the Command Center and the Campus Police Department.
15. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.
16. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.
17. Include an Emergency Medical Plan or write a separate plan.
18. Include clear procedures for a catastrophic event, requiring primary and secondary triage. Designate triage and transport sites. Identify and secure emergency routes in and out of the stadium facility.
19. All emergency routes remain clear throughout the event on campus.
20. Emergency Management response and evacuation personnel on site throughout event.
21. An ambulance and at least two Certified EMT's is onsite.
22. The stadium PA system, Communications system, data systems and the emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.
23. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders that may be required to respond in the event of an emergency.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-
-

G. Recovery Procedures

1. Identify security needs.
2. Contracts in place for immediate restoration.
3. Identify secondary locations to hold event bookings.

4. Identify insurance needs.
5. Campus setting with class cancellations addressed.
6. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders (Fire, Ambulance, Law Enforcement).

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

H. Communications

1. Communications cross jurisdictional, reporting, and management lines.
2. Command Center should have direct access to emergency communication system.
3. In house loop tapes for immediate communications.
4. Megaphones for crowd control.
5. Hand held radios with minimum 10 channels.
6. Signal enhancement of emergency responder's communications for in-house use.
7. Wireless cell service with phone to phone and group talk communication capability.
8. Identify a chain of command (decision makers).
9. Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.
10. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder. Describe the primary and backup communication systems (phones and radios).
11. Communications should be established and checked with all emergency responders (fire, police, state police, hospitals, ambulance services) prior to the game.
12. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.
13. Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

I. Security Personnel

1. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.
2. Security personnel are provided by licensed and certified providers.
3. Physical plant security personnel mandatory with full time staff, under the direction of a Director of Security.
4. Game Day Event Security Director in-house or vendor hire.
5. All personnel must have background check.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

J. Training, Modeling, and Simulation

1. Initial training in guest relations, problem solving and basic security procedures eight (8) hours.
2. Crowd control and crowd behavior techniques four (4) hours.
3. International Association of Assembly Managers “best practices” awareness.
4. Conduct annual evacuation simulations.
5. Behind the scenes evacuation drills conducted monthly.
6. Provide detailed training on inspection procedures to all security staff.
7. Train security inspection staff in what to look for and proper inspection procedures.
8. Train access control personnel in credential recognition and access.
9. Conduct table top exercises regarding all plans, practices, and procedures. Possibly include Homeland Security personnel and resources.
10. Conduct at least one annual emergency drill prior to or early in the season.
11. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.
12. Emergency Response and Evacuation Plans practiced.
13. All Campus Police and Safety Officers are trained in bomb threat response.
14. All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

K. WMD – Toxic materials protection

1. Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans and procedures.
2. On site decontamination locations identified.
3. Banner planes identified, inspected, monitored, and restricted.
4. Guided by emergency responders protocols. For any WMD, the scene is under the control of the director of operations.
5. All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level.
6. A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.
7. All potentially dangerous chemicals or materials are permanently removed from the stadium and only on site when in use.
8. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Store in a secured area and handle in compliance with state regulations.
9. A Certified Tech Level or Level I Hazmat trained individual should be on site to evaluate potential Hazmat incidents.

PLEASE LIST ANY ADDITIONAL STANDARDS (OR COMMENTS):

-
-
-
-
-
-

APPENDIX E
Standards for Effective Security Management of University Sport Venues
A Doctoral Dissertation Study
By
Stacey A. Hall

Dear Participants:

Please find enclosed the second survey (of three) in the research process. I greatly appreciate your feedback on the first survey and look forward to getting your future responses.

I am now asking each of you to review the list of standards under each category and rate the importance of each standard on a 5-point scale. It is my goal to reach a consensus among key personnel involved in college game day operations regarding security management of university sport venues.

Importance Rating Scale

very low	moderately low	average	moderately high	very high
1	2	3	4	5

This survey should take no longer than 20 minutes. Please complete and return via email Stacey.A.Hall@usm.edu or fax 601-266-4445.

A. Please check which of the following categories you are presently employed:

- Dept. of Intercollegiate Athletics _____
- Campus Police _____
- Sheriff's Office _____
- Emergency Management Agency _____

B. Please review the following standards and rate the importance of each standard on the following scale by circling your choice:

very low moderately low average moderately high very high
 1 2 3 4 5

Perimeter Control

	very low 1	moderately low 2	average 3	moderately high 4	very high 5			
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian Access points twelve (12) hours prior to the event.				1	2	3	4	5
2. Lock down stadium 24 hours prior to an event and allow only controlled access.				1	2	3	4	5
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.				1	2	3	4	5
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.				1	2	3	4	5
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.				1	2	3	4	5
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.				1	2	3	4	5
7. Security assigned to guard vulnerable systems, including air takes.				1	2	3	4	5
8. Check and empty dumpsters and trash receptacles regularly.				1	2	3	4	5
9. Do not place dumpsters under structural supports when and where possible.				1	2	3	4	5
10. Establish a 500-foot secure outer perimeter around the stadium.				1	2	3	4	5
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and				1	2	3	4	5

their vehicle inspected.	1	2	3	4	5
12. All buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	1	2	3	4	5
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	1	2	3	4	5

Access Control

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, Except as required for medical or family needs.	1	2	3	4	5
15. Publicize the policy concerning inspections and identify prohibited items.	1	2	3	4	5
16. No re-entry except for medical emergency.	1	2	3	4	5
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	1	2	3	4	5
18. Utilize tables outside entry gates for bag inspections.	1	2	3	4	5
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	1	2	3	4	5
20. Portable metal detectors at stadium entry gates.	1	2	3	4	5
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	1	2	3	4	5
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	1	2	3	4	5
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	1	2	3	4	5
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	1	2	3	4	5
25. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted					

team areas.	1	2	3	4	5
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	1	2	3	4	5
27. All tickets contain a hologram for ticket validation.	1	2	3	4	5
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	1	2	3	4	5
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	1	2	3	4	5
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	1	2	3	4	5
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	1	2	3	4	5
32. Open all main entry gates at the same time.	1	2	3	4	5
33. Schedule limited daily or weekly delivery times for vendors.	1	2	3	4	5
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	1	2	3	4	5
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	1	2	3	4	5
36. No vendor deliveries should be allowed within 90 minutes of the game.	1	2	3	4	5
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	1	2	3	4	5

Credentiaing

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
38. Background checks required for all vendors, employees, contractors, students and volunteers.	1	2	3	4	5
39. Simplify credential systems indicating zone access and color code by game function.	1	2	3	4	5
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	1	2	3	4	5
41. Credentials are substantially different from those used in prior seasons.	1	2	3	4	5
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	1	2	3	4	5

43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	1	2	3	4	5
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	1	2	3	4	5
45. Require all credentials to be worn at all times and clearly displayed.	1	2	3	4	5
46. Require all team bench staff, except players in uniform, to wear a game credential.	1	2	3	4	5
47. To assist with access control, display credential boards at all access control points.	1	2	3	4	5

Physical Protection Systems

	1	2	3	4	5
	very low	moderately low	average	moderately high	very high
48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	1	2	3	4	5
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	1	2	3	4	5
50. Bomb removal equipment is on site.	1	2	3	4	5
51. Annual structural inspection of entire facility is required and documented.	1	2	3	4	5
52. All utility areas alarmed and contain card access entry points.	1	2	3	4	5
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	1	2	3	4	5
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	1	2	3	4	5
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	1	2	3	4	5
56. 24-hour camera surveillance of perimeter and playing field.	1	2	3	4	5
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	1	2	3	4	5
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	1	2	3	4	5
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	1	2	3	4	5
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	1	2	3	4	5

61. Portable Hazmat Smart Stripes and detection equipment is on site. 1 2 3 4 5

Risk Management (threat/risk assessment)

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	1	2	3	4	5
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	1	2	3	4	5
64. Complete plans in conjunction with local law enforcement anti-terror task force.	1	2	3	4	5
65. Conduct weekly game management meetings (include risk management issues).	1	2	3	4	5

Emergency Management (response and evacuation)

	very low 1	moderately low 2	3	average 4	moderately high 5	very high
66. Develop, maintain, and practice Emergency Response Plan.	1	2	3	4	5	
67. Develop, maintain, and practice Emergency Evacuation Plan.	1	2	3	4	5	
68. Coordinate emergency plan with local, state and federal emergency management authorities.	1	2	3	4	5	
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	1	2	3	4	5	
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	1	2	3	4	5	
71. Establish a security command and control center (primary and secondary location).	1	2	3	4	5	
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	1	2	3	4	5	
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	1	2	3	4	5	
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	1	2	3	4	5	
75. The Command Center has a view of the playing field to facilitate decision making.	1	2	3	4	5	

76. Provide a secure incident room designated for decision makers.	1	2	3	4	5
77. Identification of management teams for response to command and control.	1	2	3	4	5
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	1	2	3	4	5
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	1	2	3	4	5
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.	1	2	3	4	5
81. Develop Emergency Medical Plan.	1	2	3	4	5
82. Designate primary and secondary triage and transport sites.	1	2	3	4	5
83. Identify and secure emergency routes in and out of the stadium facility.	1	2	3	4	5
84. All emergency routes remain clear throughout the event on campus.	1	2	3	4	5
85. Emergency Management response and evacuation personnel on site throughout event.	1	2	3	4	5
86. More than one ambulance and at least two Certified EMT's onsite.	1	2	3	4	5
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	1	2	3	4	5
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	1	2	3	4	5

Recovery Procedures

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
89. Identify security needs.	1	2	3	4	5
90. Contracts in place for immediate restoration.	1	2	3	4	5
91. Identify secondary locations to hold event bookings.	1	2	3	4	5
92. Identify insurance needs.	1	2	3	4	5

93. Campus setting with class cancellations addressed.	1	2	3	4	5
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	1	2	3	4	5

Communications

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
95. Communications cross jurisdictional, reporting, and management lines.	1	2	3	4	5
96. Command Center should have direct access to emergency communication system.	1	2	3	4	5
97. In house loop tapes for immediate communications.	1	2	3	4	5
98. Megaphones for crowd control.	1	2	3	4	5
99. Hand held radios with minimum 10 channels.	1	2	3	4	5
100. Each agency radio channel is also independent in case there is a breach of security.	1	2	3	4	5
101. Signal enhancement (repeater) of emergency responder's communications for in-house use.	1	2	3	4	5
102. Wireless cell service with phone to phone and group talk communication capability.	1	2	3	4	5
103. Identify a chain of command (decision makers).	1	2	3	4	5
104. Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.	1	2	3	4	5
105. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	1	2	3	4	5
106. Communications established and checked with all emergency responders prior to the game.	1	2	3	4	5
107. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	1	2	3	4	5
108. Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	1	2	3	4	5

Security Personnel

	very low 1	moderately low 2	average 3	moderately high 4	very high 5		
109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.			1	2	3	4	5
110. Security personnel are provided by licensed and certified providers.			1	2	3	4	5
111. Physical plant security personnel mandatory with full time staff, under the direction of Security Director.			1	2	3	4	5
112. Game Day Event Security Director in-house or vendor hire.			1	2	3	4	5
113. All personnel must have background check.			1	2	3	4	5

Training, Modeling, and Simulation

	very low 1	moderately low 2	average 3	moderately high 4	very high 5		
114. Initial training in guest relations, problem solving and basic security procedures.			1	2	3	4	5
115. Crowd control and crowd behavior techniques.			1	2	3	4	5
116. International Association of Assembly Managers "best practices" awareness.			1	2	3	4	5
117. Conduct annual evacuation simulations.			1	2	3	4	5
118. Provide detailed training on inspection procedures to all security staff.			1	2	3	4	5
119. Train access control personnel in credential recognition and access.			1	2	3	4	5
120. Conduct table top exercises regarding all plans, practices, and procedures.			1	2	3	4	5
121. Conduct at least one annual emergency drill prior to or early in the season.			1	2	3	4	5
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.			1	2	3	4	5
123. Include Emergency Management personnel in policy development and training.			1	2	3	4	5
124. All Campus Police and Safety Officers are trained in bomb threat response.			1	2	3	4	5
125. All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.			1	2	3	4	5

126. Ticket taker responsibilities separate and distinct from those having security responsibilities. 1 2 3 4 5

WMD – Toxic materials protection

	very low 1	moderately low 2	average 3	moderately high 4	very high 5
127. Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.	1	2	3	4	5
128. On site decontamination locations identified.	1	2	3	4	5
129. Banner planes identified, inspected, monitored, and restricted.	1	2	3	4	5
130. For any WMD, the scene is under the control of the Emergency Management Director.	1	2	3	4	5
131. All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level.	1	2	3	4	5
132. A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.	1	2	3	4	5
133. All potentially dangerous chemicals or materials are permanently removed from the stadium.	1	2	3	4	5
134. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.	1	2	3	4	5

APPENDIX F
Standards for Effective Security Management of University Sport Venues
A Doctoral Dissertation Study

By
Stacey A. Hall

Dear Participants:

Please find enclosed the final survey in the research process. I greatly appreciate your feedback on the previous surveys and look forward to getting your future responses.

The final survey is the same as the previous one you received; however, I have included the group's importance rating response (**GR**) from the previous round. Please review the group's response and again rate the importance of each standard on a 5-point scale.

It is my goal to reach a consensus among key personnel involved in security management of university sport venues.

Importance Rating Scale

very low	moderately low	average	moderately high	very high
1	2	3	4	5

This survey should take no longer than 20 minutes. Please complete and return via email Stacey.A.Hall@usm.edu or fax 601-266-4445.

A. Please check which of the following categories you are presently employed:

- Dept. of Intercollegiate Athletics
- Campus Police
- Sheriff's Office
- Emergency Management Agency

B. Please review the following standards and rate the importance of each standard on the following scale by circling your choice:

very low moderately low average moderately high very high
 1 2 3 4 5

Perimeter Control

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR		
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.			1	2	3	4	5	4.18
2. Lock down stadium 24 hours prior to an event and allow only controlled access.			1	2	3	4	5	4.36
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.			1	2	3	4	5	4.41
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.			1	2	3	4	5	3.38
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.			1	2	3	4	5	3.64
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.			1	2	3	4	5	4.41
7. Security assigned to guard vulnerable systems, including air takes.			1	2	3	4	5	3.77
8. Check and empty dumpsters and trash receptacles regularly.			1	2	3	4	5	3.90
9. Do not place dumpsters under structural supports when and where possible.			1	2	3	4	5	4.23
10. Establish a 500-foot secure outer perimeter around the stadium.			1	2	3	4	5	4.05
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.			1	2	3	4	5	3.52

12. All buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	1	2	3	4	5	3.52
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	1	2	3	4	5	3.81

Access Control

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.	1	2	3	4	5	4.76
15. Publicize the policy concerning inspections and identify prohibited items.	1	2	3	4	5	4.68
16. No re-entry except for medical emergency.	1	2	3	4	5	4.50
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	1	2	3	4	5	4.59
18. Utilize tables outside entry gates for bag inspections.	1	2	3	4	5	4.41
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	1	2	3	4	5	4.10
20. Portable metal detectors at stadium entry gates.	1	2	3	4	5	3.82
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	1	2	3	4	5	4.36
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	1	2	3	4	5	4.05
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	1	2	3	4	5	4.55
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	1	2	3	4	5	4.23
25. Assign team staff to identify players, coaches and staff entering the locker rooms and other restricted						

team areas.	1	2	3	4	5	4.59
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	1	2	3	4	5	4.41
27. All tickets contain a hologram for ticket validation.	1	2	3	4	5	3.76
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	1	2	3	4	5	3.64
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	1	2	3	4	5	4.36
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	1	2	3	4	5	3.86
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	1	2	3	4	5	3.76
32. Open all main entry gates at the same time.	1	2	3	4	5	4.00
33. Schedule limited daily or weekly delivery times for vendors.	1	2	3	4	5	4.00
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	1	2	3	4	5	4.19
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	1	2	3	4	5	4.59
36. No vendor deliveries should be allowed within 90 minutes of the game.	1	2	3	4	5	4.14
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	1	2	3	4	5	4.33

Credentiaing

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
38. Background checks required for all vendors, employees, contractors, students and volunteers.	1	2	3	4	5	3.95
39. Simplify credential systems indicating zone access and color code by game function.	1	2	3	4	5	4.29
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	1	2	3	4	5	4.38

41. Credentials are substantially different from those used in prior seasons.	1	2	3	4	5	4.43
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	1	2	3	4	5	4.24
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	1	2	3	4	5	4.19
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	1	2	3	4	5	4.24
45. Require all credentials to be worn at all times and clearly displayed.	1	2	3	4	5	4.52
46. Require all team bench staff, except players in uniform, to wear a game credential.	1	2	3	4	5	4.38
47. To assist with access control, display credential boards at all access control points.	1	2	3	4	5	4.48

Physical Protection Systems

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	1	2	3	4	5	4.48
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	1	2	3	4	5	4.14
50. Bomb removal equipment is on site.	1	2	3	4	5	3.62
51. Annual structural inspection of entire facility is required and documented.	1	2	3	4	5	4.18
52. All utility areas alarmed and contain card access entry points.	1	2	3	4	5	4.14
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	1	2	3	4	5	3.62
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	1	2	3	4	5	4.05
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	1	2	3	4	5	4.14
56. 24-hour camera surveillance of perimeter and playing field.	1	2	3	4	5	4.09
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	1	2	3	4	5	4.14
58. The system is digital and capable of being monitored at the Command Center and Campus Police						

Department.	1	2	3	4	5	4.43
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	1	2	3	4	5	4.14
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	1	2	3	4	5	4.48
61. Portable Hazmat Smart Stripes and detection equipment is on site.	1	2	3	4	5	3.95

Risk Management (threat/risk assessment)

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	1	2	3	4	5	4.38
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	1	2	3	4	5	4.14
64. Complete plans in conjunction with local law enforcement anti-terror task force.	1	2	3	4	5	4.10
65. Conduct weekly game management meetings (include risk management issues).	1	2	3	4	5	4.35

Emergency Management (response and evacuation)

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
66. Develop, maintain, and practice Emergency Response Plan.	1	2	3	4	5	4.52
67. Develop, maintain, and practice Emergency Evacuation Plan.	1	2	3	4	5	4.48
68. Coordinate emergency plan with local, state and federal emergency management authorities.	1	2	3	4	5	4.38
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	1	2	3	4	5	4.57
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	1	2	3	4	5	4.52
71. Establish a security command and control center (primary and secondary location).	1	2	3	4	5	4.57
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	1	2	3	4	5	4.33
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	1	2	3	4	5	4.24
74. Locate the backup Command Center outside the facility with good communications and sufficient						

staff/equipment to serve as a Command Center (consider mobile police command vehicle).	1	2	3	4	5	4.29
75. The Command Center has a view of the playing field to facilitate decision making.	1	2	3	4	5	4.38
76. Provide a secure incident room designated for decision makers.	1	2	3	4	5	4.33
77. Identification of management teams for response to command and control.	1	2	3	4	5	4.35
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	1	2	3	4	5	4.57
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	1	2	3	4	5	4.52
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.	1	2	3	4	5	4.52
81. Develop Emergency Medical Plan.	1	2	3	4	5	4.68
82. Designate primary and secondary triage and transport sites.	1	2	3	4	5	4.45
83. Identify and secure emergency routes in and out of the stadium facility.	1	2	3	4	5	4.57
84. All emergency routes remain clear throughout the event on campus.	1	2	3	4	5	4.57
85. Emergency Management response and evacuation personnel on site throughout event.	1	2	3	4	5	4.38
86. More than one ambulance and at least two Certified EMT's onsite.	1	2	3	4	5	4.52
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	1	2	3	4	5	4.59
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	1	2	3	4	5	4.55

Recovery Procedures

	very low	moderately low	average	moderately high	very high	GR		
	1	2	3	4	5			
89. Identify security needs.			1	2	3	4	5	4.57
90. Contracts in place for immediate restoration.			1	2	3	4	5	4.24

91. Identify secondary locations to hold event bookings.	1	2	3	4	5	4.00
92. Identify insurance needs.	1	2	3	4	5	3.81
93. Campus setting with class cancellations addressed.	1	2	3	4	5	4.00
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	1	2	3	4	5	4.29

Communications

	GR	very low 1	moderately low 2	average 3	moderately high 4	very high 5	
95. Communications cross jurisdictional, reporting, and management lines.	1	2	3	4	5	4.38	
96. Command Center should have direct access to emergency communication system.	1	2	3	4	5	4.52	
97. In house loop tapes for immediate communications.	1	2	3	4	5	4.10	
98. Megaphones for crowd control.	1	2	3	4	5	4.00	
99. Hand held radios with minimum 10 channels.	1	2	3	4	5	4.52	
100. Each agency radio channel is also independent in case there is a breach of security.	1	2	3	4	5	4.48	
101. Signal enhancement (repeater) of emergency responder's communications for in-house use.	1	2	3	4	5	4.48	
102. Wireless cell service with phone to phone and group talk communication capability.	1	2	3	4	5	4.33	
103. Identify a chain of command (decision makers).	1	2	3	4	5	4.57	
104. Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.	1	2	3	4	5	4.67	
105. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	1	2	3	4	5	4.38	
106. Communications established and checked with all emergency responders prior to the game.	1	2	3	4	5	4.62	
107. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	1	2	3	4	5	4.62	
108. Reliable communications between Command Center and the PA/video staff in order for the Command							

Center to authorize and direct the broadcast to emergency scripts and messages. 1 2 3 4 5 4.67

Security Personnel

	very low 1	moderately low 2	average 3	moderately high 4	very high 5	GR
109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	1	2	3	4	5	4.57
110. Security personnel are provided by licensed and certified providers.	1	2	3	4	5	4.48
111. Physical plant security personnel mandatory with full time staff, under the direction of Security Director.	1	2	3	4	5	4.57
112. Game Day Event Security Director in-house or vendor hire.	1	2	3	4	5	4.29
113. All personnel must have background check.	1	2	3	4	5	4.29

Training, Modeling, and Simulation

	GR	very low 1	moderately low 2	average 3	moderately high 4	very high 5	
114. Initial training in guest relations, problem solving and basic security procedures.	1	2	3	4	5	4.14	
115. Crowd control and crowd behavior techniques.	1	2	3	4	5	4.38	
116. International Association of Assembly Managers "best practices" awareness.	1	2	3	4	5	4.00	
117. Conduct annual evacuation simulations.	1	2	3	4	5	4.23	
118. Provide detailed training on inspection procedures to all security staff.	1	2	3	4	5	4.57	
119. Train access control personnel in credential recognition and access.	1	2	3	4	5	4.48	
120. Conduct table top exercises regarding all plans, practices, and procedures.	1	2	3	4	5	4.38	
121. Conduct at least one annual emergency drill prior to or early in the season.	1	2	3	4	5	4.48	
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	1	2	3	4	5	4.57	
123. Include Emergency Management personnel in policy development and training.	1	2	3	4	5	4.52	
124. All Campus Police and Safety Officers are trained in bomb threat response.	1	2	3	4	5	4.62	

125.	All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.	1	2	3	4	5	4.55
126.	Ticket taker responsibilities separate and distinct from those having security responsibilities.	1	2	3	4	5	4.45

WMD – Toxic materials protection

		very low	moderately low	average	moderately high	very high	GR
		1	2	3	4	5	
127.	Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.	1	2	3	4	5	4.45
128.	On site decontamination locations identified.	1	2	3	4	5	4.18
129.	Banner planes identified, inspected, monitored, and restricted.	1	2	3	4	5	4.25
130.	For any WMD, the scene is under the control of the Emergency Management Director.	1	2	3	4	5	4.10
131.	All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level.	1	2	3	4	5	4.14
132.	A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.	1	2	3	4	5	4.27
133.	All potentially dangerous chemicals or materials are permanently removed from the stadium.	1	2	3	4	5	4.55
134.	Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.	1	2	3	4	5	4.41

APPENDIX G
Comparison of Means between Delphi Round 2 and 3

Perimeter Control	RII	RIII
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.	4.18	4.36
2. Lock down stadium 24 hours prior to an event and allow only controlled access.	4.36	4.36
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.	4.41	4.36
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.	3.38	3.62
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.	3.64	3.64
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.	4.41	4.36
7. Security assigned to guard vulnerable systems, including air takes.	3.77	3.73
8. Check and empty dumpsters and trash receptacles regularly.	3.90	4.00
9. Do not place dumpsters under structural supports when and where possible.	4.23	4.18
10. Establish a 500-foot secure outer perimeter around the stadium.	4.05	4.09
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.	3.52	3.68
12. All buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	3.52	3.75
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	3.81	3.75
Access Control		
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.	4.76	4.50
15. Publicize the policy concerning inspections and identify prohibited items.	4.68	4.73
16. No re-entry except for medical emergency.	4.50	4.14
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	4.59	4.64
18. Utilize tables outside entry gates for bag inspections.	4.41	4.36
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	4.10	4.10
20. Portable metal detectors at stadium entry gates.	3.82	4.14

21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	4.36	4.50
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	4.05	4.23
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	4.55	4.45
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	4.23	4.32
25. Assign team staff to identify players, coaches and staff entering the locker Rooms and other restricted team areas.	4.59	4.50
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	4.41	4.18
27. All tickets contain a hologram for ticket validation.	3.76	3.77
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	3.64	3.64
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	4.36	4.32
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	3.86	3.95
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	3.76	3.77
32. Open all main entry gates at the same time.	4.00	3.95
33. Schedule limited daily or weekly delivery times for vendors.	4.00	3.68
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	4.19	3.91
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	4.59	4.45
36. No vendor deliveries should be allowed within 90 minutes of the game.	4.14	4.18
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	4.33	4.55
Credentialing		
38. Background checks required for all vendors, employees, contractors, students and volunteers.	3.95	3.91
39. Simplify credential systems indicating zone access and color code by game function.	4.29	4.41

40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	4.38	4.36
41. Credentials are substantially different from those used in prior seasons.	4.43	4.45
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	4.24	4.36
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	4.19	4.41
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	4.24	4.14
45. Require all credentials to be worn at all times and clearly displayed.	4.52	4.50
46. Require all team bench staff, except players in uniform, to wear a game credential.	4.38	4.36
47. To assist with access control, display credential boards at all access control points.	4.48	4.45

Physical Protection Systems

48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	4.48	4.41
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	4.14	4.27
50. Bomb removal equipment is on site.	3.62	3.86
51. Annual structural inspection of entire facility is required and documented.	4.18	4.27
52. All utility areas alarmed and contain card access entry points.	4.14	4.09
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	3.62	3.86
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	4.05	4.27
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	4.14	4.36
56. 24-hour camera surveillance of perimeter and playing field.	4.09	4.27
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	4.14	4.41
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	4.43	4.59
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	4.14	4.23
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	4.48	4.59
61. Portable Hazmat Smart Stripes and detection equipment is on site.	3.95	3.91

Risk Management

62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	4.38	4.45
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	4.14	4.36
64. Complete plans in conjunction with local law enforcement anti-terror task force.	4.10	4.48
65. Conduct weekly game management meetings (include risk management issues).	4.35	4.25

Emergency Management

66. Develop, maintain, and practice Emergency Response Plan.	4.52	4.73
67. Develop, maintain, and practice Emergency Evacuation Plan.	4.48	4.68
68. Coordinate emergency plan with local, state and federal emergency management authorities.	4.38	4.68
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	4.57	4.68
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	4.52	4.62
71. Establish a security command and control center (primary and secondary location).	4.57	4.55
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	4.33	4.50
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	4.24	4.55
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	4.29	4.50
75. The Command Center has a view of the playing field to facilitate decision making.	4.38	4.36
76. Provide a secure incident room designated for decision makers.	4.33	4.33
77. Identification of management teams for response to command and control.	4.35	4.41
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	4.57	4.59
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	4.52	4.64
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other	4.52	4.55

potential disasters.

81. Develop Emergency Medical Plan.	4.68	4.55
82. Designate primary and secondary triage and transport sites.	4.45	4.45
83. Identify and secure emergency routes in and out of the stadium facility.	4.57	4.59
84. All emergency routes remain clear throughout the event on campus.	4.57	4.73
85. Emergency Management response and evacuation personnel on site throughout event.	4.38	4.55
86. More than one ambulance and at least two Certified EMT's onsite.	4.52	4.55
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	4.59	4.64
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	4.55	4.68

Recovery Procedures

89. Identify security needs.	4.57	4.67
90. Contracts in place for immediate restoration.	4.24	4.24
91. Identify secondary locations to hold event bookings.	4.00	3.95
92. Identify insurance needs.	3.81	3.90
93. Campus setting with class cancellations addressed.	4.00	4.05
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	4.29	4.43

Communications

95. Communications cross jurisdictional, reporting, and management lines.	4.38	4.57
96. Command Center should have direct access to emergency communication system.	4.52	4.57
97. In house loop tapes for immediate communications.	4.10	4.33
98. Megaphones for crowd control.	4.00	4.14
99. Hand held radios with minimum 10 channels.	4.52	4.67
100. Each agency radio channel is also independent in case there is a breach of security.	4.48	4.62
101. Signal enhancement (repeater) of emergency responder's communications for in-house use.	4.48	4.55
102. Wireless cell service with phone to phone and group talk communication capability.	4.33	4.41
103. Identify a chain of command (decision makers).	4.57	4.76
104. Include contact numbers for personnel identified in chain of command	4.67	4.59

(decision makers) and give sequence of notification. Update at least annually and/or when changes are made.

105. Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	4.38	4.50
106. Communications established and checked with all emergency responders prior the game.	4.62	4.64
107. Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	4.62	4.59
108. Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	4.67	4.68

Security Personnel

109. Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	4.57	4.64
110. Security personnel are provided by licensed and certified providers.	4.48	4.55
111. Physical plant security personnel mandatory with full time staff, under the direction of Security Director.	4.57	4.41
112. Game Day Event Security Director in-house or vendor hire.	4.29	4.50
113. All personnel must have background check.	4.29	4.45

Training, Modeling, and Simulation

114. Initial training in guest relations, problem solving and basic security procedures.	4.14	4.36
115. Crowd control and crowd behavior techniques.	4.38	4.55
116. International Association of Assembly Managers "best practices" awareness.	4.00	3.91
117. Conduct annual evacuation simulations.	4.23	4.14
118. Provide detailed training on inspection procedures to all security staff.	4.57	4.59
119. Train access control personnel in credential recognition and access.	4.48	4.59
120. Conduct table top exercises regarding all plans, practices, and procedures.	4.35	4.41
121. Conduct at least one annual emergency drill prior to or early in the season.	4.48	4.55
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	4.57	4.55
123. Include Emergency Management personnel in policy development and training.	4.52	4.59
124. All Campus Police and Safety Officers are trained in bomb threat response.	4.62	4.55

- | | | | |
|------|---|------|------|
| 125. | All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium. | 4.55 | 4.59 |
| 126. | Ticket taker responsibilities separate and distinct from those having security responsibilities. | 4.45 | 4.41 |

WMD – Toxic Materials Protection

- | | | | |
|------|---|------|------|
| 127. | Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans. | 4.45 | 4.45 |
| 128. | On site decontamination locations identified. | 4.18 | 4.23 |
| 129. | Banner planes identified, inspected, monitored, and restricted. | 4.25 | 4.36 |
| 130. | For any WMD, the scene is under the control of the Emergency Management Director. | 4.10 | 4.27 |
| 131. | All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level. | 4.14 | 4.32 |
| 132. | A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level. | 4.27 | 4.32 |
| 133. | All potentially dangerous chemicals or materials are permanently removed from the stadium. | 4.55 | 4.59 |
| 134. | Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations. | 4.41 | 4.50 |

Scale (1-Low; 5-High)

APPENDIX H
Standards for Effective Security Management of University Sport Venues

Perimeter Control	Mean	SD
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.	4.36	.79
2. Lock down stadium 24 hours prior to an event and allow only controlled access.	4.36	.90
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.	4.36	.73
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.	3.62	.92
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.	3.64	1.10
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.	4.36	.79
7. Security assigned to guard vulnerable systems, including air takes.	3.73	.70
8. Check and empty dumpsters and trash receptacles regularly.	4.00	.82
9. Do not place dumpsters under structural supports when and where possible.	4.18	.85
10. Establish a 500-foot secure outer perimeter around the stadium.	4.09	.81
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.	3.68	1.00
12. All buildings located within 100 feet of the stadium is inspected prior to the event and secured by lock or security guard.	3.75	.85
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents.	3.75	.91
Access Control		
14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs.	4.50	.69
15. Publicize the policy concerning inspections and identify prohibited items.	4.73	.55
16. No re-entry except for medical emergency.	4.14	1.17
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items.	4.64	.58
18. Utilize tables outside entry gates for bag inspections.	4.36	.90
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage.	4.10	.64
20. Portable metal detectors at stadium entry gates.	4.14	.83

21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level.	4.50	.86
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter.	4.23	.75
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security.	4.45	.86
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent.	4.32	.72
25. Assign team staff to identify players, coaches and staff entering the locker Rooms and other restricted team areas.	4.50	.51
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	4.18	.80
27. All tickets contain a hologram for ticket validation.	3.77	.75
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	3.64	.85
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	4.32	.90
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	3.95	.95
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	3.77	.87
32. Open all main entry gates at the same time.	3.95	.90
33. Schedule limited daily or weekly delivery times for vendors.	3.68	.89
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	3.91	.92
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	4.45	.80
36. No vendor deliveries should be allowed within 90 minutes of the game.	4.18	.85
37. Ensure food dispensing and handling procedures are reasonably secure to prevent contamination.	4.55	.51

Credentialing

38. Background checks required for all vendors, employees, contractors, students and volunteers.	3.91	.87
39. Simplify credential systems indicating zone access and color code by game function.	4.41	.85

40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	4.36	.79
41. Credentials are substantially different from those used in prior seasons.	4.45	.67
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	4.36	.79
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	4.41	.80
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	4.14	.89
45. Require all credentials to be worn at all times and clearly displayed.	4.50	.74
46. Require all team bench staff, except players in uniform, to wear a game credential.	4.36	.85
47. To assist with access control, display credential boards at all access control points.	4.45	.74

Physical Protection Systems

48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	4.41	.80
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	4.27	.70
50. Bomb removal equipment is on site.	3.86	.99
51. Annual structural inspection of entire facility is required and documented.	4.27	.70
52. All utility areas alarmed and contain card access entry points.	4.09	.92
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	3.86	.94
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	4.27	.96
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	4.36	.90
56. 24-hour camera surveillance of perimeter and playing field.	4.27	.94
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	4.41	.80
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	4.59	.80
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	4.23	.81
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	4.59	.80
61. Portable Hazmat Smart Stripes and detection equipment is on site.	3.91	.92

Risk Management

62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	4.45	1.01
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	4.36	.90
64. Complete plans in conjunction with local law enforcement anti-terror task force.	4.48	.75
65. Conduct weekly game management meetings (include risk management issues).	4.25	.97

Emergency Management

66. Develop, maintain, and practice Emergency Response Plan.	4.73	.55
67. Develop, maintain, and practice Emergency Evacuation Plan.	4.68	.57
68. Coordinate emergency plan with local, state and federal emergency management authorities.	4.68	.57
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	4.68	.65
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	4.62	.67
71. Establish a security command and control center (primary and secondary location).	4.55	.74
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	4.50	.74
73. Designate a backup Command Center in the event primary Command Center has to be evacuated.	4.55	.74
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	4.50	.80
75. The Command Center has a view of the playing field to facilitate decision making.	4.36	.79
76. Provide a secure incident room designated for decision makers.	4.33	.86
77. Identification of management teams for response to command and control.	4.41	.73
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	4.59	.73
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	4.64	.66
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other	4.55	.67

potential disasters.

81. Develop Emergency Medical Plan.	4.55	.74
82. Designate primary and secondary triage and transport sites.	4.45	.80
83. Identify and secure emergency routes in and out of the stadium facility.	4.59	.73
84. All emergency routes remain clear throughout the event on campus.	4.73	.55
85. Emergency Management response and evacuation personnel on site throughout event.	4.55	.74
86. More than one ambulance and at least two Certified EMT's onsite.	4.55	.74
87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	4.64	.66
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	4.68	.65

Recovery Procedures

89. Identify security needs.	4.67	.73
90. Contracts in place for immediate restoration.	4.24	.83
91. Identify secondary locations to hold event bookings.	3.95	.74
92. Identify insurance needs.	3.90	.70
93. Campus setting with class cancellations addressed.	4.05	.81
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	4.43	.81

Communications

95. Communications cross jurisdictional, reporting, and management lines.	4.57	.75
96. Command Center should have direct access to emergency communication system.	4.57	.75
97. In house loop tapes for immediate communications.	4.33	.86
98. Megaphones for crowd control.	4.14	.91
99. Hand held radios with minimum 10 channels.	4.67	.58
100. Each agency radio channel is also independent in case there is a breach of security.	4.62	.67
101. Signal enhancement (repeater) of emergency responder's communications for in-house use.	4.55	.86
102. Wireless cell service with phone to phone and group talk communication capability.	4.41	.73
103. Identify a chain of command (decision makers).	4.76	.44
104. Include contact numbers for personnel identified in chain of command	4.59	.80

(decision makers) and give sequence of notification. Update at least annually and/or when changes are made.

105.	Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	4.50	.80
106.	Communications established and checked with all emergency responders prior the game.	4.64	.73
107.	Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	4.59	.73
108.	Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	4.68	.73

Security Personnel

109.	Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	4.64	.58
110.	Security personnel are provided by licensed and certified providers.	4.55	.60
111.	Physical plant security personnel mandatory with full time staff, under the direction of Security Director.	4.41	.80
112.	Game Day Event Security Director in-house or vendor hire.	4.50	.60
113.	All personnel must have background check.	4.45	.74

Training, Modeling, and Simulation

114.	Initial training in guest relations, problem solving and basic security procedures.	4.36	.73
115.	Crowd control and crowd behavior techniques.	4.55	.60
116.	International Association of Assembly Managers "best practices" awareness.	3.91	.69
117.	Conduct annual evacuation simulations.	4.14	.64
118.	Provide detailed training on inspection procedures to all security staff.	4.59	.59
119.	Train access control personnel in credential recognition and access.	4.59	.67
120.	Conduct table top exercises regarding all plans, practices, and procedures.	4.41	.73
121.	Conduct at least one annual emergency drill prior to or early in the season.	4.55	.60
122.	During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	4.55	.60
123.	Include Emergency Management personnel in policy development and training.	4.59	.59
124.	All Campus Police and Safety Officers are trained in bomb threat response.	4.55	.67

- | | | | |
|------|---|------|-----|
| 125. | All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium. | 4.59 | .67 |
| 126. | Ticket taker responsibilities separate and distinct from those having security responsibilities. | 4.41 | .73 |

WMD – Toxic Materials Protection

- | | | | |
|------|---|------|-----|
| 127. | Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans. | 4.45 | .67 |
| 128. | On site decontamination locations identified. | 4.23 | .92 |
| 129. | Banner planes identified, inspected, monitored, and restricted. | 4.36 | .73 |
| 130. | For any WMD, the scene is under the control of the Emergency Management Director. | 4.27 | .94 |
| 131. | All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level. | 4.32 | .95 |
| 132. | A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level. | 4.32 | .90 |
| 133. | All potentially dangerous chemicals or materials are permanently removed from the stadium. | 4.59 | .80 |
| 134. | Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations. | 4.50 | .80 |
-

Scale (1-Low; 5-High)

Comparison of Means between Participant Groups after Delphi Round 3
Athletic Facility Manager (AFM); Campus Police Chief (CPC); Local Sheriff (LS); Emergency Management Director (EMD)

Perimeter Control	AFM	CPC	LS	EMD
1. Establish a secure inner perimeter around the stadium with limited and controlled vehicle and pedestrian access points twelve (12) hours prior to the event.	4.43	4.60	4.50	3.75
2. Lock down stadium 24 hours prior to an event and allow only controlled access.	4.14	4.20	4.67	4.50
3. Police patrol one (1) hour before parking lots open and continue to patrol until game has concluded and traffic has disbanded.	4.43	4.00	4.67	4.25
4. Bomb dog teams (6) and bomb removal teams inspect the facilities after lock down and four (4) hours prior to opening.	3.57	3.25	4.33	3.00
5. K-9 search all vehicles, media trailers, other temporary storage units inside stadium.	3.43	3.40	4.67	2.75
6. Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, gas and fuel systems.	4.14	4.00	4.83	4.50
7. Security assigned to guard vulnerable systems, including air takes.	3.29	3.80	4.00	4.00
8. Check and empty dumpsters and trash receptacles regularly.	3.86	4.20	4.50	3.25
9. Do not place dumpsters under structural supports when and where possible.	3.86	4.20	4.83	3.75
10. Establish a 500-foot secure outer perimeter around the stadium.	3.57	4.40	4.67	3.75
11. Individuals participating in tailgating activities immediately adjacent to stadium should be identified and their vehicle inspected.	3.43	3.80	4.33	3.00
12. All buildings located within 100 feet of the stadium is inspected prior to the	3.71	3.80	4.33	3.00

- event and secured by lock or security guard.
13. All buildings on campus used by tailgaters/fans should be secured by a security guard to protect the building and its contents. 3.86 4.00 3.75 3.25

Access Control

14. Prohibit coolers, bags, large backpacks, containers, explosives, weapons, and outside food or beverages, except as required for medical or family needs. 4.57 4.40 5.00 4.00
15. Publicize the policy concerning inspections and identify prohibited items. 4.86 4.40 5.00 4.50
16. No re-entry except for medical emergency. 4.43 4.60 3.33 4.25
17. Security personnel located at each entry point to observe and inspect purses, coats and clothing, and to restrict entry of impermissible items. 4.57 4.60 5.00 4.25
18. Utilize tables outside entry gates for bag inspections. 4.14 4.20 4.83 4.25
19. Ticket entry areas identified with standard pat down and /or hand metal detector usage. 3.86 4.20 4.75 3.75
20. Portable metal detectors at stadium entry gates. 3.57 4.00 5.00 4.00
21. Facility management prepared to implement additional screening measures should Department of Homeland Security elevate the alert level. 4.14 4.20 5.00 4.75
22. All bags for media, concessions, game day personnel, etc are searched and tagged with clearly identified markings before permitted to enter. 4.00 4.40 4.67 3.75
23. Each gate area has at least one law enforcement officer to address any issues that cannot be resolved by security. 4.29 4.20 4.83 4.50
24. Apply the same security inspection criteria to employees, staff and media. Inspections must be consistent. 4.29 4.00 4.83 4.00

25. Assign team staff to identify players, coaches and staff entering the locker Rooms and other restricted team areas.	4.57	4.40	4.67	4.25
26. Each entry point has a ticket taker equipped with access management equipment and scanners.	3.86	4.40	4.50	4.00
27. All tickets contain a hologram for ticket validation.	3.57	4.20	3.83	3.50
28. Electronic scanning of all tickets implemented and capable of capturing season ticket holder information.	3.86	3.60	3.50	3.50
29. Establish access control gates for all vehicles, employees, game staff, police, media and entertainment. Ensure those authorized access are screened and identities verified.	4.57	4.00	4.67	3.75
30. Record each vehicle, driver and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification.	4.00	3.60	4.67	3.25
31. Identify, log-in/out and issue self-expiring day passes to all authorized visitors. Escort visitors in/out of facility.	3.86	3.60	4.00	3.50
32. Open all main entry gates at the same time.	4.14	4.40	4.00	3.00
33. Schedule limited daily or weekly delivery times for vendors.	4.00	3.60	4.33	3.00
34. Accept vendor deliveries by appointment only and authorization by the appropriate stadium supervisor.	4.29	3.60	4.33	3.00
35. Reserve the right to inspect any delivery. Check-in and receive delivery by person expecting it.	4.57	3.80	5.00	4.25
36. No vendor deliveries should be allowed within 90 minutes of the game.	4.43	3.80	4.67	3.50
37. Ensure food dispensing and handling procedures are reasonably secure to	4.71	4.20	4.67	3.50

prevent contamination.

Credentialing

38. Background checks required for all vendors, employees, contractors, students and volunteers.	3.86	3.60	4.17	4.00
39. Simplify credential systems indicating zone access and color code by game function.	4.57	3.80	4.83	4.25
40. Maintain a record of persons issued credentials for control purposes. Sequentially number credentials for control.	4.57	3.80	4.83	4.00
41. Credentials are substantially different from those used in prior seasons.	4.43	4.20	4.83	4.25
42. Use a hologram or other protection on the credential to reduce the potential for counterfeiting.	4.14	4.20	4.83	4.25
43. Issue photo credential to all regular game day employees, staff, media, vendors, and subcontractors.	4.25	4.00	4.83	4.50
44. Require those designated to pick up their credentials to do so in person, using government issued photo ID.	3.86	3.80	4.83	4.50
45. Require all credentials to be worn at all times and clearly displayed.	4.43	4.20	4.83	4.50
46. Require all team bench staff, except players in uniform, to wear a game credential.	4.29	3.80	4.83	4.50
47. To assist with access control, display credential boards at all access control points.	4.43	4.20	4.83	4.25

Physical Protection Systems

48. Establish an inner perimeter (100 ft) with permanent and movable barricades controlled by law enforcement.	4.57	4.20	4.67	4.00
49. Utilize jersey barriers, reinforced concrete decorative planters, bollards and/or large trucks or buses.	4.43	4.20	4.17	4.25
50. Bomb removal equipment is on site.	3.71	3.60	4.67	3.25
51. Annual structural inspection of entire facility is required and documented.	4.00	4.20	4.67	4.25
52. All utility areas alarmed and contain card access entry points.	3.57	3.80	4.83	4.25
53. Intake vents hidden from view and alarmed for weighed objects/ biohazards.	3.43	3.60	4.67	3.75
54. Install internal and external cameras (digital) with pan, tilt, and zoom.	4.00	4.00	4.50	4.75
55. Cameras monitor all areas of the stadium including the perimeter, surrounding exterior areas, concourses, playing field, and concession areas.	4.14	4.00	4.67	4.75
56. 24-hour camera surveillance of perimeter and playing field.	4.00	4.00	4.50	4.75
57. The stadium and press box is equipped with an Integrated Security Management System (ISMS) consisting of CCTV, access controls and alarms where required.	4.29	4.20	4.67	4.50
58. The system is digital and capable of being monitored at the Command Center and Campus Police Department.	4.43	4.40	4.83	4.75
59. Periodic broadcasts conducted on the PA system setting forth security procedures and prohibited items.	4.14	4.60	4.17	4.00
60. The lighting of the gate areas enhanced to allow for searching of bags and persons.	4.43	4.60	5.00	4.25
61. Portable Hazmat Smart Stripes and detection equipment is on site.	3.29	4.20	4.50	3.75

Risk Management

62. Develop risk management plans for Athletic Department events and review on an ongoing basis.	4.29	3.80	5.00	4.75
63. Risk management training is conducted biannually with athletics, university, law enforcement, security, concessions, ticket takers, ushers, and all third party staffs and personnel.	4.00	3.80	5.00	4.75
64. Complete plans in conjunction with local law enforcement anti-terror task force.	4.14	4.20	5.00	4.75
65. Conduct weekly game management meetings (include risk management issues).	4.29	4.20	4.20	4.33

Emergency Management

66. Develop, maintain, and practice Emergency Response Plan.	4.43	4.60	5.00	5.00
67. Develop, maintain, and practice Emergency Evacuation Plan.	4.43	4.60	5.00	4.75
68. Coordinate emergency plan with local, state and federal emergency management authorities.	4.57	4.40	5.00	4.75
69. Document in-house procedures for emergency response to local weather conditions, fire, electrical, and mechanical emergencies.	4.57	4.40	5.00	4.75
70. Develop a detailed plan for pedestrian and traffic flow away from responding emergency vehicles.	4.43	4.00	5.00	4.33
71. Establish a security command and control center (primary and secondary location).	4.43	4.60	4.83	4.25
72. Staff Command Center with the following: police, fire/EMS, stadium management, club representative, private security and FAA (or direct line).	4.43	4.40	5.00	4.00
73. Designate a backup Command Center in the event primary Command Center	4.43	4.40	5.00	4.25

has to be evacuated.				
74. Locate the backup Command Center outside the facility with good communications and sufficient staff/equipment to serve as a Command Center (consider mobile police command vehicle).	4.29	4.40	5.00	4.25
75. The Command Center has a view of the playing field to facilitate decision making.	4.29	4.20	4.50	4.50
76. Provide a secure incident room designated for decision makers.	4.43	4.40	4.40	4.00
77. Identification of management teams for response to command and control.	4.43	4.40	4.67	4.00
78. Copies of the Emergency Evacuation Plan maintained at the Command Center and Campus Police Department.	4.57	4.40	5.00	4.25
79. Include a detailed disaster plan and establish protocols in advance for game delays, cancellations, bomb threats, partial and full evacuation and other emergencies.	4.57	4.40	5.00	4.50
80. Develop audio and video scripts for specific emergency announcements to include, but not limited to natural disasters, weather, bomb threats and other potential disasters.	4.57	4.40	4.83	4.25
81. Develop Emergency Medical Plan.	4.57	4.20	5.00	4.25
82. Designate primary and secondary triage and transport sites.	4.43	4.40	4.83	4.00
83. Identify and secure emergency routes in and out of the stadium facility.	4.71	4.40	5.00	4.00
84. All emergency routes remain clear throughout the event on campus.	4.71	4.40	5.00	4.75
85. Emergency Management response and evacuation personnel on site throughout event.	4.57	4.40	5.00	4.00
86. More than one ambulance and at least two Certified EMT's onsite.	4.57	4.40	5.00	4.00

87. The stadium PA system, communications system, data systems and emergency lights is on an emergency generator system that automatically switches on in the event of a power failure.	4.57	4.40	5.00	4.50
88. All specialty events, fireworks, parachutes and any other unusual activity occurring during an event is identified to the community emergency responders.	4.57	4.40	5.00	4.75

Recovery Procedures

89. Identify security needs.	4.71	4.00	5.00	5.00
90. Contracts in place for immediate restoration.	4.29	4.00	4.40	4.25
91. Identify secondary locations to hold event bookings.	4.14	3.80	4.20	3.50
92. Identify insurance needs.	3.86	4.00	4.20	3.50
93. Campus setting with class cancellations addressed.	4.14	3.80	4.40	3.75
94. Written contracts or mutual aid agreements in effect with local and out of state Emergency Responders.	4.43	4.00	4.80	4.50

Communications

95. Communications cross jurisdictional, reporting, and management lines.	4.29	4.40	5.00	4.75
96. Command Center should have direct access to emergency communication system.	4.29	4.40	5.00	4.75
97. In house loop tapes for immediate communications.	4.00	4.40	5.00	4.00
98. Megaphones for crowd control.	3.86	4.20	4.60	4.00
99. Hand held radios with minimum 10 channels.	4.71	4.60	5.00	4.25
100. Each agency radio channel is also independent in case there is a breach of security.	4.57	4.40	5.00	4.25

101.	Signal enhancement (repeater) of emergency responder's communications for in-house use.	4.57	4.20	5.00	4.25
102.	Wireless cell service with phone to phone and group talk communication capability.	4.29	4.40	4.83	4.00
103.	Identify a chain of command (decision makers).	4.71	4.60	5.00	4.67
104.	Include contact numbers for personnel identified in chain of command (decision makers) and give sequence of notification. Update at least annually and/or when changes are made.	4.57	4.20	5.00	4.50
105.	Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder.	4.57	4.00	4.83	4.50
106.	Communications established and checked with all emergency responders prior the game.	4.71	4.20	5.00	4.50
107.	Ensure reliable communications with backup systems are in place and tested. Include outside lines, stadium extension phones, police, fire/EMT radios, ring downs and contact with home team public relations and owner's box.	4.57	4.00	5.00	4.75
108.	Reliable communications between Command Center and the PA/video staff in order for the Command Center to authorize and direct the broadcast to emergency scripts and messages.	4.71	4.20	5.00	4.75

Security Personnel

109.	Security personnel included in all training and planning activities to make clear duties, responsibilities, assignments, and limitations.	4.57	4.40	5.00	4.50
110.	Security personnel are provided by licensed and certified providers.	4.43	4.00	4.83	4.25

111. Physical plant security personnel mandatory with full time staff, under the direction of Security Director.	4.43	4.20	5.00	3.75
112. Game Day Event Security Director in-house or vendor hire.	4.57	4.20	5.00	4.00
113. All personnel must have background check.	4.57	3.80	4.83	4.50

Training, Modeling, and Simulation

114. Initial training in guest relations, problem solving and basic security procedures.	4.57	4.20	4.67	3.75
115. Crowd control and crowd behavior techniques.	4.71	4.00	4.83	4.50
116. International Association of Assembly Managers “best practices” awareness.	4.00	3.80	4.00	3.75
117. Conduct annual evacuation simulations.	4.14	4.20	4.50	3.50
118. Provide detailed training on inspection procedures to all security staff.	4.43	4.40	5.00	4.50
119. Train access control personnel in credential recognition and access.	4.57	4.40	4.83	4.50
120. Conduct table top exercises regarding all plans, practices, and procedures.	4.43	4.20	4.50	4.50
121. Conduct at least one annual emergency drill prior to or early in the season.	4.57	4.40	4.67	4.50
122. During training scenarios, test the chain of command, decision making process, primary/secondary communications and emergency use of the PA and video systems.	4.71	4.20	4.67	4.50
123. Include Emergency Management personnel in policy development and training.	4.71	4.20	4.67	4.75
124. All Campus Police and Safety Officers are trained in bomb threat response.	4.71	4.20	4.50	4.75
125. All volunteers, vendors and ushers are trained in security awareness and evacuation procedures for the stadium.	4.43	4.40	5.00	4.50

126. Ticket taker responsibilities separate and distinct from those having security responsibilities.	4.57	4.20	4.67	4.00
---	------	------	------	------

WMD – Toxic Materials Protection

127. Toxic materials protection and decontamination are part of the Emergency Response and Evacuation Plans.	4.14	4.40	5.00	4.25
128. On site decontamination locations identified.	3.71	4.40	5.00	3.75
129. Banner planes identified, inspected, monitored, and restricted.	4.29	4.20	4.83	4.00
130. For any WMD, the scene is under the control of the Emergency Management Director.	4.43	4.00	5.00	3.25
131. All Campus Police and Safety Officers trained to the WMD/CBRNE/Hazmat awareness level.	4.29	4.20	4.33	4.32
132. A campus Hazmat Response Team is established and trained to the Hazmat Level 2 defensive level.	4.43	4.20	4.50	4.00
133. All potentially dangerous chemicals or materials are permanently removed from the stadium.	4.71	4.20	4.83	4.50
134. Be aware of chemicals, fertilizers and propane cylinders stored in the facility area that could be used as a component in an explosion device. Handle in compliance with state regulations.	4.43	4.20	5.00	4.50

Scale (1-Low; 5-High)

REFERENCES

- Andrews, E.L. (2005, July 10). Who bears the risk of terror? *The New York Times*. Retrieved July 12, 2005, from <http://web.lexis-nexis.com/universe/printdoc>
- Ammon, R., Southall, R. & Blair, D. (2004). *Sport facility management: Organizing events and mitigating risks*. Morgantown, WV: Fitness Information Technology, Inc.
- 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 and Washington, D.C: Rand Coporation.
- Associated Press (2005a, July 6). Wider formula puts '04 terrorist attacks at 3,200. *Arizona Daily Star*. Retrieved July 28, 2005, www.dailystar.com
- Associated Press. (2005b, September 29). LSU athletic director apologizes for fans behavior. *FOXSports.com*. Retrieved September 29, 2005, from <http://msn.foxsports.com/cfb/story/4917186>
- Associated Press. (2001, September 17). League tightens security measures. *NFL News.com*. Retrieved September 13, 2005, from http://www.nfl.com/news/2001/security_091701.html
- Bagnato, A. (2001, September 17). Stadium security bolstered nationally; FAA bans aircraft from flying over Michigan's game. *Chicago Tribune*. Retrieved September 29, 2005, from www.ebscohost.com
- Bierbauer, C. (1996, July 27). Munich remembered: 1972 attack led to increased security. *CNN interactive*. Retrieved September 19, 2005, from

<http://www.cnn.com/US/9607/27/munich.remembered/>

Burgess, M. (2003, July 2). A brief history of terrorism. *Center for Disease Information*.

Retrieved September 26, 2005, from

<http://www.cdi.org/friendlyversion/printversion.cfm?documentID=1502>

Chabrow, E. (2005). Stadium security gets a boost. *Information Week*, 1022, 71.

Retrieved September 29, 2005, from www.ebscohost.com

CNN.com. (1996, July 27). *Sources: arrest in Olympic bombing could occur within days*.

Retrieved September 15, 2005, from

<http://www.cnn.com/US/9607/27/blast.am/index.html>

CNN.com. (2002, September 5). *When sport lost its innocence*. Retrieved September 26,

2005, from <http://archives.cnn.com/2002/WORLD/europe/09/05/munich.72/>

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/London: Praeger

Perspectives.

Dalkey, N.C. (n.d.). The Delphi methodology. Retrieved October 3, 2005, from

<http://www.fernuni-hagen.de/ZIFF/v2-ch45a.htm>

Decker, R.J. (2001). *Key elements of a risk management approach*. United States

General Accounting Office. [On-line]. Available:

<http://www.gao.gov/new.items/d02150t.pdf>

Dennington, V. (2004, March 19). How to conduct a study using the Delphi technique.

SSABSA Support Materials. Retrieved July 22, 2005, from

<http://www.ssabsa.sa.edu.au/support/science/pscy/psyc-tl-delphi.pdf>

- Delphi Method. (n.d.). Retrieved October 3, 2005, from
http://absoluteastronomy.com/encyclopedia/d/de/delphi_method.htm
- Department of Defense Directive: Number 5160.54. (November 24, 2003). [On
 Line]. Available: <http://www.dtic.mil/whs/directives/corres/pdf2/d516054p.pdf>
- DHS.gov. (2004, July 23). *Department of Homeland Security hosts security forum for sports executives*. Office of the Press Secretary. Retrieved September 15, 2005, from <http://dhs.gov/dhspublic/display?content=3863>
- DHS.gov. (2005). *DHS Organization*. Retrieved September 13, 2005, from <http://www.dhs.gov/dhspublic/disply?theme=9&content=4624>
- Doyle, B. (2005, June 7). Security at Mississippi stadiums evaluated. *Daily Mississippian*. Retrieved July 20, 2005, from http://www.thedmonline.com/vnews/display.v/ART/2005/06/06/42a5804b31a65?in_archive=1
- Dunham, R.B. (1998, September 1). The Delphi technique. Retrieved July 22, 2005, from <http://instruction.bus.wisc.edu/obdemo/readings/delphi.htm>
- Durling, R.L., Price, D.E., & Spero, K.K. (2005). Vulnerability and risk assessment using the Homeland-Defense operational planning system (HOPS). Retrieved October 4, 2005, from <http://www.llnl.gov/tid/lof/documents/pdf/315115.pdf>
- ESPN.com. (2004, November 21). *Artest, Jackson charge palace stands*. Retrieved September 19, 2005, from <http://sports.espn.go.com/nba/news/story?id=1927380>
- Estell, L. (2002). A banner year for stadiums? Security concerns could put an end to stadium fly-overs. *Incentive*, 176 (12), 8. Retrieved September 29, 2005, from

www.ebscohost.com

Farmer, P.J., Mulrooney, A.L., & Ammon, R. (1996). *Sport facility planning and management*. Morgantown, WV: Fitness Information Technology, Inc.

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

General Security Risk Assessment Guideline. (2003). ASIS International. [On-line].

Available: <http://www.asisonline.org/guidelines/guidelinesgsra.pdf>

Gips, M. (2003). Survey assesses sports facility security. *Security Management Online*.

Retrieved July 21, 2005, from www.securitymanagement.com

Gordon, T.J. (1994). The Delphi method. Retrieved October 3, 2005, from

http://www.futurovenezuela.org/_curso/5-delphi.pdf

Goss, B.D., Jubenville, C.B., & MacBeth, J.L. (n.d.). *Primary principles of post-9/11 stadium security in the United States: Transatlantic implications from British practices*. [On-Line]. Available:

www.iaam.org/CVMS/Post%20911%20Stadium%20Security.doc

Grossman, L., Owens-Liston, P., & Shannon, E. (2002). Playing it safe. *Time*. 159 (2), 60-61. Retrieved May 30, 2005, from www.ebscohost.com

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 September 22, 2005, 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. Janes 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/London: Praeger Perspectives.
- Larsen, R., McIntyre, D., & DeMier, M. (n.d.) *A primer on homeland security, definitions of strategic functions*. Institute for Homeland Security. [On-Line]. Available: <http://www.homelanddefense.org/bulletindefinitions.htm>
- Linstone, H.A., & Turoff, M. (Eds.). (1975). *The Delphi method: Techniques and application*. London: Addison-Wesley.
- 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.
- Ludwig, B. (1997). Predicting the future: Have you considered using the Delphi Methodology? *Journal of Extension*, 35 (5). Retrieved July 22, 2005, from <http://www.joe.org/joe/1997october/tt2.html>
- Mason, A. (2001, September 20). Security: NFL's "No. 1 priority." *NFL.com*. Retrieved September 13, 2005, from http://www.nfl.com/news/2001/security_092001.html
- McHale, J. (February, 2005). DHS launches online tool that assesses stadium vulnerabilities. *Military and Aerospace Technology*, 16 (2), 12-13.
- National Response Plan. (December, 2004). Office of Homeland Security. [On-Line]. Available: http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf
- National Strategy for Combating Terrorism. (February, 2003). [On-Line]. Available:

http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/counter_terrorism_stratgy.pdf

National Strategy for Homeland Security. (July, 2002). Office of Homeland Security.

[On-line]. Available:

http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

Official 2005 NCAA Football Records Book. [On-line]. Available:

http://www.ncaa.org/library/records/football_records_book/2005/2005_d1_football_records.pdf

OJP.USDOJ.gov. (2005). *About ODP*. Retrieved September 22, 2005, from

<http://www.ojp.usdoj.gov/odp/about/overview.htm>

Pantera, M.J. (2003). Architectural design and game day considerations for new or retrofitted sport facilities. *The Sport Supplement*, 11 (4). Retrieved September 26, 2005, from www.thesportjournal.org

Pantera, M.J., et. al. (2003). Best practices for game day security at athletic & sport venues. *The Sport Journal*, 6 (4). [On-Line]. Available:

<http://www.thesportjournal.org/2003Journal/Vol6-No4/security.asp>

Patterns of Global Terrorism. (April 29, 2004). United States Department of State. [On-

Line]. Available: <http://www.state.gov/documents/organization/31912.pdf>

Pollard, C., & Pollard, R. (Winter 2004-2005). Research priorities in educational technology: A Delphi study. *Journal of Research on Technology in Education*, 37 (2), 147-160.

Progress Report on the Global War on Terrorism. (September, 2003). The White House.

[On-Line]. Available:

http://www.whitehouse.gov/homeland/progress/progress_report_0903.pdf

Risk 101. (n.d.). US Coast Guard. Retrieved October 4, 2005, from

<http://www.uscg.mil/hq/gm/risk/background.htm>

Securing Our Homeland. (2004). U.S. Department of Homeland Security Strategic Plan.

[On-Line]. Available:

http://www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf

Securing the Homeland Strengthening the Nation. (n.d.). President George W. Bush. [On-

Line]. Available: http://www.whitehouse.gov/homeland_security_book.pdf

Snel, A. (2005, September 15). Sports authority, Bucs dispute cost of NFL rule; Most

teams pay for security. *Tampa Tribune*. Retrieved September 29, 2005, from

www.ebscohost.com

Spangler, J. (2001, September 30). Meeting the threat. *Deseretnews.com*. Retrieved

September 16, 2005, from

<http://deseretnews.com/dn/sview/1,3329,320006966,00.html>

Syken, B. (2002, September 30). Safe at home? *Sports Illustrated*, 97 (13), 28. Retrieved

September 29, 2005, from www.ebscohost.com

The American Heritage Dictionary. (2002). 4th Ed. Boston and New York: Houghton

Mifflin Company.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential

Decision Directive 63. May 22, 1998. [On-line]. Available:

<http://www.fas.org/irp/offdocs/paper598.htm>

The Global War on Terrorism - The First 100 Days. (n.d.). The Coalition Information

Centers. [On-Line]. Available:

<http://www.whitehouse.gov/news/releases/2001/12/100dayreport.pdf>

Thurber, M. (May 26-28, 1993). *The Essence of Deming 3 Day Workshop*, Meta-Quality Institute, San Francisco.

Universal Task List: Version 2.1. (2005). U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness. [On-Line].

Available: http://www.ojp.usdoj.gov/odp/docs/UTL2_1.pdf

Vulnerability Assessment Report. (July, 2003). Office of Domestic Preparedness, U.S. Department of Homeland Security. Retrieved May 31, 2005, from

<http://www.ojp.usdoj.gov/odp/docs/vamreport.pdf>

WMD Threat and Risk Assessment (Local Jurisdiction). Third Edition. January 2005. Texas Engineering Extension Service (TEEX), College Station, TX.