Command, Control and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security University Center of Excellence

BEST PRACTICES in Anti-Terrorism Security for Sporting and Entertainment Venues RESOURCE GUIDE

July 2013

Table of Contents

Introduction to the Project

Millions of Americans attend sporting events at our nation's stadiums, arenas, and other venues each year. These stadiums and arenas are a key component of what is estimated to be at least a $40 billion dollar yearly economic activity. Many of them also have significant iconic value. Because of their visibility, the large crowds in attendance, the potential for fatalities or injuries, infrastructure disruption, economic losses, and psychological impact, they present an potential target for terrorists. This "Best Practices in Anti-Terrorism Security in Sports Venues Guide" discusses the important components of a stadium anti-terrorism security plan.

More specifically, this Best Practices in Anti-Terrorism Security (BPATS) guide is aimed in assisting owners and operators of sports venues who are developing, deploying and improving the anti-terrorism readiness of their venues and who are interested in submitting an application for coverage of their venue security under the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act.[1] It is also intended to be a resource for the Department of Homeland Security (DHS) Office of Safety Act Implementation (OSAI) as it manages the SAFETY Act Program. The SAFETY Act is not a regulatory program. Applications for coverage under the SAFETY Act are evaluated utilizing procedures and criteria set forth in the SAFETY Act Final Rule, which can be found at 6 C.F.R. Part 25 and as a downloadable resource from www.safetyact.gov. DHS leadership has significant discretion in making determinations and final decisions on applications submitted.

The Guide is the result of a project carried out by the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA), a Department of Homeland Security (DHS) University Center of Excellence (COE) based at Rutgers, the State University of New Jersey.

The SAFETY Act is aimed at encouraging the development and deployment of effective anti-terrorism technologies by providing certain liability protections. While to date more than 600 technologies have been approved under the SAFETY Act, only few sporting venues have applied for and received SAFETY Act protections for their security programs. Identifying the

[1] Additional information on the SAFETY Act, its benefits, and the application process can be found on the Program's website www.safetyact.gov.

key components of anti-terrorism protection at sports stadiums is a basic step in aiding stadium operators to achieve a level of protection appropriate for SAFETY Act recognition and, at the same time, will provide tools and guidelines for OSAI in its evaluation of efforts by stadium operators and leagues.

Background

As noted, CCICADA is a DHS University Center of Excellence based at Rutgers University. CCICADA has been involved with stadium security almost since its inception in 2009. CCICADA has been joined in this project by the Center for Risk and Economic Assessment of Terrorism Events (CREATE), another COE based at the University of Southern California, and the Center for Transportation Safety, Security and Risk (CTSSR) at Rutgers University, which is part of the National Transportation Security Center of Excellence (NTSCOE).

Identifying Best Practices in Anti-Terrorism Security in Sports Venues

The project originally emphasized professional sports and their venues. Thus, we studied leagues and their venues from Major League Baseball (MLB), National Basketball Association (NBA), National Hockey League (NHL), Major League Soccer (MLS), US Tennis Association (USTA), and National Association for Stock Car Auto Racing (NASCAR). As the project progressed, we broadened the scope from its original emphasis on large, professional venues to a variety of others, including Minor League Baseball, MLB spring training facilities, minor league hockey, National Collegiate Athletic Association (NCAA) venues, and NCAA conferences, and professional golf. After the April 2013 Boston Marathon attack, we also turned our attention to lessons learned from that incident and to adjustments made or considered both for open space events like running or bicycle races and for the other venues we had been studying. We also sought specific lessons learned from large venues that had experience dealing with broad, open spaces similar to the environment of the marathon, such as NASCAR and professional golf.

Identification of best practices involved several components: (1) literature review; (2) interviews with stadium security directors, league security directors, and other sport security experts; (3) visits to a broad range of representative venues; (4) workshop with leading experts in stadium security.

We began to identify the important components of a large structure sports venue Anti-Terrorism

Plan (ATP) by examining the literature, some made available by OSAI and other DHS Science and Technology Directorate (S&T) support personnel involved in the project, and the rest based on our research. The documents we reviewed included incident After Action Reports, academic research reports, published articles, special event operational procedures, best practices and research from other industries, technology reviews and user guidance, and league and association guidance documents. All in all, we reviewed more than 65 documents and pulled more than 1,500 passages and quotes, from those documents.

We identified leading experts in sport stadium security and interviewed them, as well as interviewing representatives of standards developing organizations and accreditation and certification bodies. We chose individuals to interview based on recommendations, our own contacts, and information we gathered from discussions with other stadium security experts. We sought to interview representatives from a good sampling of types of venues, types of sports, types of leagues, and areas of expertise. To keep the interviews to a reasonable length, we focused each one on a small subset of the topics we had identified as key topics through our literature review. In all, we interviewed 28 subject matter experts, including eight security directors for venues in the US and Canada 12 private security providers, one of whom is based in the UK and has international experience; seven major sports leagues executives, including representatives from Major League Baseball, Major League Soccer, National Football League, US Tennis Association, and NASCAR; and one Executive Director of a UK National Stadium Security Organization. As we expanded the scope of the project, we added less formal interviews of officials involved in Minor League Baseball, Major League Baseball spring training, NCAA venues, and NCAA conferences.

Interviews were conducted under a guarantee of confidentiality. Materials produced from the interview reports therefore aim to protect the privacy of the participant. Information gathered from interviews aided in the development of group discussion questions for the workshop. These interviews were important because they led us to concepts not adequately covered in the literature, if at all, and brought the concerns of venue operators and security managers to our attention.

In addition to interviewing leading security experts associated with venues, we paid visits to a

variety of venues to gain insights not possible to gain from a phone interview or literature review. These venues visits, however, were informed by our literature review and phone interviews, which enabled us to prepare specific objectives for our visits. In all, we visited 12 venues. In each case, our visit included an extensive interview with venue security and a behind the scenes tour that typically included the Command Center, screening of employees and patrons, the inner perimeter, loading dock, patron seating, and VIP areas. We were given widespread access to venues, both before and during an event. Our visits included venues representing five different sports and included seven multi-use venues, located in five states. Our visits included venues for MLB, NBA, NHL, MLB spring training, minor league hockey, NCAA football, NCAA basketball, and NASCAR. Our observations at the venues were shared with venue security operators and, in some cases, with officials at DHS and New Jersey Office of Homeland Security and Preparedness.

We sought to create a dialogue among experts in stadium security by hosting a one-and-one-half day workshop at Rutgers University in February 2013. This invitation-only workshop attracted key sports stadium security experts from around the country, as well as representatives of the private sector and government agencies involved in stadium security. The goal was to engage them in a dialogue to discuss best practices and lessons learned. While we endeavored to keep the workshop small in order to facilitate dialogue, the strong interest in the topic led us to include 76 participants.

To frame the workshop goals, two expert panel discussions were featured, one on Venue Security and Counterterrorism Challenges and one on Components of an Effective Security and Counterterrorism Plan. In the first panel, we asked the participants to describe the three things that keep them up at night. There was surprising unanimity here and it served as an excellent backdrop for the rest of the workshop. We also broke the participants into ten breakout groups, five on one day and five on the next, reflecting topics our literature review had led us to emphasize: Planning and Evaluating; Venue Profile; Risk Assessment; Leadership, Organization and Authority; Physical Security Measures; Counter-Terrorism Protective Measures; Integrated Communications Systems; Exercise, Education and Training; Quality Assurance Programs; and Incident Management.

Identifying the Key Best Practices and Developing Metrics for Each

We concentrate here on addressing the technical criteria for SAFETY Act coverage: Has there been demonstrated utility and effectiveness of the component? Is the plan (and its components) readily available for deployment? Is there evidence to establish the plan's (or its components') capability to reduce risks of harm? Is the plan effective in facilitating defense against acts of terrorism? We also address questions such as: Does the plan allow for flexibility in the event of the receipt of actionable intelligence suggesting actions or responses at the stadium need to be prioritized and considered? Does the plan facilitate the Incident Command System (ICS) protocols in the event of an incident? Does the plan perform as intended? Does it conform to the stadium operator's specifications? Is the plan safe for use as intended?

There are many different components of an effective anti-terrorism plan. These include inspection procedures, access control, credentialing, perimeter control, mail room and loading dock access, training and exercises, communication, monitoring and surveillance, effect of nearby facilities, transportation access, evacuation planning, and any number of other factors. Based on the literature review, interviews, venue visits, and the workshop, we have studied the various components of an anti-terrorism plan that make it suitable for SAFETY Act coverage We provide three levels of recommendations about important components of an anti-terrorism plan such as ***strongly recommended, recommended***, and ***suggested***. We also note that some components are strongly recommended if a venue has certain characteristics, for example security collaborations with a public transportation system if one exists. While no one size fits all, most of the "strongly recommended" items can be addressed by most venues. It should not be assumed, however, that an application for SAFETY Act protections will be satisfactory just because it addresses all of the "strongly recommended" components. Rather, each applicant needs to seriously consider which of the recommendations or suggestions to address, based on the specific needs or technical characteristics of their venue.

For each important component, we attempt to give guidelines for determination of successful inclusion of the component in an anti-terrorism plan. We term such criteria ***metrics***. We believe that metrics are important enough that we highlight them in tables throughout this guide and discuss them in the text. In many cases, the "best" metrics are those that involve quantification:

How many times did you exercise so and so in the past year? How long does it take to empty your stadium? What is the length of the longest line at your security check? Other times, the best metrics are simply yes-no, but with the need to expand on a "yes" answer. For example: Are your risk assessments revised depending upon the type of event? Upon the time of year? If yes, then how? Are any technical tools or professional resources used to do the risk assessments? If so, which ones? We attempted to use metrics that are based on performance rather than prescription wherever possible. For example, we think it is more useful to know how many fans have a basic knowledge of evacuation procedures (performance metric) than to know how often evacuation procedure instructions are relayed to the fans (prescriptive metric). That said, it was not possible for us to only use performance metrics. In this guide we attempt to highlight useful metrics without providing accompanying recommended levels of performance. For example, as mentioned above, how long it takes to empty the stadium is a useful metric discussed, but we do not discuss how quickly we believe a stadium of a certain size should be able to clear out. The development of more precise, quantitative metrics could be the subject of future research.

In connection with our "important components," we have researched testing methods appropriate for an operational environment. For instance, we looked for metrics that could be used to measure things like probability of detection, false positive and false negative rates, limits of detection, interfering factors, and timing. Of course, some of these are not easy to determine, let alone measure. Our metrics and recommendations address questions like: Has the component been deployed and successful deployment documented? Is domain expertise appropriate and available for that component? Have internal or external audits been conducted and with what results? Are those audits conducted in a "double-loop" learning environment, facilitating a cyclical review and appropriate adjustment to the anti-terrorism plan based on the dynamic nature of the threat? Is there favorable patron feedback? Is the component independently testable and are the tests repeatable? Does the component consistently demonstrate low failure rates and false alarms? Does the component have high reliability? Does the component perform in accordance with specifications? Are the installation and maintenance procedures for the component proven? Are the documented processes such as training, hiring, and refreshing being followed? Are identified standards achieved?

Developing a Best Practices Resource Guide

The results of our literature review, interviews, venue visits, and workshop have been compiled into this Best Practices Resource Guide. The Guide is organized into chapters, dealing with key aspects of stadium security: Risk Assessment; Staffing Leadership, Organization and Authority; Information Management; Operations; Training and Evaluation. We considered many ways of organizing these topics, but found that all of them led to chapters with considerable overlap. Clearly many key components of stadium security can be looked at from different perspectives and points of view, and that is the case here.

Throughout the first six chapters of this document we have tried to maintain consistent usage of several key words. The term "incident" is used to refer to terrorist actions or threats (e.g. a bomb threat, an active shooter, etc.). The term "event" refers to scheduled sporting or entertainment activities. The term "venue" refers to the location where events are held including the surrounding parking areas, vendor areas, and a "facility" which is often a "stadium" or an "arena."

We asked a selection of subject matter experts to review this Guide before finalizing it. All of the reviewers were asked to send us written comments and suggestions.

Testing the Guide

We tested components of the Best Practices Guide by working with various venues and in particular with MetLife Stadium in New Jersey. We observed security practices both on games days and non-game days, collected data, analyzed it, examined changes, etc. We were given access to the inner workings of stadiums, provided key information, and escorted by key stadium security leaders.

Executive Summary

This Best Practices Resource Guide reports the results of a detailed study of best practices for sports venues' anti-terrorism security plans. Information resulting from the research arose from a literature review, more than two dozen interviews with leading sports venue security experts, reports on a dozen sports venue visits, and reports from a workshop of over 70 subject matter experts who participated in two panels and ten focused topic breakout sessions. We try here to

capture in a very short list the key components to venue security based on our analysis of this large amount of information. In the Best Practices Resource Guide, we expand on each of these elements.

1. Conduct a baseline risk assessment of the venue by means of an accepted risk methodology for prioritizing terrorist threats, and analyze those threats in terms of relative likelihood and consequence. Update the assessment regularly in accordance with world events and intelligence, after all major structural changes to the venue, and in response to any major changes in the nature of the events being hosted at the venue. In addition to venue security staff, include on the assessment team external stakeholders who are responsible for incident response and recovery.
2. Design a scalable security program that incorporates people, technology, and procedures to detect, deter, defend, mitigate, and respond to threats, focusing on those high in likelihood of attack and with the greatest consequence. The scale of the program should be consistent with the size of the venue, the expected attendance at each event, and the amount of risk exposure.
3. Hire, vet and train a security workforce with the knowledge, skills, and abilities to implement the security program and adapt to changes as needed in an ever changing threat environment. The workforce should have a clear division of work, reasonable span of control, and recognized chain of command. It should be able to transition smoothly from normal operations to an incident command structure for major incidents and interface seamlessly with management and other venue operations.
4. Manage communications (among venue staff, between staff and external responding agencies, and between staff and patrons) in a way that ensures the robust operability of communication systems, and mitigates risk effectively during normal operations and emergencies.
5. Train staff constantly and repeatedly measure the effectiveness of the security program by collecting and evaluating data on the performance of all aspects of the program, including that of security personnel, supervisors, and command elements. Some of the training should include "tabletop" and full scale exercises with external agencies responsible for incident response and recovery, and the security program should include testing of the training and use of After Action Reports. These reports can be used to evaluate and improve performance not only after training but after routine minor incidents to establish the habit of review.

Chapter 1 – Overview

1.1 Introduction

This chapter provides an overview of the best practices in anti-terrorism for stadium security in the context of the SAFETY Act. These best practices are described in detail in the five following chapters. The chapters focus on distinct aspects of the best practices: Risk Assessment, Staffing Issues (including leadership, organization and authority), Information Management, Operations, and Training and Evaluation. While these aspects of best practices are organized into separate chapters, and their implementation may be assigned to different staff members, they are not really separable. Rather, they are interlocking parts of a dynamic and adaptive stadium security plan.

The parts of the plan must be adaptable to new information and new situations. For example, new intelligence or a unique event to be hosted at the stadium may trigger a risk review, which in turn may lead to coordinated changes in staffing, information management, operations, and training to mitigate the risk. The adaptive nature of the best practices means that there must be good communication and coordination among those responsible for different aspects of the security plan, and there must be regular risk assessments for the ever-changing environment.

1.2 Risk Assessment

Best practices for stadium security begin with a thorough risk assessment for each type of event and situation. Information developed in the course of conducting a risk assessment will influence each of the other parts of the security plan. While general risk assessment has been studied for a number of different industries and has an extensive literature, assessment of risk posed by stadiums has some unique characteristics. Stadiums may host extremely high profile events (raising the value of an attack in the minds of terrorists); they may include access paths that are very difficult to control; crowds may congregate or queues may build up at gate entrances; and they are subject to conflicting goals of stakeholders ranging from ticket holders seeking entertainment to law enforcement with a deep concern for security.

Overall risk is a product of three factors: threats, vulnerability, and consequences. Threats comprise all possible forms and weapons of attack. These include the National Planning

Scenarios as updated by recent specific incidents and intelligence (e.g. active shooters, improvised explosive devices, insider threats and sabotage, cyber-attacks, etc.). Threats to the venue and nearby facilities (rail lines, chemical plants, airports, etc.) can all be considered. It would also be very useful to obtain relative probability estimates for each kind of threat. Vulnerability includes all possible attack paths and scenarios. The vulnerability analysis includes a review of all the operational security systems. Attacks from all possible access "vehicles" (people, vehicles, air- and water-borne) are considered. Consequences are the potential losses of human life, injuries, damages, business lost, environmental effects, and psychological damage. They include the possibility of cascading effects on and from interdependent infrastructure. The product of these three factors weighted by the probability of each kind of threat, when such estimates are available, gives an overall assessment of risk to the venue. A number of tools are available to assist with developing the risk assessment.

The team developing the risk assessment can include representative stakeholders of groups responsible for security planning, risk mitigation, and incident response and recovery operations. Team members internal to the venue are those involved in security and day-to-day operations. External stakeholders, including local law enforcement, emergency medical and fire services providers are important to the team in terms of coordinating planning and establishing good communication between venue staff and external officials. Large venues dealing with considerable risk may include an insurance underwriter on the team. Depending on the venue's location and surrounding infrastructure, external stakeholders can include officials from higher levels of government and managers responsible for neighboring infrastructure (transportation, gas and chemical facilities, hotels, etc.).

The venue profile is one important component of the risk assessment. The profile includes some basic information about the venue (location, ownership, capacity, etc.), a description of the typical events that take place in the venue, and an analysis of vehicle and pedestrian flow around the venue in connection with the events being hosted. The venue profile includes detailed descriptions of the critical assets associated with the venue. These include such physical assets as utilities on the premises, command and operation centers, communication centers, infrastructure and equipment, medical and fire stations, access control systems, physical security measures, etc. A site layout plan is also an important part of the venue profile as it can be used

as a means to identify vulnerabilities during planning and as a quick reference for those responding to an incident.

Policies, processes, and technologies to mitigate risk can be analyzed and then deployed as appropriate. Risk mitigation can involve measures to deter or defeat threats, as well as incident response plans to reduce the consequences of an attack. Examples of measures to deter or defeat threats include implementing vehicle and patron search procedures, and securing access to critical assets by deploying an employee access card system along with access alarms and monitoring cameras. Incident response planning can involve measures for rapid evacuation of the venue or sheltering-in-place, coordination with emergency medical and fire services, and preparations for mass decontamination.

Risk assessment is not a one-time process with static results. The assessment of threats, vulnerability, and consequences can change based on new intelligence (changes in terrorists' weapons, new attack scenarios and new target groups) and changes in any situation around or within the venue. Threats are constantly evolving, and there is a tendency to "fight the last war." Resources available to respond to an incident can change. New technology may become available that mitigates certain risks. The venue may be scheduled to host a unique event having unusually high attendance, a different stadium configuration, or significant federal security presence (e.g. United States Secret Service). For these and other changes, the risk assessment requires review and corresponding adaptation to the new information and circumstances.

In a Dynamic On-going Risk Assessment (DORA) process the initial risk assessment is constantly updated. The DORA process can address new intelligence being received continuously and incorporate the lessons learned from recent incidents at other venues. For example, the 2013 Boston Marathon bombing led to changes in security procedures at numerous venues. The DORA process also can be used to handle changes in response resources which may depend on the day, time, or nature of an event as well as budgetary restrictions.

1.3 Staffing: Leadership, Organization and Authority

Stadium security best practices put appropriate staff in place with a clear organization and command chain to respond effectively to the risks identified. Clearly defined leadership, staff organization, and lines of authority will help venue staff see where they fit into the stadium

security plan, be able to act when encountering a potential risk, and communicate efficiently to those in authority and the venue patrons.

The smooth transition of command and control during a major incident is critical to an effective response. Decisions about the roles and authority of involved individuals and agencies can be made at security planning sessions well before the time of any incident. Best practices follow the National Incident Management System's (NIMS) Incident Command System (ICS) as the model for organizing an incident response. When multiple agencies are involved (e.g. law enforcement, fire, and medical services, in addition to venue security), the ICS specifies the Unified Command doctrine. Unified Command unites the incident commanders of entities involved in incident response so that commanders of responding organizations make response decisions together according to ICS guidelines. Once these broad decisions have been made, the incident commanders retain control over the first responders reporting to them and the responsibilities assigned to their units. One principle of Unified Command is to have a common command center staffed by members of supporting and stakeholder agencies to promote efficient communications among the agencies.

The transition to the command and control structure that will respond to an incident can be practiced and tested in exercises involving the officials and staff who would respond to an incident. These exercises often are controlled "tabletops," that bring together responding agencies and venue staff to simulate the response to a scripted incident scenario. Such exercises can be held periodically to provide refresher training and counter inevitable staff turnover. The scripts for the exercise can simulate some anticipated problems such as failure of lines of communication between agencies, and people in the command structure not being available.

For venue employees involved in day-to-day operations and security, clear job descriptions, including their roles during an incident, can help ensure that employees perform their duties, and can clarify who takes over certain roles if the person originally assigned to the role is missing. Once they have the description of their roles in an incident, employees require repeated training and exercising on those roles. For contract security employees, knowing the organizational hierarchy and job responsibilities will foster efficient communication and appropriate assignment of responsibilities, but they too will require repeated training and exercises.

The organizational hierarchy and clear job descriptions are not intended to impede flexibility in

planning appropriate staffing levels. Staffing plans take attendance projections and other factors into account such as the current national threat level and any specific threats the venue has received. Specific security threats may be received with very little notice meaning the ability to add or adjust staff quickly might be necessary. Cross-training employees to handle multiple roles, improves the ability to move employees to critical locations and different roles as needed. Having enough hired personnel to staff various positions to the level necessary requires constantly checking and monitoring staff turnover. Entry-level, part-time, and seasonal work can result in high staff turnover rates and absenteeism, raising the possibility of not having sufficient staff to ensure a safe event. Robust badging and electronic key access systems can assist in monitoring employee numbers. Venues also can prioritize the staff security functions and make sure that enough qualified staffs are available for the most critical functions, even when overall staffing levels are low. Having a large pool of alternate employees and good relationships with third-party vendors also can alleviate staffing level problems.

Insider threats warrant special attention. Such attacks will likely be more difficult to detect and deter compared to attacks by outsiders, but can be mitigated using a number of processes and technologies. Employee background checks done prior to hiring for all prospective employees can be supplemented with updated background checks carried out randomly for hired employees. Venues can limit employee access to areas, computer systems, and critical infrastructure via access cards and camera monitoring. The level of access might depend partly on the strength of the background check. Finally, former employees also can pose a risk because of their detailed knowledge of the venue, including knowledge of the security plan. This risk can be mitigated by following a strict protocol for quickly repossessing items from terminated employees (e.g. credentials, access cards, keys, etc.), and randomizing security procedures as appropriate.

1.4 Information Management

Best practices for information management are part of stadium security because of the importance of communications among venue staff, between venue staff and first responders, and between venue staff and the public. Best practices for cyber-security also fall under information management, because cyber-attacks can disrupt communications causing problems in crowd management and impeding first responders. Information stored in computer systems also can be stolen, enabling terrorists to exploit employee credentials, building plans, delivery schedules, and

messaging systems for attacks.

Venue's staffs typically use radios, various forms of written reports, emergency call pagers, and landline and cellular telephones to communicate with each other. Because of the high cost of radios, their use is often limited to supervisory staff and management. Emergency call pagers have more limited functionality, but their low cost permits widespread use. Different channels on multi-channel radios can be assigned to different functions (e.g. various security levels) or locations (e.g. different tiers in the stadium), and all channels can be monitored at the command center. Training employees in the proper use of radios and maintaining the radios in good working order are two keys to their effectiveness. Written reports are most useful for information that is required to be archived and analyzed later. An example are reports of minor incidents of misbehavior from which statistics can be compiled to help determine staffing needs and crowd management strategies. Wired telephones for emergency use may be installed throughout the venue and can indicate instantly to control room staff where in the venue the call was placed. Cellular phones and smart phones are increasingly being used for communication within venues, although their effectiveness can be curtailed during times of network overload unless steps are taken to boost network capacity in and around the venue. A wired telephone not connected to the facility system can provide communications should the base system be compromised. In some cases, satellite phones are used for backup.

Venue security and operations staff need to communicate to people outside the venue, including law enforcement officers, emergency medical and fire services providers, and managers of nearby critical infrastructure if a terrorist incident occurs. It is important that channels of communication be established with each of these groups prior to any incident. While it is possible to communicate externally using any of the means used for internal communication, it is advisable that law enforcement agencies, medical and fire service providers have people stationed on site in a venue's control center during events. If these agencies cannot have people on site, direct lines of contact within the control center can be set up to each agency. Points of contact with managers of nearby critical infrastructure can be established prior to events and verified periodically.

Venue staff may need to communicate with the public during emergency and non-emergency situations. The means for public communication include public address systems, electronic message boards (e.g. LED boards and video boards) and television monitors, temporary or

permanent signage, and, increasingly, the use of social media and text messages. Some public address announcements can be prepared in advance and in multiple languages; others will require composition at the time of an incident. The same is true of electronic messaging boards which are also suitable for presenting phone numbers and website addresses for patrons to contact in emergency situations. Television monitors can provide access to media coverage as well as depict how patrons can handle various emergency situations. Posted signage, either temporary or permanent, can be useful in crowd management and letting patrons know the kinds of items that are permitted or not during the screening process. Text messaging systems and social media provide opportunities for two-way asynchronous communication between venue staff and patrons. Patrons can use such systems to ask questions and report complaints or disturbances. The messages can be attended to immediately and can be archived and mined for patterns. Venues can use these systems to assist in crowd management, for example by suggesting that patrons use different gates that may be lightly loaded during entrance or exit. The use of social media for stadium security is growing rapidly and new uses are still developing. Social media may be an effective way to distribute pre-event information updates to patrons expecting to attend an event. Following an event, social media may present efficient ways to collect data concerning patron satisfaction and fan experience. One caution concerning social media is that since there is little or no control over how patrons use it, social media can be a source of miscommunication and misinformation. It is critical that venue staff constantly monitor for and respond to inaccurate information.

Best practices for cyber-security protect digital information stored in computer systems including the personal information of employees and patrons, ownership and management emails and personal information, building plans, security measures, etc. Risk mitigation includes plans, policies, and technologies to prevent and deter cyber-attacks.

1.5 Operations

Operations management best practices include venue security operations and venue emergency response operations. Venue security operations are often implemented using a layered approach of outer, middle, and inner zones.

The outer perimeter of every venue is connected to the area transportation network, and the venue can use this point (coordinating with local transportation agencies and law enforcement,

re-routing traffic as necessary, etc.) as a start to reduce risk. Parking lots and structures typically are the next component of the outer perimeter. These may be owned by the venue or other companies and may be divided into areas for patrons, media, employees, or vendors. A variety of monitoring techniques including cameras and foot patrols, as well as structural and landscape design features can be part of outer zone security. The closer vehicles park to the venue stadium, the more important it is to implement detailed vehicle screening processes. Parking in areas reserved for vendors and service deliveries can require that a list of vehicles, their plate numbers, and their personnel be available ahead of their arrival for verification. Depending on the venue location, outer zone security could also involve coordinating with mass transportation agencies and even airports (to reduce the risk of air-borne attacks around the time of major events).

As patrons enter the security middle zone, they usually undergo some form of screening with pat-downs, wanding, and magnetometers being the most common. Bags brought in by patrons warrant detailed screening and the risk associated with bags may be mitigated by providing clear plastic bags and by implementing bag size restrictions. Choice of method for patron screening depends on several factors including the effectiveness of the method, the time taken to screen each patron (with resulting effects on queue length), the availability of trained staff, and patrons' reactions to the type of screening used. Randomization of screening, the use of multiple screening methods, educating patrons as to optimal arrival times, providing incentives to patrons to arrive early, and cross-training staff to do various forms of screening can help make patron screening more efficient and effective. Monitoring of queuing lines is important, because those standing in the lines can be a target for terrorist acts. This concern has caused some venues to implement screening simulation models that give information for decisions on the best configurations and procedures to use.

Besides patron screening, other concerns in the middle security zone include special access to the venue by vehicles using loading docks, and by the media. For the days of events, deliveries for everything except perishable items can be prohibited. For other days, the arrival of vehicles using the loading docks can be scheduled to allow time for vetting the delivery company, the driver's license of the delivery person, and the contents listed on the manifest. Delivery vehicles themselves can be screened outside the inner perimeter using an undercarriage survey and search of the trunk or trailer. If available, K-9 units also can be used to screen for explosives. Similar

attention is required for media personnel and trucks, which may be assigned a separate entrance. Cameras and sweeps by security staff are two measures that can be deployed effectively throughout the middle and inner security zones. Cameras can be placed so that critical areas can be monitored at the command center. Sweeps can be scheduled and/or randomized before and during events and supplemented with K-9 units as need and resources permit.

The security for the inner zone also addresses food delivery, storage, and preparation. Food delivery is a way terrorists could gain access to the venue, and food could be contaminated during storage or preparation. The inner zone also can be clearly marked using signage indicating which areas are off limits for patrons. Electronic access control and camera monitoring systems can be used to enforce these limits.

Operations management is also concerned with mitigating potential consequences of an attack through response planning. An important element of response planning is planning the evacuation of the venue. This process begins with the understanding that total evacuation is a last resort and may not be the correct response compared to shelter-in-place or partial evacuation. In fact, total evacuation can pose additional risks to patrons, since a large number of people will be exposed in an unscreened area outside the venue. Evacuation planning includes developing procedures and metrics for determining whether an evacuation is required, and preparing fans with information regarding evacuation procedures before the start of an event. If a total evacuation is necessary, it is expected that ushers and front-line staff will direct patrons, an extension of what they do during normal operations. For them to be able to execute this task effectively, prior awareness and training are needed. Arranging for patrons to leave the area surrounding the venue quickly requires coordination with local authorities and transit agencies. Venues may develop general response principles that can be applied to any type of terrorist incident, and more specific response plans for incidents that may be regarded as having higher priority such as bomb threats, fires, utility outage, CBRN incidents, active shooter scenarios, etc. Response planning involves collaboration with external agencies and joint tabletop training exercises. Response plans may have to be adjusted for higher profile events including those escalated to the National Special Security Event (NSSE) designation. In such cases the United States Secret Service takes the lead on security operations, and other federal agencies may lead response operations.

1.6 Training and Evaluation

Best practices for stadium security in the areas of training and evaluation focus on venue security and guest services staff (who may be employees or contractors), patrons who need training on such topics as evacuation procedures and screening processes, and internal and external first responders who may be called during an emergency. Since patron education and tabletop training exercises for first responders have been covered previously, this overview will focus on best practices for training and evaluation of venue security and guest services staff.

Some training needs and procedures for security and guest services staff depend on whether the staff members are venue employees or contractors. Employees can be expected to undergo regular training, while contractors may come with some training certified by their company, or by the state. A long-term regular employee will have a documented training history, but it may be more difficult to assess the skill of an incoming temporary contract employee. Venue managers can learn their state's guard certification requirements, do background checks on potential contractors, and request documentation regarding their certification. Venue operators can request language to be added to contracts with security and event-day vendors to allow the venue to perform quality assurance checks and certification verification in accordance with local legal limitations.

The venue's Director of Security can establish a set of minimum competency standards for venue security employees and contractors at all levels. Resources are available for assuring quality minimum competencies, including frequent short (5 min.) refresher training modules.

The Security Director also can implement a security training and assessment program for all venue staff with assessment results kept as part of employees' permanent records, and updated training administered periodically. Assessments can extend beyond answering test questions to quality assurance employing such on-the-job procedures as "secret shoppers" (patrons employed to ask questions or observe employee behavior), "red-teaming" (checking whether it is possible to bring prohibited items into a venue without being discovered by the screening process), incentive games (e.g. rewarding employees based on how quickly they can find a suspicious item) and "pop quizzes" administered on the job on a random basis. These kinds of quality assurance checks can be augmented by using the organizational hierarchy of the staff so that

those in a supervisory position continually audit the performance of front-line staff.

1.7 Summary

Here is a single statement of best practices for stadium security from each chapter:

1. Conduct a thorough risk assessment that is on-going and adaptive
2. Put staff in place with the appropriate organization and training on how to transition quickly to an incident command structure
3. Manage communications among venue staff, between staff and external responding agencies, and between staff and the public
4. Implement an operational plan including the staff, procedures, and technology for securing the venue and responding to incidents
5. Train staff constantly and use metrics to evaluate their performance

Chapter 2 – Risk Assessment

Introduction

Best practices for stadium security begin with a thorough risk assessment. The outcome of the risk assessment informs the other aspects of best practices discussed in subsequent chapters: staffing issues, information management, operations, and training and evaluation. Conducting a risk assessment is ***strongly recommended***. It is further ***recommended*** that the scale of the risk assessment carried out (the number and kinds of internal and external stakeholders involved, the number of consultants employed (if any), the deployment of security technologies, etc.) be appropriately sized for the venue and its associated risk.

While there is an extensive literature on general risk assessment procedures and analyses, sports venues pose some unique challenges in assessing risk. Some venues have an iconic character, and may host extremely high profile events, raising the value of an attack at the venue in the minds of terrorists. A venue may have extra vulnerability, because certain access paths are difficult or impossible to control. Venue and event stakeholders may have conflicting goals, including those of ticket holders who have paid to be entertained or to be part of a community experience. These and other factors must be taken into account as risk is assessed for each type of event held at specific venues. These risks must be evaluated and considered to make conscious decisions and understand what risks still exist and how best to mitigate those risks that are inherent given the goal and intent of the event.

Overall risk is essentially a product of three factors: threat, vulnerability, and consequences. Utilizing a risk assessment, a venue is able to articulate the overall risk it faces. Plausible potential threats include, but are not limited to, those in the National Planning Scenarios outlined within the National Response Framework. Vulnerability accounts for a facility's susceptibility to a given threat through the exploitation of security gaps or weaknesses. Consequences include loss of life, injuries, infrastructure damage, business losses, and environmental effects. These core elements of any risk assessment provide a big picture to a venue in understanding the potential damages caused by an incident and a starting point from which to devise an appropriate venue security plan. At a league level, it is ***recommended*** that officials become familiar with assessments of risk that pertain to all league venues and also those risks specific to unique

venues or venue attributes.

Through the risk assessment process, it is ***strongly recommended*** that the facility collect information including but not limited to the venue's profile, threat evaluations and a catalogue of current safety measures and policies. Venues are expected to use this information by assigning values based upon the relative probability, vulnerability and consequences of the identified threats. Risk management strategies and tactics are to be identified, analyzed, and if appropriate, implemented. This process results in a useful and comprehensive assessment that decision makers can reference when developing plans and procedures, purchasing and implementing technology, and determining the proper actions to reduce their facility's risk. Therefore, when implementing selected tactics, the tactics will reduce the risk identified within the assessment.

Although continual review and update of the risk assessment is an important part of the process, these primary risk assessments outlining baseline information are static. It is ***strongly recommended*** that these static risk assessments be supplemented by establishing a Dynamic On-going Risk Assessment (DORA) process to enhance risk management capabilities. A DORA process enables a venue to take just-in-time information such as updated intelligence, changes in resource availability, or other potential changes to the baseline risk assessment assumptions, and incorporate them into an event-specific security plan to reduce the risk to a venue. A DORA process uses the baseline risk assessment as a starting point, then considers and adjusts for factors unique to the specific event and time.

A number of tools and options (e.g. the RSAT tool and others described in the chapter appendix) are available to support a venue's effort to conduct a base-line risk assessment. These tools and options may be designed for in-depth self-assessments or third-party assessments. Some experts believe internal self-assessments provide a better operational perspective to the risks, while others believe that base-line risk assessments completed by an independent agency increases its validity in the eyes of executive personnel and possibly other stakeholders. A mixed approach also may be considered, but note that risk assessments developed by third-party consultants may be costly and unrealistic for facilities with limited resources. Regardless of the tool and method selected, it is ***strongly recommended*** that a venue understand and be able to describe the tool and process used, including the methodology for assigning risk, to ensure the assessment is carried

out properly.

Questions	Metric
Was a risk assessment conducted?	Y/N
Was the risk assessment self-conducted?	Y/N
Was a contractor used to support the risk assessment development?	Y/N
Was an off-the-shelf, free or purchased risk assessment tool used?	Y/N
Is a risk assessment conducted for each event?	Y/N

Open Ended Questions	Anticipated Response
What methodological approach did the venue take?	Methodology Description
What risk assessment tools were utilized in development of the risk assessment?	Tool Identification
What is done with the risk assessment? How is it used and implemented? Who knows of it and uses it?	Description of the Uses of the Risk Assessment

2.1 Risk Assessment Team

It is important to ensure that stakeholders with planning, mitigation, response, and recovery responsibilities are involved in a collaborative approach to developing the risk assessment. Prior to initiating the base-line risk assessment process, it is ***strongly recommended*** that the venue identify internal stakeholders involved in day-to-day operations and security who can be part of the process. Internal stakeholders may include, but are not limited to, the on-site engineer, senior technology and communications equipment staff, and key operations staff including security directors and supporting staff. These critical internal staff may improve the results by providing additional detail and insight into the facility's vulnerabilities beyond what may be known by some senior staff.

It is ***recommended*** that external stakeholders for the risk assessment process include local law enforcement, emergency medical services providers, fire services providers (including the fire marshal) and other first responders who may respond to an incident at the facility. Depending on

the venue profile, further involvement of outside agencies including all levels of government and law enforcement, interdependent infrastructure operators including area hospitals, transportation systems, utility providers, and industrial facilities, vendors, government critical infrastructure liaisons, and insurance underwriters, among others, may be needed.

Questions	Metric
Was a risk assessment team formed?	Y/N
How many people were on the risk assessment team?	#
What was the ratio of external to internal members of the risk assessment team?	:
In what percentage of revisions of the risk assessment were outsiders involved?	%

2.2 Venue Profile

Developing a complete venue profile ensures a base layer of data is available for conducting vulnerability assessments of the facility. It is ***strongly recommended*** that a venue develop a complete profile to include detailed lists and site locations of critical assets. It is ***strongly recommended*** that the venue profile include some high level general facility information such as the facility name, owner/operator, address, GPS coordinates, size and capacity, and the basic facility operational purpose. As part of detailing the characteristics of the owner/operator, each venue is ***recommended*** to specify the ownership of not only the venue but also the owners of the property the venue is located on and, if necessary, the owner(s) of the organization/team primarily utilizing the venue. In some instances in which not-for-profit (NFP) agencies own part or all of the ownership of any of these items, it is ***suggested*** the venue provide additional details as it relates to the venue's ownership structure, legal requirements and standards, and security funding mechanism(s) as it relates to these NFPs. As venue operators develop the details around the facility's operational purpose, it is also ***strongly recommended*** that a description of the typical events that take place at the venue, their frequency, and how the venue is used during those events be included. These typical events are those which the venue conducts on a regular basis and for which the venue has extensive operational experience. These may include various sporting events, festivals, concerts (concerts may be further broken out into types of

concerts), etc. which may occur daily, weekly or annually. Characterizing these event types by their attendance, vehicle throughput, cash transactions, as well as food and drink consumption supports understanding each event's crowd size and culture.

One-time events may warrant a risk assessment specific to that event, an example of the Dynamic On-going Risk Assessment process (see Section 2.5.2). Some of the venue profile information developed for typical events may not apply, and additional profile information (e.g. temporary changes in capacity, expected attendance, restrictions in access, special transportation needs, etc.) may have to be developed for the unique event.

Stadium operations naturally overlap with traffic/transportation operations. It is ***strongly recommended*** that venues conduct an analysis, in coordination with the surrounding roadway management agencies, to understand the flow of vehicles and pedestrians as well as general traffic demand. It is ***strongly recommended*** that the analysis include the development of specific traffic flow egress maps for the venues that include specific egress routes for responding emergency vehicles and/or first responders. It is ***recommended*** that this analysis include the identification of hot spots or critical intersections where traffic and crowds build. This information will support the risk analysis. It is important to specifically consider the risks during arrival and departure. For example, risk may increase due not only to the potential of an attack on these crowds, but also due to the hindrance these crowds place on egress of patrons during an evacuation.

Once the various operational uses by a venue are detailed, it is ***strongly recommended*** that the venue profile expand to describe the various critical assets. These assets will include both the critical physical assets and personnel assets. Many of these critical assets are described in detail in the subsequent chapters. It is ***recommended*** the critical assets be described so that their importance to operations is highlighted, so that this information can feed into the risk assessment. Physical critical assets include all utilities on premises; command and operation centers; all communication centers, infrastructure and equipment; medical and fire station(s) and equipment; access control systems; physical security measures; etc. The recommended information to be included as part of the critical asset description (if applicable), is detailed in Table 1.

By knowing the elements in Table 1, the risk assessment team will understand the value assignment during the risk assessment process. For example, if the asset is accessible to all, there is an increased risk due to tampering, access by terrorists, surveillance and monitoring of the asset by potential attackers, and other possible risks. Maintenance issues and failure rates could lead to asset inconsistencies and potential security failures. Critical assets also include personnel such as in-house security and staff, contractors, and vendors. These assets, like the physical assets, may be lost due to injury or death and therefore must be addressed in the venue's profile detailing their importance to operations and command.

Table 1. Critical Asset Description Information

Description Point	**Explanation**
Purpose	Description of the purpose and functionality of the asset to understand its importance to operations.
Location	Identification of the asset's location(s) or deployment area to assist in understanding what threats may impact the asset.
Access Information	Identification of access points to the critical asset(s) and who has access to them.
Visibility & Recognizability	The description of the ease with which an asset can be seen and identified
Age & Maintenance	Description of the asset's age and maintenance requirements.
Failure Rate/Resiliency	Description of how often the asset fails based on maintenance issues or external factors such as weather, etc., and the resiliency the asset has to threats such as forced entry, contamination, weather, tampering, etc.

It is ***recommended*** that a detailed site-layout plan also be developed depicting all structures on the premises, and the locations of emergency response equipment specifically identifying on venue maps the locations of fire extinguishers, fire hoses, pull stations and related fire/life safety equipment along with the location of automated external defibrillator (AED) units throughout the venue. If necessary, adjacent interdependent infrastructure that impacts operations such as parking lots/garages and/or transportation systems also can be depicted. By detailing these items in a site layout, the risk assessment team may gain a better

understanding of the vulnerabilities to the venue as each intrusion path is examined. These site layouts may also serve as a quick reference tool to assist those responding to an incident. For example, on a small scale, staff may be notified of the location of a fire extinguisher through the command center to put out a small fire. On a larger scale, an emergency response team may be able to use the site layout to support its response to an active shooter attack.

Questions	Metric
Does the venue detail the ownership structure of the venue structure, property and/or primary team(s) utilizing the venue?	Y/N
How many events occurred at the venue in the past year?	#
What was the average attendance of these events?	#
What is the maximum capacity by event type?	#
Does the venue have a list of critical asset descriptions?	Y/N
Does the venue asset description identify its importance to operations?	Y/N
Do asset descriptions include a list of personnel who have access?	Y/N
Do asset descriptions describe the asset's visibility and recognizability?	Y/N
Do asset descriptions identify the asset's maintenance requirements?	Y/N
Do asset descriptions identify the asset's failure rates and/or resiliency rating?	Y/N
Does the asset description include the importance of staffing positions to operations?	Y/N
Does the venue have a site layout plan?	Y/N
Does the site layout plan identify all facility access points?	Y/N
Does the site layout plan identify all utilities?	Y/N
Does the site layout plan detail all structures on premises?	Y/N
Has the venue conducted a traffic and pedestrian analysis?	Y/N

Open Ended Question	Anticipated Response
Describe the typical events the facility conducts.	Venue Functional Purpose Description

2.3 Threat, Vulnerability and Consequence

2.3.1 Threat Identification

The risk assessment team assembled by the venue needs to determine what the plausible threats

are to a venue. It is ***strongly recommended*** that the risk assessment include a thorough threat assessment and be as inclusive as possible in its threat consideration. It may include the scenarios detailed within the DHS Target Capabilities List (TCL) as well as those discovered through research and risk assessment team discussions. Terrorist threats may include active shooter attacks (single or group); improvised explosive devices (IED) placed in or around the facility or on a suicide bomber; vehicle borne IED (VBIED); forced entry attacks; chemical, biological, nuclear or radiation attacks; insider threats/sabotage; cyber-attacks; and food and/or water contamination. These attacks may occur anywhere in and around the facility. For example, the 2013 Boston Marathon IED attack shows that any area may be threatened if a concealed explosive device can be carried, placed, and detonated in the area in a rather short time frame. Experts have become concerned for the safety of those patrons gathering at gate entry points prior to security screening (see section 5.2.1). Venue operators can identify similar concerns for their own facilities.

Other threat considerations may include incidents or attacks on nearby facilities that may pose a risk to the venue such as freight rail lines, chemical facilities, airports and military installations.

Once the range of possible threats is identified, it is ***strongly recommended*** that venue operators determine the relative likelihood of each threat occurring at the venue. Exact probabilities may be impossible to determine. However, it is ***recommended*** that venues consider conducting research into incidents which have occurred nationally or internationally through established terrorism databases, potential incidents that have occurred at the venue operator's facility or an in-kind facility, or may have been deterred or stopped by current security measures. Venues can address the relative likelihood of incidents by rank ordering them, or putting them into categories, e.g. High, Medium, or Low likelihood. An estimate of incident likelihood can be assigned as part of the risk assessment. As an alternative, due to the limited experience with some of the threats that may be identified, simply assigning the same likelihood to all terrorist attacks will limit the impact probability estimates have on the risk assessment output given the generally unknown nature of some threat probabilities.

Questions	Metric
Has a thorough threat assessment been conducted describing each potential threat as part of the risk assessment?	Y/N
What is the estimated likelihood for each threat to occur?	:
Were the threats cross-checked with other risk assessments carried out by local municipalities, county, or state?	Y/N

Open Ended Questions	Anticipated Response
How were incident likelihoods determined?	Describe process for determining threat likelihood.

2.3.2 Vulnerability and Consequence Analysis

After identifying the threats and their likelihood, the venue staff in collaboration with representatives from local law enforcement and first responders will review each threat to understand its relation to vulnerability and consequence. In addition, it is ***suggested*** venues also consider criticality, accessibility, the ability to recover from threats, and the ability to recognize threats. Under this review process, a value will be assigned to each category detailing the level of risk each threat poses. The value will depend extensively on the systems and security practices in place by a venue which are described throughout the other chapters within this guide.

To assist in determining values, it is ***strongly recommended*** that the risk assessment include standard staffing plans and training for event and non-event days detailing the number of staff available, and their assigned positions. It is further recommended that details include the number of staff, location, and their responsibilities inside and outside the venue. In addition, some experts suggest inclusion of flow charts depicting the process for handling vendor deliveries, mail deliveries, and cash transactions.

It is ***strongly recommended*** that a risk assessment contain a detailed fire safety risk assessment and a medical response risk assessment. These core support assessments provide a facility with an understanding of their fire response and suppression capability, as well as their medical response capabilities. It is ***recommended*** that the ability for response systems to surge during mass fatality incidents and other major threats be identified. The results of the vulnerability analysis and subsequently the risk assessment will drive the changes to the security plan components.

The vulnerability analysis will account for a facility's susceptibility to a given threat. The susceptibility may include how likely an attack would be to reduce or cease operations by affecting the venue's critical systems. In addition, the vulnerability analysis involves assessing the venue's susceptibility to the exploitation of security gaps or weaknesses and/or the infrastructure's increased risk of destruction. This may include understanding the queue times at gate entry points as described in Chapter 5 to understand crowd vulnerability to attacks. It is ***recommended*** that vulnerability assessment also include inherent facility design flaws that a terrorist may exploit to increase the consequences of an attack. Examples include explosive device attacks near fuel storage areas or weak structural areas, or a chemical release attacking an insufficient HVAC system causing it to spread airborne chemicals rather than filtering them out. In addition, it is ***suggested*** that visible vulnerability be addressed. Should a terrorist be able to gather intelligence through reconnaissance and identify the location of critical systems, those systems become more vulnerable.

Vulnerability also can be affected by the information released, willingly or unwilling by the venue. For example, expanding information sharing systems between agencies may increase the number of individuals who have information available to them regarding the venue's security system. Publically available information such as venue blue prints also may make the venue more vulnerable. Venue management can consciously balance benefits and drawbacks, and then decide between sharing information and keeping the information private for an optimized security posture.

Vulnerability may be broken down into pre- and post-incident vulnerabilities. It is ***strongly recommended*** that venues measure the security system's ability to detect a threat prior to an occurrence. This includes a review of the various operational security systems, including a review of the perimeter security system's ability to deter and detect a threat by analyzing all potential intrusion paths an attacker may take. These operational security systems are described in the subsequent chapters which provide measurable metrics that venues may consider using for supporting the value assignment during the vulnerability assessment. While reviewing intrusion paths, it is ***recommended*** that venues consider attacks from various originating access points such as vehicles, persons, air-borne attacks, and water-

based attacks. Attack access points and paths may have an effect on consequences (see below). For example, a separate media entrance may be more vulnerable to a bag placed with an IED outside, but such a scenario also has limited consequences compared to an IED placed at a busy patron access point.

Some experts believe methods of attacks by terrorists evolve and therefore the understanding of these intrusion paths can also evolve. The Boston Marathon attack highlights the need to evolve the understanding of attack paths including the time at which an attack may be carried out.

Venues are also ***recommended*** to consider their ability to respond and recover from an incident as part of their vulnerability assessments. For example, a mass casualty response plan may mitigate human consequences, or a backup generator may mitigate all potential cascading consequences from an attack on the power grid.

It is ***strongly recommended*** that consequences be considered (see Table 2 for some types of consequences). It is recommended that consequences be measured first in human losses. Human losses may be defined in terms of deaths and expanded to include injuries, the quality of life and the life expectancy of those injured. Public health and effects on human psychology may also be considered consequences if attacks focus on spreading disease or contamination causing public health scares.

In addition to the most notable consequence, human casualties, venues are ***recommended*** to consider how a threat may cause economic impacts. This may be as simple as calculating the financial cost to a venue in terms of costs to repair infrastructure, immediate and possibly long term loss of revenue, insurance costs, lawsuits, etc. Higher level economic impacts also may be analyzed. Venues may consider how the incident affects their industry or the local municipality and area businesses such as local restaurants, hotels, or transportation services. It is possible that a terrorist act could have statewide, regional, national or even global effects. Insurance rates may rise for all venues across the state or country, national airlines may see a significant decrease in air travel, all levels of government may see a drop in tax revenue and perhaps a significant national response to a public health emergency will be needed. In addition to revenue costs, changes in insurance and spending patterns, costs in elevating response to protecting the public

and economic impact to the victims of any such incident may also be considered. In some cases, venues may place dollar amounts on casualties as each victim would carry healthcare cost to support personal recovery.

It is ***recommended*** that other consequences such as cascading effects on interdependent infrastructures and resources be considered. Perhaps destruction causes the loss of a number of public transport buses limiting availability of buses to address normal transportation operations. Or perhaps an attack causes the loss of multiple municipal EMS resources causing the municipality's medical services to be backfilled by neighboring jurisdictions. Increased response times may result, affecting patients in multiple jurisdictions.

Consequences may also take time and environmental impact into account. It is ***suggested*** that consequence identification include the length of time it will take for the venue to begin operating again and the time it will take to recover fully. Finally, it is ***suggested*** that environmental impacts be addressed. A chemical, biological, radiological and/or nuclear attack may pose significant challenges and resulting consequences to the environment including significant contamination. The time course of the contamination will figure into the consequence analysis.

Table 2. Consequence Types & Description

Consequence Type	Consequence Description
Human	Deaths Injuries Overall Casualties Psychological Impacts Public Health Emergency Impacts (Local, State, Regional, National, Global)
Environmental	Impacts to air quality Impacts to water quality Impacts to vegetation Impacts to wildlife Impacts to land use

Economic	Damage costs to venue Damage costs to area infrastructure Venue insurance and legal liabilities costs Lost venue revenue due to venue closure Lost venue revenue due to incident both immediate and future Lost league revenue due to incident Lost industry revenue Lost local business and municipal/city revenue Lost state revenue Lost regional revenue Lost national revenue Lost global revenue Victims health care costs in dollars Victims costs for burial services Venue property devaluation Surrounding property devaluation Incident response costs
Infrastructure & Resource	Damage Impacts to operations Impacts to adjacent infrastructure (transportation, rail lines, etc.)

Questions	Metric
List the consequences of each threat by incident type in terms of deaths and injuries.	#
List the consequences of each threat by incident type in terms of economic loss.	$
List the consequence of each threat by incident type in the time it will take the venue to recover to full operation.	t

Does the risk assessment identify environmental consequences?	Y/N
Does the risk assessment identify public health consequences?	Y/N
Was a fire safety assessment completed as part of the overall risk assessment?	Y/N
Was a medical response assessment completed as part of the overall risk assessment?	Y/N

Open Ended Questions	Anticipated Response
Describe how the threats identified impact/relate to the facility's vulnerability for each incident type.	Detailed vulnerability assessment.
How were the threats prioritized in the risk assessment?	Description of risk assessment valuation of threats including estimated likelihoods and consequences.
How were the consequences compared across the threats analyzed (e.g. how were human consequences compared to economic consequences)?	Description of comparison analysis conducted between consequences to support threat prioritization and risk management decisions.
How were the economic consequences calculated and what do they represent (venue loss, local economic loss, league loss, regional loss, etc.)?	Description on the criteria and formulas used to calculate the economic consequences.
What criteria were used for assigning consequence values?	Description of inputs used to assign values.
What do the consequence values represent?	Definition of what the value means.
What criteria were used for assigning vulnerability values?	Description of inputs used to assign values.
What do the vulnerability values represent?	Definition of what the value means.

2.3.3 Addressing the Risk Assessment

Upon completion of the prioritization of the threats and potential impacts, it is ***strongly recommended*** the risk assessment team thoroughly identify the available security control measures available to them on a regular basis and deployed based upon the results of the threat prioritization. The deployment of assets may include mobile technology and

equipment and staffing resources. In addition, it is ***recommended*** that venues expand the risk assessment further to detail how an expected and anticipated variation to each event impacts the prioritization and risks posed to the venue. These potential impacts, which may be anticipated, include the time of day the event occurs, the day of week the event occurs, the patron demographic and fan culture, and weather/climate changes.

Questions	Metric
Does the risk assessment identify the available security control measures available to the venue on a regular basis?	Y/N
Are resources deployed based on the risk assessment?	Y/N
Does the risk assessment describe how the variations in the event timing, demographics and weather impact the results of the risk assessment?	Y/N

Open Ended Questions	Anticipated Response
Describe how these control measures are deployed against the risk assessment for the base-line security plan.	Description of facility resource deployment plan.

2.4 Infrastructure Interdependencies

The location of the facility will have a unique relationship to surrounding infrastructures and therefore it is ***strongly recommended*** that venues identify potential interdependencies with those infrastructures. An attack on key support infrastructures may lead to significant cascading consequences. Supporting infrastructure may include area transportation providers such as rail, bus, taxi services, waterway services, airports, etc. For example, a venue may have a rail station located on-site. Should a threat be made against that transportation network, the venue will need to address that threat as well. These interdependencies may also allow for shared security and intelligence between the station operator and the venue. It is ***recommended*** that utility providers also be reviewed. Should a utility be attacked or fail, how does the venue address the possible loss of electricity, gas, or water in their security plan? What sort of impact might an attack or failure within the venue have on the utility provider?

Furthermore, it is ***recommended*** that a review of infrastructure interdependencies include support service facilities such as food and drink vendors, local hotels and motels and parking structure owner/operators. These businesses may have unique risks unto themselves but may provide key intelligence for potential threats against a venue. Suspicious behavior may be relayed to venues or these industries may share equipment and resources to reduce risk. Other stakeholders that are ***recommended*** for inclusion are all facilities that pose a risk to the venue if an incident occurs at that facility. A chemical facility may exist near a venue in which a chemical release will require immediate response by the venue. There are also facilities that venue operators may depend on should an incident occur at the facility. These include hospitals which have inherent risks of their own but have a need to be knowledgeable of the venue's capability to respond to an incident.

Questions	Metric
Does the risk assessment identify potential cascading consequences from incidents at interdependent infrastructures?	Y/N
Does the risk assessment address area transportation systems?	Y/N
Does the risk assessment address area utility providers?	Y/N
Does the risk assessment address area hospitals?	Y/N
Does the risk assessment address vendor facilities?	Y/N
Does the risk assessment address area parking lots/garages?	Y/N
Does the risk assessment address area hotel and motels?	Y/N
Does the risk assessment address those facilities identified within the list of potential incidents?	Y/N

2.5 Dynamic Re-assessment Protocol

2.5.1 Risk Assessment Review Process

Once the base-line risk assessment is completed, it is ***recommended*** that venues share the results with law enforcement agencies with direct jurisdictional responsibilities and, if deemed appropriate, escalate the results to higher levels of government and law enforcement. In addition, it is ***strongly recommended*** that continuous evaluation of the base-line risk

assessment be carried out based on the quality assurance program implemented by the venue. Continuous evaluation will support on-going re-assessment and stakeholder coordination. It is ***strongly recommended*** that on-going re-assessment of the base-line risk assessment be done annually at a minimum. A more frequent review is ***suggested*** and may include pre-, mid- and/or postseason review. Continuous review of the base-line risk assessment through jurisdictional exercises, re- assessments, and evaluations allows the venue to address issues experienced since the last risk assessment. The continuous review will allow updates to the risk assessment and the security plan as changes occur in security standards, tactics, technologies, and personnel. Examples of technology changes include improvements in magnetometers, new screening tactics, and advanced behavioral assessment systems.

Questions	Metric
How often does the venue conduct a re-assessment or review of the base-line risk assessment?	Freq.
When was the original base-line risk assessment completed?	Date
When was the last base-line risk assessment updated?	Date
Has the law enforcement agency with primary jurisdiction been notified of the risk assessment results (and on-going updates to the risk assessment)?	Y/N
Does the venue share the results of the base-line risk assessment with local or state law enforcement?	Y/N

2.5.2 Dynamic On-Going Risk Assessments

It is ***strongly recommended*** that venues incorporate a Dynamic On-going Risk Assessment (DORA) process to address intelligence being received continuously, lessons learned from previous events and incidents, and unique events that may occur at the venue. In the aftermath of the Boston Marathon bombings, venues around the country immediately re-assessed their risk following the attack and responded accordingly. Some removed trash cans from the exterior of the venue; others changed bag policies, and some venues cancelled events altogether. As part of this DORA process, it is ***suggested*** that venues consider developing a cost benefit analysis procedure that allows decision makers to effectively manage risk. The

benefit may be measured in terms of the reduction in risk. These risk mitigation efforts may enhance deterrence, harden a threatened or weakened security system or decrease the likelihood an attack occurs or succeeds. Increases in cost may include the cost of increased consequences as well as the cost for implementing mitigation efforts. It is appropriate for venues to consider if such efforts are affordable based upon this cost-benefit analysis.

Changes addressed by the DORA process can vary widely. Resources made available by public entities or other stakeholders may change by event. Resource changes could be due to the day of week; other event operations going on around the municipality; other incidents occurring around the municipality such as local law enforcement investigations, which pose additional concerns; and budgetary reasons. Intelligence may be received specifying a type of attack where the security is needed for in-depth bag checks or thorough inspection of specific vehicle types.

Crowd behavior changes may cause changes in threat as well. Weather, field intrusions, political dignitary attendees, on-field incidents between teams, polarizing opponents, changes in event timing, alcohol sales, promotions (providing objects available for throwing) all can affect crowd behavior. Special ceremonies, commercial activities, or other special events in the area, may raise cause for concern as well. For example, a dignitary throwing out the first pitch may be threatened by protesters, some possibly with violent intentions. Other changes include utility and technology failures, including loss of radio communication technologies and/or cell phone service. A DORA process also may be required to implement a security plan for events not typical for the venue such as speeches by dignitaries and religious leaders or to address weaknesses in security discovered during an incident that require immediate attention. Venues also may encounter threats against a specific employee or threats made by an insider. Other issues such as public health emergencies or high media exposure for an event also can necessitate a DORA process.

Questions	Metric
Has the venue developed a DORA process?	Y/N
Does this process address the redeployment of security control measures?	Y/N
Does this process include a cost-benefit analysis for deploying/re-deploying additional resources?	Y/N

Does the venue implement a corrective action process in response to an incident based after action reports?	Y/N
Is an event-day risk assessment developed?	Y/N
For unique events, does the venue conduct a suitability assessment?	Y/N

Open Ended Questions	Anticipated Response
Who conducts this event-day/week assessment?	List of Agency(s) or Staff Position(s)
How does the venue ensure these corrective actions are implemented?	Description of Implementation
Describe the integration of the new intelligence into the base-line risk assessment?	Description of new intelligence use against base-line risk assessment.

2.6 Risk Assessment: Key Points

- Overall risk is essentially a product of three factors: threat, vulnerability, and consequences.
- Continual review and update of the risk assessment are important after establishing a risk assessment baseline.
- One-time events may warrant a risk assessment specific to that event; this is part of the Dynamic Ongoing Risk Assessment (DORA).
- It is important to ensure that stakeholders with planning, mitigation, response, and recovery responsibilities are involved in a collaborative approach to developing the risk assessment.
- The risk assessment team assembled by the venue needs to determine what the plausible threats are to a venue.
- After identifying the threats and their relative probability, the risk assessment team will review each threat to understand its relation to vulnerability and consequence.
- Developing a complete venue profile ensures that a base layer of data is available for conducting vulnerability assessments of the facility.
- Critical assets are addressed in the venue's profile detailing their locations and importance to operations and command.
- The vulnerability analysis accounts for a facility's susceptibility to a given threat.
- An attack on key support infrastructures may lead to significant cascading consequences.
- Continuous review of the base-line risk assessment through jurisdictional exercises, re- assessments, and evaluations allows the venue to address issues experienced since the last risk assessment.

2.7 Recommendations – Chapter 2 Risk Assessment

Chapter 2 – Risk Assessment	
Strongly Recommended	Section
Each venue conducts a risk assessment.	Intro
The venues collect information including but not limited to the venue's profile, threat evaluations and a catalogue of current safety measures and policies.	Intro
Static risk assessments to be supplemented by establishing a Dynamic On-going Risk Assessment (DORA) process to enhance risk management capabilities.	Intro
Venues understand and be able to describe the risk assessment tool(s) and process used, including the methodology for assigning risk, to ensure the assessment is carried out properly.	Intro
The venues identify internal stakeholders involved in day-to-day operations and security who can be part of the [risk assessment] process.	2.1
Venues specify [as part of the venue profile] the ownership of not only the venue but also the owners of the property on which the venue is located and, if necessary, the owner(s) of the organization/team primarily utilizing the venue.	2.2
Venues develop a complete profile to include detailed lists and site locations of critical assets.	2.2
The venue's profile includes some high level general facility information such as the facility name, owner/operator, address, GPS coordinates, size and capacity, and the basic facility operational purpose.	2.2
A description of the typical events that take place at the venue, their frequency and how the venue is used during those events be included in the venue profile.	2.2

Venues conduct an analysis, in coordination with the surrounding roadway management agencies, to understand the flow of vehicles and pedestrians as well as general traffic demand.	2.2
The traffic/transportation analysis includes the development of specific traffic flow egress maps for the venues that include specific egress routes for responding emergency vehicles and/or first responders.	2.2
The venue profile expands to describe the various [physical and personnel] critical assets.	2.2
The risk assessment includes a thorough threat assessment and be as inclusive as possible in its threat consideration.	2.3.1
Venue operators determine the relative likelihood of each threat occurring at the venue.	2.3.1
The risk assessment includes standard staffing plans and training for event and non-event days detailing the number of staff available, and their assigned positions.	2.3.2
A risk assessment contains a detailed fire safety risk assessment and a medical response risk assessment.	2.3.2
Venues measure the security system's ability to detect a threat prior to an occurrence.	2.3.2
Consequences to be considered (see Table 2 for some types of consequences).	2.3.2
The risk assessment teams thoroughly identify the available security control measures available to them on a regular basis and deployed based upon the results of the threat prioritization.	2.3.3

Venues identify potential interdependencies with surrounding infrastructures.	2.4
Continuous evaluation of the base-line risk assessment be carried out based on the quality assurance program implemented by the venue.	2.5.1
On-going re-assessment of the base-line risk assessment to be done annually at a minimum.	2.5.1
Venues incorporate a Dynamic On-going Risk Assessment (DORA) process to address intelligence being received continuously, lessons learned from previous events and incidents, and unique events that may occur at the venue.	2.5.2
Recommended	
The scale of the risk assessment carried out (the number and kinds of internal and external stakeholders involved, the number of consultants employed (if any), the deployment of security technologies, etc.) to be appropriately sized for the venue and its associated risk.	Intro
League officials become familiar with assessments of risk that pertain to all league venues and also those risks specific to unique venues or venue attributes.	Intro
External stakeholders for the risk assessment process include local law enforcement, emergency medical services providers, fire services providers (including the fire marshal) and other first responders who may respond to an incident at the facility.	2.1
The traffic/transportation analysis includes the identification of hot spots or critical intersections where traffic and crowds build.	2.2

The critical assets be described so that their importance to operations is highlighted, so that this information can feed into the risk assessment.	2.2
A detailed site-layout plan also be developed depicting all structures on the premises, and the locations of emergency response equipment specifically identifying on venue maps the locations of fire extinguishers, fire hoses, pull stations and related fire/life safety equipment along with the location of automated external defibrillator (AED) units throughout the venue.	2.2
Venues consider conducting research into incidents which have occurred nationally or internationally through established terrorism databases, potential incidents that have occurred at the venue operator's facility or an in-kind facility, or may have been deterred or stopped by current security measures.	2.3.1
The ability for response systems to surge during mass fatality incidents and other major threats to be identified.	2.3.2
The vulnerability assessments include inherent facility design flaws that a terrorist may exploit to increase the consequences of an attack.	2.3.2
Venues consider attacks from various originating access points such as vehicles, persons, air-borne attacks, and water-based attacks.	2.3.2
Venues consider their ability to respond and recover from an incident as part of their vulnerability assessments.	2.3.2
Venues consider how a threat may cause economic impacts [in addition to human casualties].	2.3.2
Other consequences such as cascading effects on interdependent infrastructures and resources to be considered.	2.3.2
Venues expand the risk assessment further to detail how an expected and anticipated variation to each event impacts the prioritization and risks posed to the venue.	2.3.3

Utility providers also to be reviewed. [How to address loss of electricity, gas, or water should a utility be attacked or fail?] What sort of impact might an attack or failure within the venue have on the utility provider?	2.4
A review of infrastructure interdependencies include support service facilities such as food and drink vendors, local hotels and motels and parking structure owner/operators.	2.4
All facilities that pose a risk to the venue if an incident occurs at that facility be included in the analysis of infrastructure interdependencies.	2.4
Venues share the results with law enforcement agencies with direct jurisdictional responsibilities and, if deemed appropriate, escalate the results to higher levels of government and law enforcement.	2.5.1
Suggested	
Venues provide additional details about the venue's ownership structure, legal requirements and standards, and security funding mechanism(s) in those instances where not-for-profit (NFP) agencies own part or all of the venue, the property, or the team or organization primarily using the venue.	2.2
Venues also consider criticality, accessibility, the ability to recover from threats, and the ability to recognize threats.	2.3.2
Visible vulnerability be addressed. Should a terrorist be able to gather intelligence through reconnaissance and identify the location of critical systems, those systems become more vulnerable.	2.3.2
Consequence identification includes the length of time it will take for the venue to begin operating again and the time it will take to recover fully.	2.3.2
Environmental impacts [consequences] be addressed.	2.3.2

Risk assessments be updated more frequently than once per year, and may include pre-, mid-, and/or postseason reviews.	2.5.1
Venues consider developing a cost benefit analysis procedure that allows decision makers to effectively manage risk.	2.5.2

Appendix - Chapter 2

This Appendix provides information about resources to assist with risk assessments, and details concerning the makeup of the risk assessment team and the content of the venue profile. It also offers some further information on threat identification, risk and vulnerability analysis, infrastructure interdependencies, and dynamic reassessment protocols.

Risk Assessment Tools

- The U.S. Department of Homeland Security has developed a free tool, the Risk Self-Assessment Tool (RSAT) for commercial facilities (http://www.dhs.gov/risk-self-assessment- tool-commercial-facilities). This tool requires a relatively short time commitment and can be used by in-house staff. In addition to RSAT, the Site Vulnerability Assessment (SVA) is a vulnerability assessment tool, and the Infrastructure Survey Tool (IST) is a survey of protective measures.
- Two additional DHS programs, "Site Assessment Visits (SAV)" and "Buffer Zone Protection Plan (BZPP)," have the advantages that individuals with specific skill sets are brought to the venue through these assessment processes and they are able to provide an outsider's assessment of the facility as opposed to conducting the assessment in-house. The DHS RSAT Tool accomplishes the same objective by directing the facility to answer specific questions and then ranking the assessment profile for the venue against industry peers.
- Methodological approaches to risk assessment include but are not limited to: Criticality, Accessibility, Recognizability, Vulnerability, Effect, Recuperability (CARVER); Risk Analysis and Management for Critical Asset Protection (RAMCAP); Failure Mode, Effects and Critical Analysis (FMECA); Hazard Operability Analysis (HazOp).

- Venues also can look for outside facility risk assessment assistance through their state, city and county Homeland Security offices. In most instances, major professional sports venues are considered to be critical infrastructures and, as such, most of these Homeland Security offices will offer assessment services to these venues.

Risk Assessment Team

- Risk assessment teams can include the following individuals. Primary team members (those required for assessments at most venues) are indicated by an asterisk (*). Other individuals may be required depending on the venue's size, location, and surrounding infrastructure.
  - Law Enforcement* (Local*, State, & Federal)
  - Fire Safety Officials*
  - Fire Department
  - Emergency Medical Services*
  - Emergency Management* (Local* & State)
  - Homeland Security (State & Federal)
  - Utility Providers
  - Elected Officials (Local)
  - Transportation Agency's (State & Private)
  - Interdependent Infrastructure Representatives
  - Facility Executive Staff & Leadership*
  - Security Director*
  - Crowd Management (supervisors and staff)*
  - Information Technology Staff
  - Communication Technology Staff*
  - Staff Engineers*
  - Parking Operators (third-party and venue)*
  - Vendors/Contracted Staff (Food, Technology Maintenance, Security, etc.)

- Development of the static base-line risk assessment may incorporate a larger number of experts and staffing roles than a team developed to conduct a DORA process.

Venue Profile

- When evaluating critical assets, venues may consider describing inherent incompatibility issues between systems. For example, law enforcement and the on-site command center do not have interoperable radio systems.
- A comprehensive pedestrian and traffic analysis may include: the identification of hot spots or critical intersections at which traffic backs up, pedestrian flow is constrained, or interaction between vehicle and pedestrian traffic causes critical impacts; identification of general travel demand for each roadway leading to and from the facility during normal ingress/egress operations; staffing of parking lots, roadways, and traffic control; policies for limiting egress evacuation operations from being impacted by vehicles already on the transportation network; consideration for event types; work to separate pedestrian movements from vehicle movements; coordination with public parking garages; analysis of potential contra- flow lane operations; lanes of roadways around venues; capacity of roadways in area; locations of traffic management devices (i.e. Virtual Message Signs, Cones, Barrels, Barriers, etc.); and the timing of when these devices are set up and removed.
- Capacity estimates may use federal guidelines detailed within the Highway Capacity Manual. Examples include 1800 vehicles per hour per lane for free flowing highways and 1200 vehicles per hour per lane along roadways with intersections (as long as lane is the major approach to the intersection). Additional information may be gathered through coordination with a local and/or state transportation agency.
- Identification of general travel demand may be done via the following techniques: observation and vehicle counts; spot counts at major intersections; origin zip codes based on season ticket holders and likely route to the venue. Additional information may be gathered through coordination with local and state transportation agencies.
- Hot spots may be identified through the use of camera footage to identify bottlenecks due to pedestrian flow across roadways or vehicle back-ups. Additional information may be gathered through coordination with local and state transportation agencies.
- The Automated Critical Asset Management System (ACAMS) is a web-based portal run

by DHS that may be used to add the venue profile information to a database of critical infrastructure data. As described on its website: "ACAMS is a secure, online database management and analysis platform that allows for the collection and management of critical infrastructure asset data; the prioritization, analysis, and visualization of this data; the production of tailored infrastructure reports; one-click access to critical asset data to inform emergency response, and the development of a variety of pre- and post-incident response plans useful to strategic and operational planners and tactical commanders."

Threat Identification

- VBIEDs include motorcycles, and air-based attacks.
- Comparing threats with local and state hazard and risk analysis may improve reliability of inputs and ensure all potential threats are covered.

Risk and Vulnerability Analysis

- Research may be conducted utilizing the Global Terrorism Database (GTD) or the RAND Database of Worldwide Terrorism Incidents (RDWTI).
- The attack on the Boston Marathon has highlighted that vulnerability may not only include determining the venue's ability to detect suspicious bags but also the speed of identifying and responding to the suspicious bags.

Infrastructure Interdependencies

- Creation of a public and private Memorandum of Understanding can enable the sharing of security camera feeds between nearby infrastructures, the venue and law enforcement. This arrangement may assist in decreasing risk. However, note that depending on sources that have poor security systems may increase risk.
- Working with interdependent infrastructures such as hotels may provide information concerning suspicious behavior of guests. For example, working to train hotel staff on identifying suspicious behavior by using available state and local law enforcement resources may increase connectivity and information flow, and regular communication with hotel security could encourage sharing of concerns about suspicious behavior.
- To reduce risks of adjacent chemical facilities, venues can coordinate with these

organizations to see if high risk activity such as chemical delivery, movement, etc. could occur outside of event-day times.

- Response plans for utility failures could reduce risk and avoid cascading effects.
- Risk assessment may include understanding the risks vendors have as part of their overall supply chain. For example, the likelihood and risk assessment results of food vendors having their food contaminated prior to delivery to a venue.

Dynamic Re-Assessment Protocol

- Venues may consider implementing annual risk assessment reviews supplemented by in-season re-assessments during normal operational breaks (All-Star Game; bye weeks) and more frequently in many situations. In addition, venues can consider developing a process for collecting information from staff concerning current security practices and their effectiveness. Addressing this feedback quickly (daily, days following events, weekly), allows for on-going dynamic re-assessments and updates to the security plan.
- Venues that may be considered for a National Special Security Event (NSSE), or something similar, can build a process for incorporating additional agencies into the assessment process. In such cases, federal agencies will take over many security functions with corresponding effects on risk.

Chapter 3- Staffing: Leadership, Organization and Authority

Introduction

This chapter discusses operational staffing and decision making processes and protocols. The three components of this chapter's title can each be thought of as a necessary element of the answer to the question "Have I established personnel in order to effectively respond to the risks assessed?" While each venue is unique in scale and the nature of event produced, the best practices in this section provide the framework necessary for implementing a security plan and

the seamless transition from event management to incident command structure. Similar to concepts discussed in other chapters, leadership, organization and authority are not static concepts. Each needs to be assessed and refreshed with employees so that reaction time and quality of service are not eroded.

While we often think of leadership, authority, and organization at the macro-scale for venues, each concept can play a crucial role for each venue employee. Employees, through their occupational responsibilities would benefit from a strong understanding of security organization so as to truly understand the part they play within it. Additionally, front-line security personnel might feel both educated enough and supported enough to "take the lead" when seeing a potential risk occurring within their area. Finally, these personnel must use their knowledge of the organization to communicate efficiently to those on the security team who possess the authority to make the right call.

This chapter comprises the following topics: command and control; organizational hierarchies; staffing plans; human resource issues; and an appendix.

3.1 Command and Control, and Unified Command

It is ***strongly recommended*** that a venue incident response plan involve coordination and communication with public safety and public health officials, as well as the local JTTF (Joint Terrorism Task Force) and fusion centers where possible. It is ***strongly recommended*** that decisions on the roles and authority of involved agencies and individuals be made during security planning sessions, and not during an incident.

The National Incident Management System (NIMS), especially the Incident Command System (ICS), is used as a tool to assist many venues in planning for managing incidents. A key component of the ICS system is the unified command structure. Unified command unites the incident commanders of entities involved in incident response. In the unified command framework, commanders of responding organizations make response decisions together according to ICS guidelines. Once these broad decisions have been made, the incident commanders retain control over the first responders that report to them and the responsibilities assigned to their units. At a venue, unified command is likely to include stadium security and management along with local law enforcement and fire services at a

minimum. It is ***strongly recommended*** that venues follow a model similar to the unified command model. However, individuals can be trained to take command and make decisions themselves in the event that communications within a unified incident command are cut off.

Of particular note regarding transferring from normal operations to incident management are instances where the decisions to do so are not entirely clear. This is most common with weather conditions, but it is also plausible with terrorist threats such as a suspicious bag or a bomb threat. It is therefore ***strongly recommended*** that communication with outside groups remain open even during normal operating procedures.

It is ***strongly recommended*** that a venue identify a centralized location as an operations center. It is ***strongly recommended*** that this command center be staffed by members of supporting and stakeholder agencies to efficiently communicate with security team members. The physical location and security of the command center is important to consider. It can be a security issue if the command center is compromised and this greatly inhibits the incident response capabilities of a venue. It is ***recommended*** that a venue consider how insulated their on-site security center is. If possible, it is ***recommended*** that the venue try to keep the public from accessing the location of the command center and other areas crucial to the implementation of the security plan and the response to any security incidents. A few metrics to measure the security of the command center itself are listed below.

If an event is especially large or identified as particularly at risk for a terrorist attack, it is ***recommended*** that a secondary, remote command center be set up. When doing so, a venue and participating stake-holders should be careful not to develop two parallel, but non-communicating command centers. A serious flaw in stadium security plans can be the lack of communication between the venue security command center and the law enforcement/outside agency command center.

To test how well a plan has been coordinated with outside agencies, tabletop exercises can be run with these agencies present. It has been noted that turnover in leadership and point of contact positions within these outside agencies can be relatively high. Thus, in order to

ensure good communication and understanding of role, it is ***recommended*** that venues consider how frequently they reiterate and review unified command structure and planning, and how often they run joint tabletop exercises. It is also ***recommended*** that a structure be in place to identify and brief newly appointed individuals on their role in incident command operations whenever turnover internally or in outside agencies does take place.

It is possible that lines of communication will not be available during an emergency. Assuring that this does not happen is a goal that is discussed later in the communication chapter. Even so, it is ***recommended*** that venues design contingency plans in case it does. A venue may estimate its performance during an emergency with the added complication of isolated communication structures via tabletop exercises in which groups of individuals are isolated from one another. In these exercises, as would happen in a real emergency, the groups must independently make decisions given the, most likely different, information they have available. Chapter 5 includes a more extensive discussion of tabletop exercises.

Time is of the essence in emergency situations. The speed with which decisions are made and then implemented is one important metric, although some decisions may be made hastily under pressure before sufficient information is available. It is ***recommended*** that a test of the strength of a unified command system, to be it through tabletop exercises or some other method, include measuring both the speed with which decisions are made as well as the validity of the decisions.

There are potential opportunities to collaborate with other sports venues or similar facilities. Equipment and personnel can be shared between venues in order to defray costs. Management can also tour nearby venues to learn from their procedures and to offer up advice to these venues on anything they see. It is ***suggested*** that venues contact nearby locations to determine if any such partnerships could be mutually beneficial. For smaller venues or smaller leagues, it is ***recommended*** that they seek out a larger, more established venue to observe their security procedures and develop a point of contact to consult with on security issues.

Questions	Metrics

Are tabletop exercises done in coordination with local law enforcement, public health and other relevant agencies? How many times per year are tabletop exercises done?	Y/N, Freq.
How many times per year are incident response plans reviewed with relevant outside agencies?	Freq.
Are measurements in place for both the speed and validity of the decision making process in a unified command situation?	Y/N
Are procedures in place to identify and brief new points of contact and leadership elements both internally and in outside agencies?	Y/N
Has the security of the command center been studied?	Y/N
How close to the command center are patron accessible areas?	#
Is there a secondary, remote command center for some events?	Y/N
How many individuals (employees) have access to the command center?	#
Have nearby venues been contacted to explore possible collaborative partnerships?	Y/N

3.2 Organizational Hierarchy

Clear job descriptions of event staff, including their role in the event of a security incident at the venue, can help ensure that employees correctly perform their duties. It is ***strongly recommended*** that venues develop job descriptions for every employee, and it is ***recommended*** that employees be given index cards or some other job aid to help remind them what their responsibilities are during an event and what is expected of them during an emergency situation. It is ***strongly recommended*** that, as part of the job descriptions, venues clarify who takes over certain roles if the individual originally in that position is not present or is incapacitated. This is often found as a component of a Continuity of Operations Plan (COOP) for a venue. In addition, mapping is an important component when setting up the venue since it speeds the ability to locate potentially suspicious items and it allows law enforcement to quickly identify whom to contact and where they are on site.

It is ***strongly recommended*** that a venue maintain a detailed staffing organization chart. Such a chart, updated frequently, can provide a way to keep track of job responsibilities and accountability as well as the chain of command. This point is even more important when a venue employs contracted security labor. In this case, it is ***strongly recommended*** that in-house security directors provide and communicate an organizational structure with contract labor management so response time efficiency is not eroded due to hierarchical confusion. For example, if there is an issue among the contract staff without an internal contract manager, often none of the staff will take individual responsibility. Staffing levels and supervisor to staff ratios can be good measures of how appropriately sized and organized the security staff for a venue is. Supervisors and team leaders might remain constant at each event since often the local law enforcement who donate their time will not necessarily be the same during each event.

It is ***strongly recommended*** that a venue consider ways that the resiliency of the chain of command can be strengthened. The resiliency of the chain of command might be measured by testing the effectiveness of security teams when some key members are not present. This might be done in coordination with tabletop exercises, where, at the start of the exercise, certain members of the team are removed, presumably due to being incapacitated during the incident being simulated in the exercise, but also due to the possibility that some staff, even at high levels, won't be on site on event-day for various reasons. A designated backup is always identified for each member of the chain of command.

Questions	Metrics
Does the venue have a Continuity of Operations Plan?	Y/N
Are security personnel removed from tabletop exercises to test the resiliency of the chain of command? Are they removed at random and without warning?	Y/N , Y/N
Are staffing levels tested for their projected performance during various conceivable scenarios such as severe weather?	Y/N
What is the Supervisor to Staff ratio?	:
Are employees provided a clear, concise job description?	Y/N
Are employees provided job aids to carry with them and remind them what to do in various circumstances?	Y/N

3.3 Staffing Plan

Planned staffing levels can benefit from accurate attendance and security incident projections. Other factors a venue might consider when staffing an event are the current national threat level, expected support from outside groups such as state law enforcement, and any specific security threats the venue has received. (These topics are considered in Chapter 2 on Risk Assessment.) How well a stadium can predict fan attendance and conduct can be easily and naturally quantified by measuring past predictions against actual fan attendance numbers and various markers for fan behavior, such as the number of ejections. Since specific security threats can be received with very little notice, an ability to add staff with little notice can be useful. It is ***strongly recommended*** that a venue assess its ability to predict fan attendance accurately, and its ability to quickly add staff to respond to changes in the risk profile of an event.

It is ***strongly recommended*** that a venue consider ways of increasing the flexibility of the front- line workforce. The flexibility of the workforce might be measured by how well the staff can, in theory, respond to a number of scenarios such as low staff turnout or severe weather that can increase the duties required of the security team. It is ***suggested*** that venues train staff for multiple roles in order to increase the flexibility of the workforce. For example, if patron screeners are also trained as ushers, then the venue can more quickly respond to issues that require more staffing in one of these two areas. It is ***strongly recommended*** that a venue assess the importance of various security functions and analyze the ability of staff to perform the functions considered critical even under the adverse conditions described previously. As part of this analysis it may be helpful to prioritize assignments for the same role. For example, if not all patron screeners show up, it would be helpful to know which gates are busiest, and be sure to fully staff those gates.

	Metric
Past predicted and actual attendance	Comparison
Past predicted number and actual number of security incidents	Comparison

Have the importance of various security priorities been ranked, and have priorities of crucial importance been identified? At what percentage level of front-line staffing can all functions of crucial importance be met?	Y/N, %

3.4 Human Resource Issues

3.4.1 Hiring and Employee Turnover

It can be difficult to find and hire qualified individuals willing to accept low-wage, part-time and/or seasonal work. If a stadium is understaffed due to this issue, then these problems could eventually be reflected through other metrics. For example, if there is not enough event staff trained to screen patrons, this might be reflected in long queue lines to enter the stadium. It is ***strongly recommended*** that venues monitor security employment levels in order to identify issues before a lack of employees begins to affect other metrics of performance.

Stadium security can also suffer due to high employee turnover. In general, at venues with proprietary staff, turnover rates are thought to be lower. Just like the inability to hire enough qualified individuals described above, problems related to high employee turnover might eventually be reflected in other metrics. But, just as above, a venue might determine how to monitor employee turnover rates in order to identify this problem as early as possible. It is ***strongly recommended*** that a venue track employee turnover rates, and address the issue if rates become so high that they adversely affect the ability of the venue to fully implement the security plan.

The issue of maintaining high quality job performance does not end with front-line or lower-level security employees. Security professionals – including managers and directors – often work multiple jobs due to the realities of today's economy. This reality can lead to performance fatigue that becomes compounded due to managers' decision-making responsibilities high atop the organizational chart. It is ***strongly recommended*** that a venue's human resources department institute language into the employment contract for annual or bi-annual performance interviews with top security managers or directors. These interviews can be used to update the current occupational situation of key personnel (e.g. "How many jobs are you currently working?"), and also to quiz these personnel on key organizational, procedural, and infrastructure-specific details that are significant to high-quality performance

in their current role.

It is ***strongly recommended*** that security clearly define which employees have the authority to grant credentials to employees, media and other groups, and that the credentialing process be written down and reviewed by security. It is ***strongly recommended*** that a database of credentials granted be maintained. It is ***recommended*** that entries in this database be randomly audited to ensure that credentials are being properly disseminated.

Questions	Metrics
What is the monthly/yearly employee turnover rate for various positions?	%
What are current staffing levels and estimated current staffing needs?	Comparison
Is it clear who has the authority to grant credentials?	Y/N
Is a database of credentials maintained?	Y/N
Are credentials randomly audited to ensure proper distribution?	Y/N

3.4.2 Insider Threat

Employees naturally have easier access to the venue, the players ,and the overall security plan than does the average event-day patron or other outsiders. Attacks by insiders may be more difficult to detect and deter and ultimately may be more likely to succeed compared to attacks by others. For this reason, it is ***strongly recommended*** that a venue consider how to limit the threat of an insider attack. For example, a venue could use background checks prior to employment combined with monitoring and occasionally updating background checks during employment. It is ***suggested*** that the updating of background checks be done at random as well as whenever there are indicators of a re-check (e.g. employees who show up driving expensive vehicles clearly outside their apparent economic means). Venue security can work with the human resources group to let employees and event staff knows that this process is in place and what can happen if a person fails the background check. As another way to limit the threat of an insider attack, it is ***strongly recommended*** that a venue limit the access of employees to only what is determined necessary for their specific job. Some metrics that could be used to gauge the threat of an insider attack are the number of employees with certain levels of access, such as access to computing systems, and the strength of the background check that they have been through.

Metrics can also be developed to assess how well internal monitors recognize unusual employee behavior. This second metric could be part of a red-team exercise or training game. For example, third party consultants could attempt to access certain areas or do something that would pose a threat if they had malicious intent, and they could be rewarded if they successfully do so without setting off employee monitors that are in place.

Former employees also pose a risk because of their possibly detailed knowledge of the security plan, as long as it remains unchanged since their employment, as well as their potential possession of ID badges and employee uniforms. One metric available to measure this threat is the repossession rate of such items. A second metric is the ability of an individual to gain access to the facility without proper credentials. This can be tested, via red-teaming, not just at initial employee entrances, but also at secondary checkpoints. Details about how to set up this red- teaming can be found in the appendix.

Questions	Metrics
What is the number of access levels?	#
Can a red-team access off-limit areas?	Y/N
What are the repossession rates of terminated employees' badges/keys/uniforms/etc.	%
Can a red-team access the venue, or pass through secondary screening, with outdated or terminated credentials?	Y/N
Are repeated background checks run on potential employees? If so, how often?	Y/N, Freq.

3.5 Staffing: Leadership, Organization and Authority: Key Points

- A key component of the ICS system is the unified command structure. Unified command unites the incident commanders of entities involved in incident response. Communications between partner agencies before and during an incident is important.
- The physical location and security of the command center is important to consider. For larger, higher profile events, a remote secondary command center might be used.
- Tabletop exercises can be used to assess the resiliency of the chain of command.

- Venues can collaborate with each other. Smaller venues especially can seek out larger venues for advice.
- A detailed staffing organization chart, updated frequently, is a way to keep track of job responsibilities and accountability as well as the chain of command.
- Planned staffing levels can benefit from accurate attendance and security incident projections. Other factors a venue might consider when staffing an event are the current national threat level, expected support from outside groups such as state law enforcement, and any specific security threats the venue has received.
- The flexibility of the workforce might be measured by how well the staff can, in theory, respond to a number of scenarios, based on the jobs they are prepared for. Venues can train individuals for multiple roles in order to increase the flexibility of the workforce.
- The ability to add staff with little notice is required to respond quickly to changes in the risk profile of an event.
- Monitoring employee workforce levels and employee turnover rates can prove useful.
- Attacks by insiders may be more difficult to detect and deter and ultimately may be more likely to succeed compared to attacks by others.
- The use of background checks prior to employment combined with monitoring and occasional updating of background checks during employment is an important security measure.
- Security measures can be designed to prevent staff (or former staff) from entering areas for which they are denied access.

3.6 Recommendations – Chapter 3 Staffing: Leadership, Organization and Authority

Chapter 3 – Staffing: Leadership, Organization and Authority	
Strongly Recommended	Section
A venue's incident response plan involve coordination and communication with public safety and public health officials, as well as the local JTTF (Joint Terrorism Task Force) and fusion centers where possible.	3.1

Decisions on the roles and authority of involved agencies and individuals to be made during security planning sessions and not during an incident.	3.1
Venues follow a model [for managing incidents] similar to the Incident Command Structure unified command model.	3.1
Communication with outside groups remains open even during normal operating procedures.	3.1
Venues identify a centralized location as an operations center.	3.1
The venue's command center to be staffed by members of supporting and stakeholder agencies to efficiently communicate with security team members.	3.1
Venues develop job descriptions for every employee.	3.2
As part of the job descriptions, venues clarify who takes over certain roles if the individual originally in that position is not present or is incapacitated.	3.2
Venues maintain a detailed staffing organization chart.	3.2
In-house security directors provide and communicate an organizational structure with contract labor management so response time efficiency is not eroded due to hierarchical confusion.	3.2
Venues consider ways that the resiliency of the chain of command can be strengthened.	3.2
Venues assess its ability to predict fan attendance accurately, and its ability to quickly add staff to respond to changes in the risk profile of an event.	3.3
Venues consider ways of increasing the flexibility of the front-line workforce [to respond to severe weather, low staff turnout, etc.].	3.3

Venues assess the importance of various security functions and analyze the ability of staff to perform the functions considered critical even under adverse conditions.	3.3
Venues monitor security employment levels in order to identify issues before a lack of employees begins to affect other metrics of performance.	3.4.1
A venue track employee turnover rates, and address the issue if rates become so high that they adversely affect the ability of the venue to fully implement the security plan.	3.4.1
A venue's human resources department institute language into the employment contract for annual or bi-annual performance interviews with top security managers or directors.	3.4.1
Security clearly defines which employees have the authority to grant credentials to employees, media and other groups, and that the credentialing process be written down and reviewed by security.	3.4.1
A database of credentials granted to be maintained.	3.4.1
Venues consider how to limit the threat of an insider attack.	3.4.2
Venues limit the access of employees to only what is determined necessary for their specific job.	3.4.2

Recommended	
Venues consider how insulated their on-site security center is.	3.1
Venues try to keep the public from accessing the location of the command center and other areas crucial to the implementation of the security plan and the response to any security incidents.	3.1
A secondary, remote command center be set up, if an event is especially large or identified as particularly at risk for a terrorist attack.	3.1
Venues consider how frequently they reiterate and review unified command structure and planning, and how often they run joint tabletop exercises.	3.1
A structure to be in place to identify and brief newly appointed individuals on their role in incident command operations whenever turnover internally or in outside agencies does take place.	3.1
Venues design contingency plans in case lines of communication are not available during an emergency.	3.1
A test of the strength of the unified command system, to be it through a tabletop exercise or some other method, include measuring both the speed with which decisions are made as well as the validity of the decisions.	3.1
Smaller venues and smaller leagues seek out a larger, more established venue to observe their security procedures and develop a point of contact to consult with on security issues.	3.1
Employees be given index cards or some other job aid to help remind them what their responsibilities are during an event and what is expected of them during an emergency situation.	3.2

Entries in the credentials granted database be randomly audited to ensure that credentials are being properly distributed.	3.4.1
Suggested	
Venues contact nearby locations to determine if any [collaborative] partnerships could be mutually beneficial.	3.1
Venues train staff for multiple roles in order to increase the flexibility of the workforce.	3.3
The updating of background checks to be done at random as well as whenever there are indicators of a re-check (e.g. employees who show up driving expensive vehicles clearly outside their apparent economic means).	3.4.2

Appendix – Chapter 3

This chapter appendix provides specific ideas to potentially incorporate into a sports venue's testing of its security procedures. The examples given are purely illustrative, and by no means intended to be comprehensive.

Tabletop Exercises

- To simulate the possibility that individuals crucial to the security plan might not be present during a security incident, one might remove certain individuals at the beginning of the tabletop exercise at random. There are many ways to achieve randomness. For example, it can be done by drawing cards from a deck and removing anyone who drew certain types of cards.
- Separate groups of individuals during a tabletop exercise in order to simulate the possibility that lines of communication between isolated groups might not be open.
- Quiz public safety, public health, other outside agencies and internal security management about the chain of command during certain venue events or security incidents. Compare answers to make sure that all groups are on the same page.

Flexibility of workforce:

- Train front-line employees for multiple tasks. Change assignment of workers at the last minute and monitor how well they perform. Reward workers for good

performance.

Insider Threat/Red-teaming

- Give individuals expired employee credentials, and have them attempt to access the venue.
- If possible, use actual employees in the above drill. These employees can attempt to use their personal relationship with other employees to their advantage when trying to enter an area they don't have access to.
- Cash rewards can be used to properly incentivize such an employee to truly attempt to access an area in a red-teaming drill.
- Clearly marked employee credentials and uniforms can assist in assuring employees will be unsuccessful when attempting to enter areas for which they are not permitted access. For example, large color-coded badges make it easy to determine whether an employee is allowed access to an area, and to spot an employee who is currently located in a place they shouldn't be.
- Electronic access controls assist the human element of security in maintaining the integrity of a secure zone. Command centers can be set up with alarms that can alert staff upon attempted inappropriate access. Electronic access can be cut off immediately for terminated employees.
- Secondary and not just initial screening areas might be tested. For example, it could be tested how often an employee with proper general employee credentials but not credentials for a specific part of the stadium, such as an electric room, can gain access to this room.

Span of Control

Under the Incident Command System proposed by FEMA, the staff to supervisor ratio is typically between 3:1 and 7:1, with a 5:1 ratio recommended as ideal. Normal event-day supervisor to staff ratios at major venues often exceed 10:1, so the structure developed to manage active incidents will typically involve more supervision than normal operations.

Chain of Command

The following are examples of Chain of Command stakeholder consideration:

First Example:

The President and CEO of the stadium would make a decision after consulting with key members of his staff and external stakeholders including:

a. Guest Services Director

b. Safety/Security director

c. Law Enforcement representatives

d. County Office of Emergency Management Coordinator

e. Other representatives of law enforcement present (i.e. FBI)

Second Example:

The Security Director of the Stadium might make a decision to brief front-line staff involved in patron screening to be on the lookout for a new type of weapon after receiving warnings from the local JTTF and law enforcement, and reviewing the potential threat this weapon poses as part of a risk assessment update.

Incident Command

Effective leadership models are those that mirror incident management. On the morning of the event, there can be a crisis response team meeting where the unified command comes together and primarily discusses two things:

1) What has changed?

2) What do we do if that "bad thing" does happen (e.g. weather, suspicious package, etc.)?

In a sophisticated attack, it is possible that the incident command structure (personnel, equipment, and command center) could be targeted as part of the attack. In a risk assessment, the threat to this structure from various attacks can be addressed.

Similarly, the vulnerability of incident response systems to outsider influence can be tracked. For example, it would be damaging if an evacuation order was broadcast throughout a venue by accident or by malicious intent, when there is no need for evacuation.

Chapter 4 – Information Management

Introduction

Information management is a significant component of sports venue security because it encompasses systems for communications between venue personnel and systems for delivering

information to first responders, law enforcement agencies and the public during an emergency. Beginning from a macro perspective of communication structures – internal stakeholders, external stakeholders, and the public/patron stakeholder – this chapter provides recommendations for information management with a heavy focus on specific communication technologies. Cyber-security issues, a related topic, are also covered in this chapter.

4.1 Communication Structures – The Three "Buckets"

Understanding vulnerabilities within your information management system requires you to understand it as a set of interlocking structures comprised of internal stakeholder communication systems, external stakeholder communication systems, and public/patron communication systems. Cyber-security can have an impact on all three communication "buckets," so it is important to assessing information management risks. Here is an example of how these communication structures work together for effective information management. These communication systems play an important role in crowd management (internal and patron stakeholders) and emergency response (external stakeholders). A terrorist seeking to cause harm may choose to exploit vulnerabilities in any one of these systems in order to increase the consequences of an attack. First responders may be prevented from delivering help (external stakeholders), crowd notification of an evacuation may be impeded (patron stakeholders), and communication among managing agents may be disrupted (internal stakeholders). Computer systems and electronic files pose a significant vulnerability because these systems are accessible remotely through cyberspace. Information contained on computer systems can be used to obtain building plans, to assist in gaining entry into venue access points via employee identification credentials, to exploit contract vendors and deliveries, and to shut down or hijack public address systems, electronic message boards, and text messaging systems, social media, and websites.

Establishing communication protocols for internal, external, and public/patron	Metric
Is there a protocol for internal communication?	Y/N
External communication?	Y/N
Public communication?	Y/N

Open Ended Questions	Anticipated Response
Identify the protocol for internal communication, external communication, and public communication.	Descriptions of communication protocols
List the entity-pairs that have a communication link identified in each protocol.	List of sender/receiver pairs

This chapter translates the macro-perspective of communication buckets and their associated stakeholders by breaking down information management into four subject areas: internal stakeholder communication (i.e. venue security to venue security), external stakeholder communication (i.e. venue security to local municipal services and vice versa), public/patron stakeholder communication (i.e. venue to patrons and vice versa), and cyber-security, (i.e. the venue's digital footprint). For specific examples related to this topic, please see the appendix for chapter 5.

4.1.1 Internal Stakeholder Communications

Internal communication includes any mode of communication inside the venue shared among venue personnel. Internal communication includes radios used by venue staff (if any) and venue management (if different), written communication (incident reports and other documents), emergency call pagers, and traditional landlines and cellular phone networks.

4.1.1.1 Radios

It is ***strongly recommended*** that an internal communications structure and protocol be established as part of a sports venue security plan regardless of size or event type. A basic security structure often deploys multi-channel radios to management and supervisory security staff only, due to the high cost of the equipment.

Security personnel at outdoor venues and frontline security staff closest to large crowds may require unique earpieces and microphones to help ensure the clarity of communication in these noisy environments. If radios are in use by management at the venue it is ***strongly recommended*** that radio communications be monitored at the command center. If radios are in use at the venue it is ***recommended*** that a system of channel assignment be employed, so as not to crowd any single channel with excessive traffic. Multi-tiered venues could consider issuing unique radio channels per tier or security level, with emergency communications reserved for separate

channels. Deployed radios must be maintained properly. It is ***recommended*** that radios be checked before being needed for events. Radio batteries can be tested and replaced regularly with backup batteries readily available. It is ***recommended*** that first responders including law enforcement test the capabilities of their radio systems within all areas of the venue at least annually to ensure their operability. Venues also may consider including the use of law enforcement radios so as to establish a channel for direct law enforcement contact. It is ***suggested*** that the venue operators consider the use of multi-channel radios for internal communication for ALL staff. It is ***suggested*** that venue security personnel be trained to properly utilize their communication technology, e.g. they may use coded messages about emergencies so as not to instill panic in patrons, which may help speed reaction time during times of emergency.

Questions	Metric
Are radios utilized for communication among venue staff?	Y/N
What percentage of employees is provided radios?	%
Do channels include a direct law enforcement channel?	Y/N
Are coded messages used for radio communications?	Y/N
How often are radios tested?	Freq.
Is a backup supply of radio batteries readily available?	Y/N

Open Ended Questions	Anticipated Response
Identify the type of radios used at the venue.	List of radio types
Describe the channel assignment structure.	Channel assignment list
Identify which staff positions have radios and explain the reasoning. A hierarchical chart or diagram may be used.	Identity of staff having radios along with rationale for assignment
List the message codes used for radio communications.	List of codes

4.1.1.2 Written Communication

Protocols for sharing and archiving written communication are an integral component of a venue's security plan for both communication and quality assurance (see chapter 6). It is ***strongly recommended*** that venues use a computer database to record features of incidents or

communications that can then be used for later analysis. A venue might consider the use of a paper-based form of written communication. Whether electronic or paper-based, it is ***recommended*** that protocols include incident reporting following any type of disturbance at the venue, such as public intoxication, physical altercation, underage alcohol consumption, drug use, and illegal ticket sales. This is not per se an anti-terrorism plan, but it is a way of exercising incident reporting and gives rise to corresponding metrics that might be useful in assessing an anti-terrorism plan. It is ***recommended*** that written communication, either paper or electronic, be used as a channel from staff to management regarding areas that require improvement or signal a need for attention. It is ***suggested*** that venues consider whether electronic or paper-based communication should be utilized to apprise security staff of known threats prior to an event. Additionally, an organizational chart for employee reporting and supervisor-staff communications may provide a useful tool for managing communication flow and maintaining accountability.

Questions	Metric
Are protocols in place for internal written communication?	Y/N
Are databases created based on written reports?	Y/N
Is there an organizational chart that details the flow of communication among security staff?	Y/N

Open Ended Questions	Anticipated Response
Describe the protocol in place for internal written communication.	Protocol description
Identify the types of reports that are kept.	List of report types
Identify data that is recorded in a database for analysis.	Description of database
Provide the organizational chart that details the flow of communication among staff.	Organization and process chart

4.1.1.3 Emergency Call Pagers

It is ***suggested*** that venues consider the use of an emergency paging system. This type of

system includes a device that allows an emergency notice to be placed to the command center at the press of a button. The call indicates the location of the signal so that help can be dispatched.

This system is less costly than distributing radios to all personnel. With the use of emergency pagers even non-supervisory staff can help ensure that emergency situations are attended to in an expedient manner.

Questions	Metric
What percentage of employees has emergency call pagers?	%
On average, how many pagers per patron population are in use?	:

4.1.1.4 Telephones

Telephone lines are an important mode of communication within the venue. Traditional landlines may be utilized for communication with the command center and other key vantage points inside the venue. Alternatively, landline telephones may be installed at concessions and guest services booths for emergency use only. It is ***recommended*** that if an emergency telephone reporting system is in place that it be coupled with a system of identification that indicates the precise location of the phone from which the call is placed. This helps to minimize location reporting error and ensure that in the case of an emergency assistance is dispatched to the proper location. It is ***recommended*** that a wired telephone independent of the facility's system be installed in the command center in case the system is compromised.

Cellular telephones may also be used as a primary source of contact among management within the venue. Smart phones provide additional modes of communication through the handset, allowing venue security managers to receive instant notifications via text messages and email. Satellite phones may be used for backup if commercial cellular service is unavailable. Cellular communications can encounter problems with volume overload on the network during times of increased use in a concentrated area such as a sports venue. Several measures can be taken to resolve the issue of overload on cellular networks. These include the use of Cellsites-on-Wheels (COWs) and the use of a Distributed Antenna System (DAS). These solutions can be costly and may additionally require a large physical space to accommodate the equipment. A call load

triggered access class agreement with cellular providers in the immediate region of the venue would assure that in an emergency, venue personnel will receive priority in cellular call routing and message notification. If the cellular call volume at the venue causes network overloads, it is ***suggested*** that the venue investigate the available technical solutions to resolve the problem.

The remarks about testing and maintaining radios apply to other communication devices as well. Specifically the reception of cellular phones, smart phones, and satellite phones can be tested at various locations in the venue, and their batteries checked and kept charged.

Questions	Metric
Are emergency telephones in place throughout the venue?	Y/N
If yes, what is the number of patrons per emergency phone?	:
Do the command center and other key locations have a dedicated phone line?	Y/N
Is an additional system in place for cellular network overload?	Y/N
How many calls/texts per minute from the venue is the system projected to handle? What percent larger than the average number of calls/text per minute in the venue is this number?	#, %
Is there a call load triggered access agreement with local cellular providers in place for emergencies?	Y/N
Has the reception of cellular phones and smart phones been tested at various locations in the venue?	Y/N
Is there a process in place that cellular phone and smart phone batteries are tested regularly with backups available?	Y/N

Open Ended Questions	Anticipated Response
Identify the locations of emergency call phones located in the venue. A map may be included with the descriptions.	Locations of emergency phones
Indicate which locations have a dedicated phone line.	Locations of dedicated phones
Describe the system(s) in place for cellular network overload.	Description of system(s)
Detail the agreement in place with local cellular providers for emergencies.	Description of agreement

4.1.2 External Stakeholder Communications

External communications includes communication between venue operations and security management and those staff from outside entities such as local and federal law enforcement agencies, emergency medical, fire, and rescue personnel. External communication between the venue and outside entities such as local utility providers, as well as contacts at adjacent critical infrastructure such as airports, rail lines, ports, oil terminals (tank farms), and utility stations, are also included in this section.

4.1.2.1 Local and Federal Law Enforcement

Communication with local and federal law enforcement officers may occur through various modes including telephone communication, automatic messaging through email notification services, and via personal contact with agents posted at the venue. It is ***strongly recommended*** that venues arrange a direct line of contact to the local law enforcement within the command center. It is ***strongly recommended*** that the Security Director of the venue subscribe to a notification list in order to receive incident and threat notifications from the local fusion center, the Joint Terrorist Task Force (JTTF) or other federal alert systems. If the venue is large and the event has a high profile, it is ***recommended*** that the venue include a law enforcement presence in the command center from federal authorities as well as local law enforcement. It is ***recommended*** that venues employ a paid law enforcement detail during event day operations. It is ***suggested*** that if law enforcement radios are in use at the venue, a law enforcement frequency channel that allows direct communication with local law enforcement be considered. It is recommended that law enforcement officials test the capabilities of their radio systems within all areas of the venue at least annually to ensure their operability.

Questions	Metric
Are there direct modes of communication with local law enforcement authorities?	Y/N
Are there direct modes of communication with federal law enforcement authorities?	Y/N
Does Security Management receive automatic threat alerts from a federal agency?	Y/N
Is there a representative from local and/or federal law enforcement present on-site during an event?	Y/N

Is there paid law enforcement detail at the venue during an event?	Y/N
How many law enforcement officers are on detail during en event?	#

Open Ended Questions	Anticipated Response
Indicate which direct modes of communication with local law enforcement authorities are used.	Modes of communication used with local law enforcement
Indicate which direct modes of communication with federal law enforcement authorities are used.	Modes of communication with federal law enforcement
Indicate from which federal agency Security Management receives automatic threat alerts.	Federal agencies sending automated alert threats to Security Management
Indicate which type of representative from local and/or federal law enforcement is present on-site during an event.	Representatives on site

4.1.2.2 Emergency Medical, Fire and Rescue Personnel

Communication with first responders such as emergency medical, fire and rescue personnel is vital in an emergency. It is ***strongly recommended*** that a direct line of contact be established with the local fire department as well as with the local medical center or hospital through telephone lines, personal contacts, emergency radios or several of the above. It is ***strongly recommended*** that a venue have emergency medical personnel on staff during an event. It is ***strongly recommended*** that a venue reserve one or more rooms as a medical center. Venue medical rooms may be designed for larger capacity if venue patron capacity is especially high. Extremely large venues may have a complete, separate medical facility on site, possibly managed in cooperation with the local hospital. Communication with on-site medical facilities may be carried out in person, or through the use of staff radios or mobile phones. It is ***recommended*** that an EMS representative as well as a representative from the local fire department be stationed inside the command center during events.

Questions	Metric
Are there direct modes of communication with emergency medical services?	Y/N
Are there direct modes of communication with the local fire department?	Y/N
Is there a medical treatment center on site?	Y/N
Is there a representative from EMS and/or fire and rescue present on-site during an event?	Y/N

Open Ended Questions	Anticipated Response
Indicate which direct modes of communication with emergency medical services are used.	Modes of communication with EMS
Indicate which direct modes of communication with the local fire department are used.	Modes of communication with fire department
Indicate the primary modes of communication with the medical treatment center during an emergency.	Modes of communication with emergency medical center
Indicate which representative from EMS and/or fire and rescue is present on-site during an event.	Names of on-site representatives

4.1.2.2 Critical Infrastructure

Some venues may be located adjacent to or nearby critical infrastructure such as airports, rail lines, ports, oil terminals (tank farms), or utility stations. Each of these critical infrastructure sites poses an additional vulnerability to the venue through threats to the infrastructure site. Threats from such sites include the large-scale storage of combustible materials (airports, tank farms, ports) or the potential for alternate access to the venue (airports, rail lines, utility stations); there is also the threat of access from the venue into the adjacent vulnerable infrastructure site. For these reasons it is ***strongly recommended*** that venues establish a channel of communication with these sites. It is ***strongly recommended*** that contact be established with the local utility companies providing utility services to the venue. It is ***recommended*** that venue representatives establish a point of contact at a critical infrastructure site with a person holding the authority to make necessary operational decisions in an emergency. It is ***recommended*** that venues

periodically verify the point of contact and update the contact information if necessary. At least annual or semi-annual verification is ***suggested.***

Questions	Metric
Have critical infrastructure sites nearby the facility been identified?	Y/N
Has a channel of communication been established with each of the sites identified?	Y/N
Is there a direct mode of contact with the utility providers for the venue?	Y/N
Does the point of contact at each site have the authority to make operational decisions during an emergency?	Y/N
How often is the point of contact information verified?	Freq.
Are test messages sent to these points of contact? What percentage of the time are these messages successfully relayed/received?	Y/N, %

Open Ended Questions	Anticipated Response
Indicate which critical infrastructure sites are adjacent to the venue and the proximal distance of each.	List of sites and distances
Indicate which modes of communication with the critical infrastructure sites are used.	Communication modes used
Indicate with which utility provider(s) to the venue contact has been established and the mode of contact.	Utility providers and contact modes
Indicate the title of the point of contact for each critical infrastructure site.	Points of contact with titles

4.1.3 Patron/Public Stakeholder Communications

Communication starts before the public arrives at the venue through the use of text messages, social media, and websites providing information prior to an event. As patrons arrive, communication begins before patrons enter the facility through effective use of the public address system and clear, highly visible signage. Once patrons are inside the facility, venue

staff, the public address system, electronic message boards and television monitors work in coordination to enhance patrons' experience and, if needed, to direct patrons during emergency or evacuation procedures.

4.1.3.1 Public Address System

It is ***strongly recommended*** that a venue have the use of an audio public address system in order to communicate with the patrons at the facility during a public event. An audio public address system is designed to relay spoken messages using a loudspeaker system installed throughout the venue. It is ***strongly recommended*** that emergency messages include specific evacuation instructions, shelter in place instructions, incident notification and incident status updates (for example in the case of a blackout), and any other necessary information. It is ***strongly recommended*** that these messages be prepared in advance of an emergency and ready for use. It is ***strongly recommended*** that each specific message be recorded in advance so that is may be played remotely if the public address announcer has to evacuate. There are some emergency situations, such as the case of an active shooter incident or a toxic plume, when messages with the precise steps patrons should take will require composition at the time of the emergency. It is ***recommended*** that the Director of Security or the Director's designee take responsibility for composing the content of the message during such an emergency. Non-emergency messages may include event-related information, as well as precautionary public safety information such as brief instructions for an evacuation in case an emergency occurs. It is strongly recommended that the public address system be connected to the emergency generator, UPS, or other power source so that it can continue to operate if electrical service is interrupted.

Questions	Metric
Is a public address system utilized for communication with patrons?	Y/N
How many pre-scripted messages are prepared for emergency situations? How many languages are used for these messages?	#,#
Is there a procedure in place to compose an emergency message that is not pre-scripted?	Y/N

Open Ended Questions	Anticipated Response
Identify the types of messages prepared for public announcements, including emergency & non-emergency messages; event related and precautionary messages.	Message types
Identify which staff position is responsible for message composition.	Staff assigned to compose messages

4.1.3.2 Electronic Message Boards

Electronic messaging boards may be used at a venue. These boards may be composed of LEDs and may be located at various locations throughout the venue or as a ribbon of contiguous screens encircling the patron seating area so that messages are visible from all angles. Before, during, and after events, advertisement and entertainment messages may be displayed on the boards. If electronic message boards are in use at the venue it is ***strongly recommended*** that during an evacuation or other emergencies, the electronic message boards may be used to display evacuation instructions and guidance. It is ***strongly recommended*** that basic messages addressing a variety of potential emergency situations be prepared in advance so that they may be activated in case the area where the messages are controlled has to be evacuated.

If electronic message boards are in use it is ***recommended*** that the system to be utilized during non- emergency situations to regularly test its functionality. The electronic message boards may also provide useful information for patrons, such as contact telephone numbers for incident reporting. When a text messaging system is available, the contact telephone numbers for messages encouraging fans to support team-sponsored events, and for questions and incident reporting can be displayed on the message boards and used by patrons. The volume of response to posted contact numbers on the message boards may be considered an indicator of patron attention to the messages. The message control system and some number of electronic message boards can be connected to the emergency generator, UPS, or other power source so that they can continue to operate if electrical service is interrupted.

Questions	Metric
Are message boards used for relaying messages to patrons?	Y/N
Is the system utilized during non-emergency situations, such as entertainment?	Y/N

If a text messaging system is available is the phone number displayed on message boards?	Y/N
If a text messaging number is displayed on message boards, what is the quantity of text messages received?	#
Has the quantity of received messages increased over time and, if so, by what percentage?	Y/N, %

4.1.3.3 Television Monitors

Television monitors provide a wider range for the type of message that can be sent. Such monitors may also provide access to media coverage and video display. Both media coverage and video display may be helpful in an emergency situation because of the amount of information that can be relayed through the medium and because of the level of familiarity that has been established with the medium. Television monitors may also be utilized for non-emergency, entertainment purposes. If television monitors are in use at a venue it is ***strongly recommended*** that the visual quality and the size of the monitors be sufficient and that they are effectively and strategically placed at appropriate locations. If television monitors are in use at a venue it is ***recommended*** that the system be utilized during non-emergency situations to regularly test its functionality.

Questions	Metric
Are television monitors used for relaying messages to patrons?	Y/N
Are television monitors used for providing patron access to media coverage?	Y/N
Are television monitors used for non-emergency purposes?	Y/N
Are television monitors able to provide video messages to patrons during an emergency?	Y/N
How many pre-scripted video messages are prepared?	#

4.1.3.4 Posted Signage

Posted signage may contain information on expectations of patron behavior. It is ***strongly recommended*** that venues employ the use of temporary or permanent signage to assist in crowd management in and around the venue. It is ***recommended*** that permanent signage provide

emergency contact information, incident or suspicious item reporting telephone numbers, evacuation routes and exits, and the location of emergency equipment. It is ***recommended*** that posted signage be used at the entrances for queuing and patron screening procedures, e.g. to identify objects that are restricted or prohibited from the venue. It is ***suggested*** that pictorial depictions be used on signs to help patrons, including those with limited proficiency in English, understand and remember what items are permissible. Quick and easy comprehension and memory retention across events will help to accelerate the speed of the screening process and thereby help to reduce a potential terrorist target. Some considerations for effective signage use may include size, design, and placement of the signs. In addition, removing temporary signs and observing crowd movement may yield an indication of the effectiveness of the signage.

Questions	Metric
Is information communicated through permanent signs at the venue?	Y/N
Are temporary signs used to communicate information?	Y/N
If signs are removed, what is the slow-down in corresponding behavior (e.g. moving to a different gate to enter)?	#

Open Ended Questions	Anticipated Response
Indicate which information is permanently displayed and the quantity & locations of the signs.	Signage locations and displayed information
Indicate which information is temporarily displayed and the quantity & locations of the signs.	Signage locations and displayed information
If temporary signs have been removed during events, describe the crowd behavior with and without the presence of the signs.	Descriptions of crowd behavior

4.1.3.5 Text Messaging

Text messaging systems provide a simple and convenient mode of communication for venues and patrons. It is ***recommended*** that venues consider establishing a text messaging system that provides patrons with a number to which they can text a complaint or report of a disturbance. These messages can be received in the command center and attended to immediately. An

advantage of such a system is that it gives guests the opportunity to report about a nearby patron without the knowledge of that individual. This helps ensure that the incident does not escalate due to interpersonal aggression. It is ***recommended*** that if guest text messaging is in use at the venue, a database of reported incidents be maintained for analysis. The guest text messaging system is also used during non-emergencies for patron entertainment. If a text messaging system is in use at the venue it is ***suggested*** that this system be considered for the dissemination of information to patrons during an emergency. Venues may wish to establish an emergency message distribution list by providing patrons with an opportunity to add their mobile number to the list. The system may also provide a choice for patrons who wish to receive either emergency notification only, or both emergency and non-emergency notifications. With a sufficient number of non-emergency participants the system may be utilized for crowd management at entrance queues and during intermission and exit crowding.

Questions	Metric
Is a text messaging system available to patrons for communication with security services?	Y/N
Are incidents reported through the texting system retained in a database?	Y/N
If so, how many incidents per event are reported? What is the response time for attending to incidents?	#, Time
Has an emergency message distribution list been established? What is the increase in the number of people listed there compared to last year?	Y/N ,#
Is the system utilized during non-emergency situations? How often?	Y/N
How often are test messages sent to patrons?	Freq.

4.1.3.6 Social Media Feeds

Social media may also provide a mode of communication with the public. It is ***recommended*** that venues consider having an online presence through social platforms such as Twitter, Facebook or Instagram. These platforms provide the opportunity for the venue to accrue "followers" or "fans" on the site and establish an ongoing relationship with the followers/fans who are likely to be patrons of the venue. They also provide a medium for the dissemination of

information and can establish a communication network of trust between the venue and their patrons. If social media is in use it is ***recommended*** that the venue engage patrons in discussions prior to events, answer questions and concerns, as well as provide event day relevant information and updates. For example, a venue may post important announcements, pictures, or informative videos on their Facebook page. It can also post incentives for getting patrons into the stadium faster, which would help with vulnerability due to long inspection queues.

Monitoring social media feeds can provide the venue with various insights such as patron satisfaction and fan experience, but may also prove useful as an investigative or security risk tool for the venue. Crowd sourcing through social media provides a method to obtain situational information and awareness that otherwise might not be easily available. Specifically, software packages such as Bright Planet, Vigilance and others allow the venues to build risk-based dashboards where security staff can monitor, in real-time, Twitter, Facebook, Instagram and other social media platforms in an attempt to identify inappropriate, if not illegal, behavior. These tools are very effective and, for the most part, are not prohibitive in cost. If a venue uses social media it is ***recommended*** that protocols be developed for ingesting, evaluating, and acting upon reports of various kinds (e.g. "See something, say something"). Actions might include dispatching security staff to the location of interest, training a camera on the location, etc.

Questions	Metric
Are social media used for relaying messages to patrons?	Y/N
For each platform used, how many followers does the venue have? How much has the number of followers increased since last year?	#, #
For each platform used, how frequently are updates made?	Freq.

4.2 Cyber-Security

As cyber-attacks are a growing concern, it is important to ensure the security of the computer-based systems within the venue. This includes protecting digital information and computer systems and ensuring that employee personal information, patron personal information, ownership and management emails and personal information, incident filing systems, etc. are

stored in a secure, protected environment to prevent access by unauthorized users. Cyber-security will also protect against the possibility of terrorists using personal information to blackmail employees into assisting an attack.

4.2.1 Cyber-security Plan and System Maintenance

Cyber-attacks cause damage by injecting viruses, worms, or eavesdropping programs into the computer system. These attacks are often used to obtain private or sensitive information, gain access through false authentication, cause interruptions in operations possibly by destroying or overloading the network, disrupting electrical systems, etc. It is essential and therefore ***strongly recommended*** to protect and monitor computer systems and network infrastructure to be prepared against such threats.

It is ***strongly recommended*** to regularly test computer systems and to perform security reassessments to help identify any potential vulnerabilities as well as assist in detecting any patterns of probing, hacking, or intrusions.

It is ***recommended*** that venues build a plan to mitigate cyber-security risks. The plan can include establishing policies, identifying personnel, and utilizing technologies to prevent and deter attacks, as well as monitor and manage the system. The plan also might consider issues such as possible system malfunctions, system overload, and interdependencies with external systems. Information and data confidentiality and safety is also essential. Policies will determine who has authorized access and how it may be obtained.

It is ***recommended*** that cyber-security technologies be used to ensure that system processes are functioning properly, data is not compromised, and information can be accessed when needed. These technologies include firewalls, content management tools (e.g. spam filters), authentication methods (e.g. passwords and access tokens), antivirus software, cryptography controls, data encryption, digital signatures and certificates. Network intrusion detection technologies may be used to monitor and detect possible abnormal behavior or malicious activity on the computer systems.

To ensure continuity, secure backup and system recovery tools can be used to maintain operations during a disruption or power outage, or restore and recover from a cyber-attack.

Questions	Metric
Is there a security plan for computer and information systems hardware and software? How often is the plan revisited?	Y/N, Freq.
Is there any cyber-security software or protective measures implemented?	Y/N
Is there a process for testing and evaluating computer security measures?	Y/N
Have penetration tests been performed? How often are such tests performed?	Y/N, #

Open Ended Questions	Anticipated Response
Describe the security plan.	Plan description
Identify cyber-security software and technologies being used	List of cyber-security software and other technologies
Describe the testing evaluation procedures used.	Testing procedures

4.3 Information Management: Key Points

- Communication systems play an important role in crowd management and emergency response.
- Establishing communication protocols for internal, external, and public communication helps ensure clear and effective communication during emergencies.
- An organizational chart for employee reporting and supervisor-staff communications is a useful tool for managing communication flow and maintaining accountability.
- An emergency paging system includes a device that allows an emergency notice to be placed to the command center at the press of a button.
- Traditional landlines, cellular telephones and smartphones may be utilized for communication with the command center and other key vantage points inside the venue as well as a primary source of contact among management within the venue.
- Several measures can be taken to resolve the issue of volume overload on the cellular network during times of increased use.
- Communication with local and federal law enforcement officers, emergency medical,

fire, and rescue personnel can use telephones, alerts and emails, and personal contact with agents posted at the venue.

- Nearby critical infrastructure such as airports, rail lines, ports, oil terminals (tank farms), or utility stations pose an additional vulnerability to the venue through threats to the infrastructure site.

- Communication between the venue and the patrons is essential in both emergencies and normal events. Communication channels include public address systems, electronic visual displays such as electronic message boards and television monitors, and temporary or permanent signage around the venue, and have also grown to include text messaging and social media.

- Signs to help patrons understand and remember what items may be carried into a venue will help to accelerate the speed of the screening process and thereby help to reduce a potential terrorist target.

4.4 Recommendations – Chapter 4 Information Management

Chapter 4 – Information Management	
Strongly Recommended	Section
An internal communications structure and protocol be established as part of a sports venue security plan regardless of size or event type.	4.1.1.1
Radio communications be monitored at the command center.	4.1.1.1
Venues use a computer database to record features of incidents or communications that can then be used for later analysis.	4.1.1.2
Venues arrange a direct line of contact to local law enforcement within the command center.	4.1.2.1
The Security Director of the venue subscribe to a notification list in order to receive incident and threat notifications from the local fusion center, the Joint Terrorist Task Force (JTTF) or other federal alert systems.	4.1.2.1

A direct line of contact be established with the local fire department as well as with the local medical center or hospital through telephone lines, personal contacts, emergency radios or several of the above.	4.1.2.2
Venues have emergency medical personnel on staff during an event.	4.1.2.2
Venues consider reserving one or more rooms as a medical center.	4.1.2.2
Venues establish a channel of communication with nearby critical infrastructure sites.	4.1.2.3
Venues establish contact with the local utility companies providing utility services to the venues.	4.1.2.3
Venues have the use of an audio public address system in order to communicate with the patrons at the facility during a public event.	4.1.3.1
Emergency messages include specific evacuation instructions, shelter in place instructions, incident notification and incident status updates (for example in the case of a blackout), and any other necessary information.	4.1.3.1
Public address messages to be prepared in advance of an emergency and ready for use.	4.1.3.1
Each specific message be recorded in advance so that it may be played remotely if the public address announcer has to evacuate.	4.1.3.1
The public address system be connected to the emergency generator, or some other power source so that it can continue to operate if electrical service is interrupted.	4.1.3.1
During an evacuation or other emergencies, the electronic message boards may be used to display evacuation instructions and guidance.	4.1.3.2

Basic messages addressing a variety of potential emergency situations be prepared in advance so that they may be activated in case the area where messages are controlled has to be evacuated.	4.1.3.2
If television monitors are in use, the visual quality and the size of the monitors to be sufficient and that they are effectively and strategically placed at appropriate locations.	4.1.3.3
Venues employ the use of temporary or permanent signage to assist in crowd management in and around the venue.	4.1.3.4
Venues protect and monitor computer systems and network infrastructure to be prepared against cyber-attacks.	4.2.1
Computer systems be tested regularly and security reassessments be performed to help identify any potential vulnerabilities as well as assist in detecting any patterns of probing, hacking, or intrusions.	4.2.1
Recommended	
A system of channel assignment be employed, so as not to crowd any single channel with excessive traffic.	4.1.1.1
Radios to be checked before being needed for events.	4.1.1.1
First responders, including law enforcement, test the capabilities of their radio systems within all areas of the venue at least annually to ensure their operability.	4.1.1.1

Protocols to be instituted for incident reporting following any type of disturbance at the venue, such as public intoxication, physical altercation, underage alcohol consumption, drug use, and illegal ticket sales.	4.1.1.2
Written communication, either paper or electronic, be used as a channel from staff to management regarding areas that require improvement or signal a need for attention.	4.1.1.2
If an emergency telephone reporting system is in place that it be coupled with a system of identification that indicates the precise location of the phone from which the call is placed.	4.1.1.4
A wired telephone independent of the facility's system be installed in the command center in case the system is compromised.	4.1.1.4
Venues include a law enforcement presence in the command center from federal authorities as well as local law enforcement.	4.1.2.1
Venues employ a paid law enforcement detail during event day operations.	4.1.2.1
An EMS representative as well as a representative from the local fire department be stationed inside the command center during events.	4.1.2.2
Venue representatives establish a point of contact at a critical infrastructure site with a person holding the authority to make necessary operational decisions during an emergency.	4.1.2.3
Venues periodically verify the point of contact at infrastructure sites and update the contact information if necessary.	4.1.2.3
The Director of Security or the Director's designee take responsibility for composing the content of the message during an emergency when pre-recorded messages cannot be used.	4.1.3.1

If electronic message boards are in use, the system be utilized during non-emergency situations to regularly test its functionality.	4.1.3.2
If television monitors are in use, the system be utilized during non-emergency situations to regularly test its functionality.	4.1.3.3
Permanent signage provide emergency contact information, incident or suspicious item reporting telephone numbers, evacuation routes and exits, and the location of emergency equipment.	4.1.3.4
Posted signage be used at the entrances for queuing and patron screening procedures, e.g. to identify objects that are restricted or prohibited from the venue.	4.1.3.4
Venues consider establishing a text messaging system that provides patrons with a number to which they can text a complaint or report of a disturbance.	4.1.3.5
If guest text messaging is in use at the venue, a database of reported incidents to be maintained for analysis.	4.1.3.5
Venues consider having an online presence through social platforms such as Twitter, Facebook or Instagram.	4.1.3.6
If venues use social media, they engage patrons in discussions prior to events, answer questions and concerns, as well as provide relevant event day information and updates.	4.1.3.6
Protocols be developed for ingesting, evaluating, and acting upon reports of various kinds (e.g. “See something, say something”).	4.1.3.6
Venues build a plan to mitigate cyber-security risks.	4.2.1
Cyber-security technologies be used to ensure that system processes are functioning properly, data is not compromised, and information can be accessed when needed.	4.2.1

Suggested	
Venue operators consider the use of multi-channel radios for internal communication for ALL staff.	4.1.1.1
Coded messages to be used so as not to instill panic in patrons.	4.1.1.1
Venues consider whether electronic or paper-based communication should be utilized to apprise security staff of known threats prior to an event.	4.1.1.2
Venues consider the use of an emergency paging system.	4.1.1.3
Venues investigate available technical solutions if cellular call volume causes network overload.	4.1.1.4
Venues verify contact information at nearby infrastructure sites at least semi-annually.	4.1.2.3
Pictorial depictions to be used on signs to help patrons, including those with limited proficiency in English, understand and remember what items are permissible in the venue.	4.1.3.4
If a text messaging system is in use, this system be considered for the dissemination of information to patrons during an emergency.	4.1.3.5

Appendix – Chapter 4

This Appendix provides ideas for the design and placement of signage and ways the effectiveness of signage might be evaluated for crowd management. It also presents some information on systems for managing incident reports, metrics for evaluating the effectiveness of social media, and ideas for cyber-security penetration tests.

Posted Signage on Crowd Management

The following items may be considered in the use of posted signage for crowd control:

- Placement and size of posted signage

- Visibility of signage, i.e. if a large crowd forms, is the sign still noticeable or does it become impractical?
- Design considerations for signage, such as use of colors, font sizes, pictures, diagrams, etc.
- The following ideas may be used for evaluating the effectiveness of posted signage:
    - Experiment with the usage of temporary signs along with barriers and stanchions for providing way finding information and directions
    - Remove temporary signs and observe the effect on crowd movement
    - Experiment with visual design of permanent signs for providing general information or emergency information
    - Ask patron to text a specified word to a phone number for a chance to win a prize. This may be used as a way to encourage patrons to subscribe to a venue's text alert system.

Systems for Managing Incident Information

Commercial systems are available to help collect, track, filter, and generate summary reports for incidents reported at venues. Two examples of such systems are AwareManager and ISS. These systems can take in incident reports from a variety of sources, help venue staff identify trends, and automatically escalate reports to the security director or other appropriate venue managers.

Text Messaging

GuestAssist is one example of a text messaging system that provides information about security, guest services, concessions, and first aid at sports venues.

Social Media

The following metrics may be used for evaluating effectiveness of social media:

- Size of following (number of fans, followers, subscribers, etc.)
- Frequency of interaction, e.g. updates, posts, replies
- Types of interactions, for example: post "likes" and "shares" on Facebook; "retweets" and "favorites" on Twitter
- Social media analytics tools may also be used to help track the effectiveness of social

media activities, e.g. Google Analytics, Klout, HootSuite, Facebook Analytics, etc. These metrics and tools provide an overview of how well a user/brand may influence or engage their audience, and are useful for designing social media campaigns and using social media as a mode of communication.

- Pre-event engagement, i.e. provide relevant information and updates on event day procedures
- Post-event engagement, i.e. fan satisfaction survey

Cyber-Security

In addition to utilizing firewall, anti-virus software, network monitoring software, etc., penetration tests may also be conducted for testing and evaluating computer system security.

Possible tests to perform include:

- Attempting to gain access to confidential information
- Disrupting network service by overloading server activities
- Attempting to modify a piece of data in a database system
- Identifying system recovery time following a disruption, i.e. if a power outage was to occur, how long would it take for the system to come back up?

Chapter 5 – Operations

Introduction

This chapter discusses operations management in the context of stadium security. It will focus on two main areas: facility security operations and response operations. As part of any planning cycle, a venue will implement preparedness planning and mitigation activities in an effort to reduce risk. The focus of many anti-terrorism efforts is to establish and implement core physical and protective security measures to mitigate risks. Should an incident occur, incident response operations utilizing the preparedness planning conducted by the venue can support mitigating the consequences of the incident. Therefore a clear response plan for incidents identified through the risk assessment process described in Chapter 2 will ensure venues not only address mitigation via security operations to reduce risk, but also will address the mitigation of consequences as a result of an incident.

Recent incidents may cause some rethinking of risk mitigation strategies. For example, what changes are needed after the 2013 Boston Marathon? What can be learned from what more open access venues and events, such as NASCAR and PGA, are doing? Changed perimeters at stadiums are under discussion to have "layers" of security inspection. There may be some indoor venues at which bags and containers can be banned entirely, but this may be much more difficult to implement at outdoor venues where fans want to bring extra clothing and covers for harsh weather. How much can patron education help? For instance, getting people into stadiums early will cut down on patron screening lines that create vulnerabilities.

At a practical level, security is often implemented using a layered approach. The attack during the 2013 Boston Marathon has highlighted this need. It is ***strongly recommended*** that specific "zones" or concentric rings be established, for which there is a reasonable expectation that a certain level of security can be maintained within the zone. Access points into and out of each zone are then identified, and proper screening measures control ingress and egress. The use of multiple concentric security zones also will help mitigate the threat to a large number of unscreened patrons gathered at one place and time. This chapter deals with those physical and protective security measures that are taken within those zones. The number of zones may vary and if one imagines all the possible layers of security that encompass a stadium, the outermost would be the customs and border protection services that monitor foreign VIPs as they travel to the event. The innermost might be the security officers who protect players' locker rooms. Somewhere in between lies the point at which patrons may exit major thoroughfares and public transportation and begin their final approach to the stadium. It is this core area in which a venue may establish a number of zones, most commonly three.

This section will also address the incident response operations that venues may include in their security plans to ensure that consequences are mitigated should an incident occur. In order for response operations to be effective, it is ***strongly recommended*** that training and exercises focus on them as part of the venue's training plan (see Chapter 6). Effective incident response operational plans described in this section include evacuation/shelter-in-place plans and special event plans.

5.1 Outer Zone

The outer perimeter for many venues starts at the point of access to the parking lots. For others, it may be a set distance beyond the walls of the venue's structure or property boundaries. Not only is this area a potential staging ground for attacks, but it is also a potential target. Perimeter control needs to balance safety and security. For example, locked facility doors can help keep a venue secure, but they decrease safety for evacuation purposes and may even conflict with fire safety codes. As another example, if bomb sniffing dogs can be deployed only within a secure perimeter, it may be better to forego deploying the dogs and maintain an established security perimeter so that potential bomb threats cannot get close to the venue.

Regardless of the footprint of the outer perimeter, a number of security efforts may be implemented to reduce risk. The outer perimeter of every venue is connected to the area transportation network, and this connection point may provide the initial opportunity for the venue to start reducing its risk. Whether through coordination with area transportation officials or access to area Intelligent Transportation Systems (ITS), the use of traffic lights provides an opportunity to re-route and meter traffic as it approaches the venue in an effort to allow for effective screening and security.

5.1.1 Parking Structures

If a venue owns and operates parking lots or structures, it is ***strongly recommended*** that security tactics be implemented prior to, during, and after people access these lots or structures. Different lots and structures may be used by patrons, media, employees, and vendors, requiring perhaps different security tactics. It is ***strongly recommended*** that tactics include assigning staff to these areas who are able to relay information to the command center. It is also ***recommended*** that some assigned staff include patrols of trained security or law enforcement personnel. It is ***recommended*** that these patrols be on foot and visit locations in random order. In addition, it is ***recommended*** that all lots be surrounded by physical infrastructure such as fences, trees or walls, and that a network of Closed Circuit Television (CCTV) cameras be used to support monitoring and response. CCTV specifically can aid in identifying unauthorized vehicles circumventing parking lot access control. It is ***suggested*** that some personnel be in plain clothes to allow for their integration into parking lot activities without drawing the attention of suspicious persons

and that some of them be trained in behavioral assessment.

Access to the parking lots can also be monitored by staff. It is ***strongly recommended*** that vehicles parking within 100 feet of the venue structure be checked utilizing a detailed vehicle security screening process. It is ***recommended*** that vehicles be kept at least 100 feet away from the facility whenever possible. In addition, it is ***suggested*** that vehicles parking further than 100 feet from the structure also be checked utilizing a detailed vehicle security screening process. This stand-off distance may be expanded to incorporate moving vehicles and may be supplemented by or implemented under a Buffer Zone Protection Plan (BZPP). To further enhance parking security and reduce venue risk, in-depth strategies or technological security measures may also be implemented. It is ***suggested*** that venues consider integrating license plate reader devices at parking access points to identify potential threats.

It is ***suggested*** that venues with larger budgets devoted to security development consider the following pilot program on a small scale. The venue would set up target vehicle parking areas in which vehicles in high risk of drawing criminal activity or identified by intelligence reports as such may be located in sight of parking lot staff. Alternatively, staff may be assigned to monitor vehicles if parking in these target areas is not possible.

The 2013 Boston Marathon attack also highlighted the need for securing garbage cans and other locations where an IED may be placed. It is ***recommended*** that venues use clear garbage cans with clear liners and have security personnel check them regularly during an event.

Questions	Metric
If applicable, does the venue have vehicle screening protocols in place? Do these protocols include media, staff, vendors and service providers?	Y/N, Y/N
How close may a vehicle park to the stadium without being screened?	#
Are license plate readers or other devices used to identify patrons or their vehicles in the parking lot areas?	Y/N
How many security personnel are patrolling the parking lot areas? How many CCTVs are monitoring these areas?	#, #
What is the average ratio of patrol staff to vehicles?	:

Are patrols randomized?	Y/N
Is behavioral assessment used? If so, how many law enforcement officials with behavioral assessment training are utilized on event days?	Y/N ,#
How many plain clothes law enforcement officials are utilized on event day?	#
If applicable, are parking infrastructures protected by physical security measures?	Y/N
How many clear garbage cans with clear liners (contents visible) are in place? How many opaque garbage cans (contents not visible) are in place?	Y/N, Y/N

5.1.2 Coordination with Public Transportation

It is ***strongly recommended*** that any public transportation systems that intersect the outer perimeter be addressed by venues in their security plans. Coordination with the transit operating agency, covered in Chapter 4, is critical. Additional and stronger barriers between the transit system and the venue may produce a great benefit to the venue, since physical structures may be used to reduce cascading consequences to the venue should an incident occur on those systems. CCTV's in and around the system will support a common operating picture for those in the venue's command center. Interactions between the venue and public transportation systems may include entering into a memorandum of understanding (MOU).

Questions	Metrics
Are structures in place to ensure safe and speedy movement to and from critical transportation systems around the venue?	Y/N
How many CCTVs are in place monitoring the area between transportation systems and the venue?	#

5.1.3 Vendors and Service Providers

In addition to public transportation and patron personal vehicles, the outer perimeter deals with a myriad of security issues related to service providers and deliveries (see also section 5.2.2 concerning access to loading docks). It is ***strongly recommended*** that venues develop and implement a vendor and service provider security protocol to ensure only those cleared to pass through the outer perimeter can do so. In addition to deliveries, some vendors or service providers may also request access during both event and non-event day operations. Access may be required for mail deliveries, utility repairs, trash collection, etc. It is ***recommended*** that all

vendors provide a list of personnel and their vehicles, plate numbers, and other information for verification. As a general rule, it is ***recommended*** that access for mail, deliveries, and non-essential repairs be cut off well in advance of the event start time. VIPs can also provide similar information and be announced ahead of their arrival. During sports events, it is ***suggested*** that visiting teams be inspected off-site.

Questions	Metrics
Is there an initial screening for vendor deliveries? How far away from the venue?	Y/N ,#
At this checkpoint, is the delivery driver information checked with information provided by the vendor?	Y/N
Do service providers have to schedule a time to conduct service repairs?	Y/N
Is trash collection conducted outside of event operational times?	Y/N

Open Ended Questions	Anticipated Response
What screening techniques are used when conducting patron vehicle screening?	Technique Description
What screening techniques are used when conducting employee vehicle screening?	Technique Description

5.1.4 Airports

It is ***suggested*** that those venues located near airports and venues having established flight takeoff or approach paths over them coordinate with airport officials and the Federal Aviation Administration to see if alternative paths are available during event-day operations. Some airports may be able to utilize alternative runways as much as possible to limit low flying airplanes above venues. Venue security also can raise the issue of flight rules for general aviation aircraft in the vicinity of a venue especially during the day of an event. The decision to change flight paths may be out of the venue's control, but initiating the conversation can lead to some reduction in risk and at a minimum will establish a connection with the airport staff for future coordination needs and communication.

Questions	Metrics
How frequently do airplane takeoffs or approaches at nearby airports coincide with time of events? How close do airplanes come to the venue?	Freq. ,#

5.2 Middle Zone

5.2.1 Patron Access

When developing an access control plan, a venue must balance security concerns for patrons inside the venue with concerns about security for patrons outside the venue, specifically those waiting in a queue to enter the venue. More diligent patron screening can increase safety inside the venue, but if this screening creates long lines outside the venue, then the increased security might actually increase overall risk. Especially in light of the 2013 Boston Marathon bombing, the risk posed to a large gathering as occurs in a queue outside a venue is readily apparent.

There are three common methods of patron screening: pat-down, wanding and magnetometer. It is ***strongly recommended*** that venues employ at least one of these methods for all patrons. It is ***suggested*** that a venue consider using a combination of these methods in patron screening in order to take advantage of the value of the most effective screening techniques, and the speed of alternative techniques. For example, a venue might pat-down half their entering patrons and wand the other half, with the decision about which method to use for a given patron being made randomly using a randomization device or method. One key issue about such a procedure is implementing randomization in practice without being accused of profiling. More information on implementation of randomization in patron screening may be found in the appendix. Which of the three screening methods, or combination of methods, is best for a venue depends on consideration of the balance of security inside versus outside a venue as well as the speed of throughput and number of employees involved in the screening. Here are some of the issues and concerns with each procedure.

The use, and therefore the effectiveness, of pat-downs and wanding, is very inconsistent, varying from screener to screener. These procedures are also potentially less effective over time as staff grows tired or bored or as staff feels pressured to work quickly either because of long lines building up or the impending starts of the event. It is ***strongly recommended*** that venues employ

training and random tests of patron screening staff to mitigate these issues. It is ***suggested*** that venues consider rotating staff in and out of the busiest and most stressful patron screening jobs. (Combined with training staff for multiple front-line roles, this latter suggestion also has the benefit of adding to staff flexibility as discussed in Chapter 3.)

Magnetometers are the third common method for screening patrons. They have been used in airports since 1970 to check passengers for weapons. Magnetometers are considered to be more effective than the other two methods, but there are good reasons not all venues use them. They are expensive, take up a lot of space, and do not work well in windy conditions. If a venue does use magnetometers, it is ***strongly recommended*** that the venue limit the possibility of these magnetometers acting as an obstruction during an evacuation (see chapter appendix).

One of the costs of using magnetometers can include changing the footprint of the inspection area, perhaps requiring use of some of the parking area. Future development of wider magnetometers that will allow several people to walk through at once is an "outside the box" idea of a technology that might take advantage of theoretical tools such as combinatorial group testing. Additional details about these possible methods are discussed in the appendix.

It is ***strongly recommended*** that venues also screen bags upon entering stadiums (see reference to DHS bag search guide in chapter appendix). Bags pose an especially large threat as a container to deliver an IED. It is ***recommended*** that some method is employed to lessen this risk such as an initial layer of screening to check large bags quickly for IEDs. Since bags pose a risk and slow down inspection procedures, it is ***suggested*** that guidelines to limit the size of bags be established, taking into account the needs of patrons along with the venue risk assessment. It is ***suggested*** that venues provide incentives for those coming without bags, for instance moving those patrons to faster-moving inspection lanes.

In order to assess the risk to patrons waiting in line to enter the stadium, it is ***strongly recommended*** that venues estimate queue length at patron screening lines. While physically counting each patron in line might be impossible, a venue can use a few tricks to estimate queue length. First, they can estimate size by the space in which the queue is contained, and then use an estimate for the density of patrons. One issue with this method is that as the queue builds,

patrons might crowd in more, and patron density might increase. A second way to measure queue size is by measuring the time it takes to enter the venue.

Leagues and stadiums take very different stances with regard to modifying patron behavior. What some regard as unchangeable constraints (e.g., patron arrival patterns), other organizations are modifying through patron education and incentive programs. Since leagues are reluctant to distress their patrons, it is ***recommended*** that simulation and modeling be used to understand and project variations in screening, and in patron behavior. It is also ***recommended*** that venues attempt to modify fan behavior to reduce queue lines and track the success of various programs.

It is ***recommended*** that venues set and meet queue size goals. It is ***suggested*** that venues do some of the following to limit queue size and consider other methods by which they can reduce queue length, and thus the risk:

- Employ more patron screeners and/or train screeners more thoroughly to maximize their effectiveness and speed
- Develop incentives to encourage patrons to arrive earlier and/or arrive at less busy gates
- Employ a patron screening strategy that is responsive to queue size, for example switching procedures or instituting random procedures if the size gets too large
- Cut off access to a gate if the queue size at the gate gets too large

It is suggested that venues study and potentially pilot a program for expedited screening of season ticket holders and other trusted patrons, possibly patterned after the TSA PreCheck program (see a discussion of the PreCheck program in chapter appendix).

Questions	Metric
Are queue lengths measured or estimated?	Y/N
What size bags are allowed inside the venue?	#
Are procedures in place to encourage early arrival or arrival at gates with less traffic? Are measures of the success of these procedures in place?	Y/N, Y/N
Is there an initial layer of screening before patrons enter the queue?	Y/N

Are models use to estimate the impact of changes in the patron screening process?	Y/N

Open Ended Questions	Anticipated Response
What are goals related to queue length and are they being met?	Comparison of goals to standards, and of performance to goals.
What method(s) of screening is employed at patron entry points in comparable venues?	Comparison to similar stadiums

5.2.2 Loading Dock Access

It is ***strongly recommended*** that deliveries be allowed only if scheduled in advance (see also section 5.1.3). Advanced scheduling can be completed with sufficient time to permit vetting of the delivery company, the driver's license of the delivery person, and the contents listed on the manifest. It is ***strongly recommended*** that the contents listed on the submitted and vetted manifest be reconciled with the contents of the vehicle or truck at the time of delivery. It is ***strongly recommended*** that the previously submitted and vetted driver's license of the delivery person match that of the person making the delivery. It is ***strongly recommended*** that all vehicles requesting access to a loading dock at the venue undergo thorough screening. It is ***recommended*** that this screening include a survey of the vehicle undercarriage as well as of the vehicle contents including the trunk of any vehicle and both the inside and cab of the truck or trailer. If a K-9 resource is available, it is ***recommended*** that the delivery vehicle be screened for explosives using the K-9 unit. If no K-9 unit is present, it is ***recommended*** that the vehicle be swiped for the detection of explosive materials. The material used to swipe the vehicle is analyzed in a detection machine and the entire process takes between one and two minutes.

Questions	Metric
Are the contents of the vehicle inspected to ensure they correspond to the delivery manifest? If this inspection is random, what percentages of vehicles and/or packages are inspected?	Y/N ,%

Is the undercarriage of the delivery vehicle inspected?	Y/N
Are K-9 units deployed to screen the vehicle for explosives?	Y/N
Are vehicles swiped to detect explosive materials?	Y/N

5.2.3 Media Access

Media personnel require dedicated access and screening due to their broad access credentials and media equipment such as cameras, laptops, wiring, and large bags; items that are restricted to general access patrons. For example, it is ***strongly recommended*** that all broadcast camera transfer cases either be removed to the broadcast truck, or secured and locked. These large cases are both large enough to hide an explosive device while at the same time very familiar to security personnel who may tend to overlook these objects once inside the perimeter.

It is ***strongly recommended*** that all media trucks and vehicles that are permitted to enter the premises of the venue be thoroughly inspected. It is ***recommended*** that this screening include a survey of the contents. It is ***suggested*** that media personnel be screened separately in order to allow a careful and attentive screening of equipment and credentials. It is ***suggested*** than venues consider a separate entrance for media personnel access.

Question	Metric
Are media inspected before entry?	Y/N
Are media vehicles inspected before entry?	Y/N

5.2.4 Cameras

Cameras are frequently utilized within the middle security zone. If cameras are available it is ***strongly recommended*** that cameras be placed along the outside perimeter of the venue and at key vantage points within the zone that grant a view of the crowd, including queues and entrances. It is ***recommended*** that these cameras be monitored at the command center. It is also ***recommended*** that all personnel monitoring the cameras be trained in how to detect suspicious activity and behavior. It is ***recommended*** that cameras be trained on key air intake and electrical

delivery systems so as to help harden security against the introduction of a chemical or biological agent into the system or disrupting venue power. A combination of devoted camera and positioned security personnel at key intake or electrical station is ***suggested***. It is ***suggested*** that the venue consider moving cameras from time to time, perhaps using random procedures. It is ***suggested*** that venues consider utilizing a software tool that can identify unattended bags. It is important to note that some similar software packages have shown a substantial quantity of false alarms and were determined not to be useful.

Questions	Metric
How many cameras are used in the middle zone of the venue?	#
How frequently is camera performance monitored?	Freq.
Are camera positions changed from time to time? If so, how often?	Y/N, Freq.
Are any cameras equipped with intelligent analytics to detect potential threats?	Y/N

5.2.5 Sweeps

The middle zone can also include regularly performed sweeps. It is ***strongly recommended*** that each sports venue incorporate into its security plan operational protocols for the purposes of sweeping by trained security staff. It is ***strongly recommended*** that these regularly scheduled sweeps build upon incentive-based training scenarios so as to leverage continuity between exercise and practice. It is ***strongly recommended*** that pre-event sweeps include protocols (see chapter appendix) to ensure that rooms, the merchandise and concession warehouse, and other venue spaces are properly swept as part of the pre-event process and/or response to a bomb threat.

It is ***suggested*** that venues with either mutual aid agreements or the appropriate budget might consider the use of local law enforcement bomb or K-9 units to perform the sweep for the venue. It is ***suggested*** that certain venues also consider investing in their own K-9 unit for both scheduled and random sweeps prior to the event.

5.3 Inner Zone

5.3.1 Cameras

The inner zone of any venue includes everything just past where patrons are checked and ticketed. Commonly referred to as the "inside of the stadium" this zone is both significant and multi-faceted. It is ***strongly recommended*** that venues have cameras installed that provide coverage for all major and minor areas within the venue – including blind corners, and that venues have the ability to store copious amounts of digital videotape footage captured by the cameras. For those venues that are either outside or potentially encompass miles of area, camera coverage need not be as extensive; however, key coverage areas and regular testing of little-used camera equipment can be implemented as part of the security's quality assurance plan. It is ***suggested*** that venues consider incorporating camera software with facial recognition software if budget and threat determination warrants.

Questions	Metrics
How many cameras are utilized in the inner zone? Do they have zoom capability?	#, Y/N
How often are cameras in the inner zone checked?	Freq.
Are cameras in the inner zone moved from time to time to avoid a stagnant pattern of placement?	Y/N
What percentage of the inner zone can be seen by camera?	%
For what length of time is camera footage stored?	#

5.3.2 Sweeps

Regular manned security sweeps within the inner zone can work in conjunction with a venue's electric eyes. It is ***strongly recommended*** that all sports venues perform manned sweeps before every event to look for suspicious items including signs of equipment tampering. Guards, janitors and other venue staff will be familiar with the surroundings, so they can notice changes (e.g. the number or position of trash cans has changed). It is ***strongly recommended*** that these sweeps incorporate a random check of food vendor product as it is unloaded from the vendor truck to the product storage within concession areas. Sweeps can also include equipment storage

areas and restrooms. As noted in section 5.2.5 venues may consider ways to incorporate K-9 units in sweeps either through cooperation with another agency or investing in in-house K-9 units housed on site.

Questions	Metrics
How frequently are areas in the inner zone swept for suspicious materials?	Freq.
Are bomb-sniffing K-9 units involved in these sweeps?	Y/N

5.3.3 Access Control

Clearly defined sensitive or critical areas and access points for security personnel are also a key factor for the inner zone. This can lead to a complicated discussion among venue security. On one side of the discussion, venues may not want to "advertise" where their vulnerable or strategically significant areas are to the general public. However, such obfuscation may actually make security personnel inefficient if they are never trained regarding areas and their purposes. It is ***strongly recommended*** that venues draft proper signage indicating to patrons which areas within the inner zone they can access and which they cannot. It is ***strongly recommended*** that all sports venues draft a plan that clearly defines areas and access points for all personnel within the hierarchy. The plan may well be an extension of one that is already in place to safeguard rooms where cash or tickets are kept, or areas where alcoholic beverages are stored. It is ***recommended*** that the plan correspond to key-card level access, if such a system is in place. Other cues (barricade tape, potted trees, change in carpeting or wall color, etc.) can also be used to reinforce that an area is off-limits to patrons. It is ***recommended*** for certain venues with unique footprints and appropriate budgets to also incorporate alarms systems that trigger when unauthorized entry is made through access points within the inner zone. Camera systems could work in conjunction with alarms to alert when access points have been breached and increase the chance of recording the transgression.

It is ***strongly recommended*** that a venue use credentialing to assist in limiting employee and patron access to appropriate areas. DHS has provided excellent suggestions for developing and implementing credentialing procedures (see reference in chapter appendix). It is ***strongly recommended*** that color coding on credentials be used to delineate clearly the access levels of an

employee, and that a photo also be present on the ID to ensure its use by the rightful owner only. It is ***recommended*** that venue security review the protocol concerning who gets what kind of credentials and how those are verified. It is ***recommended*** that smart card technology be used, since this technology can assist in tracking employee movements and monitoring for suspicious behavior. It is ***suggested*** that a venue make temporary credentials substantially different from one event to another. There have been reports that imposters posing as venue staff or part of the event-day entertainment (e.g. a person in military uniform carrying a rifle posing as part of the color guard) have been able to get into venues without being verified. Thus far, these cases have been for the purpose of pranks or hoaxes, but they provide an existence proof that imposters can gain access to the inner security zone.

5.3.4 Security

In addition to the key security tactics outlined above, there is a need for ensuring the safety of all persons within the inner perimeter by addressing all possible intrusion paths discovered in the venue's vulnerability analysis. Terrorists may utilize various points of attack including food contamination, mail delivery, and others.

Food security is an issue addressed with widely varying degrees of effectiveness and thoroughness. Effective measures can be as simple as putting out condiments in packets, rather than large dispensers that serve as targets of opportunity for chemical or biological agents. It is ***recommended*** that venues establish food security policies which address the entire supply chain beyond just the inner security zone. However, within the inner perimeter, ***suggested*** simple policies include thoroughly securing food and ice storage areas and conducting in-house health inspections in addition to the locally required inspections, while more in-depth policies may include strict procedures for inspecting food containers prior to opening to ensure tampering did not occur.

Like food security, mail security may also pose an avenue for a terrorist attack. It is ***strongly recommended*** that venues implement mail-handling security policies based upon guidance by the United States Postal Service. Additional policies that may enhance security could also include addressing mail processing procedures, staff training, and mail inspection technologies.

Detailed examples are provided in the attached appendix.

Questions	Metrics
Are there alarm systems in place to recognize unapproved entry to off-limits areas?	Y/N
Are protocols in place to address alarms from access systems?	Y/N
Are statistics kept on the number of unauthorized attempts to enter secure areas?	Y/N
Is the ability to enter secure areas with expired or missing credentials tested? What percentage of the time can secure areas be accessed successfully with such credentials?	Y/N, %
Is there a plan in place clearly delimiting different areas of the stadium, their access points, and the card level access required to enter them?	Y/N
Are there established food security policies in place?	Y/N
Are there established mail security policies in place?	Y/N

5.4 Response

Response refers to all activities that are involved in mitigating the damage inflicted by a terrorist attack. In order to be effective, incident response must be a process that is trained and drilled clearly and consistently. Everyone involved must be clear about their role, and also the roles of those around them. Furthermore, the security manager must be aware of the different corporations, government agencies, and outside entities that are to be involved in the response plan, and ensure that they too are clear on procedures. Finally, the security manager must also be responsible for integrating all the response organizations, ensuring that communication and cooperation can and do occur.

5.4.1 Incident Response Plans

Incident response planning is an important component of venue security operations management and it is ***strongly recommended*** that every venue have an incident response plan, at minimum formalizing in writing the existing unwritten plans. Every venue has at least informal plans for attending to and transporting an injured player or patron that include EMS, security, and crowd

control. As the magnitude of an incident increases, the level of response and the need for a coordinated plan increases dramatically. Thus an incident response plan will involve many parties, including venue staff, outside agencies, VIP attendees (e.g. players, coaches, ownership, political dignitaries) and their security staff, etc. As such, they may become quite complex and the potential for confusion is high, unless roles and responsibilities are explicit, understood, and exercised. Security managers must therefore ensure that policies and procedures are clearly understood, and it is ***strongly recommended*** that they be drilled regularly. Incident response plans may include a variety of operational response plans addressing a number of identified threats based upon the results of the risk assessment. It is ***strongly recommended*** that DHS Best Practices (see chapter appendix) be incorporated into these incident response plans as appropriate. These response plans may be supplemented by additional operational plans meant to minimize consequences such as mass decontamination, on-site medical services, shelter-in-place, and expedited evacuation. It is ***strongly recommended*** that evacuation and shelter-in-place plans be a core component of the security incident plans developed to support response capabilities. It is ***strongly recommended*** that a plan for handling the possibility of mass fatalities also be developed.

Questions	Metric
How many incident response plans has the venue developed?	#
Do these response plans cover the threats identified as having the greatest risk as identified in the risk assessment?	Y/N

How often are exercises conducted on implementing the incident response plans?	Freq.
Are response plans changed based on the results of exercises?	Y/N
Has the venue developed a mass fatality plan?	Y/N
Has the venue developed a mass decontamination plan?	Y/N

Open Ended Questions	Anticipated Response
Describe the resources available on-site to support implementation of the mass fatality plan?	Resource Description
Describe the resources on-site to support the mass decontamination plan?	Resource Description

5.4.2 Evacuation

The most important thing to note regarding evacuation is that it can be considered a last resort. Even when a serious incident occurs, complete evacuation might not be the correct response. Shelter-in-place and partial evacuations are other responses to incidents that might be considered by a venue. It is ***strongly recommended*** that a venue develop procedures and metrics for quickly determining whether an evacuation is necessary. Inevitably some decisions will need to be made on-the-fly, but it is ***recommended*** that a venue try to minimize the number of decisions that are not predetermined. Information developed by FEMA, OSHA, and other government agencies can be useful in developing procedures and decision criteria. It is ***recommended*** that testing of these procedures be done via tabletop exercises, and also that plans be developed in consultation with public partners.

It is ***recommended*** that a venue use the tools at its disposal to prepare fans for potential evacuation before the start of an event. For example, venues might use pre-event messages to instruct fans on basic procedures for active evacuation routes in the event of an emergency. This will help some fans learn what to expect if an evacuation occurs, but it also simply allows fans to process the possibility of an evacuation well before one must take place. Such precautionary messages have proven useful in other settings, including for example, the instructions at the start of an airline flight.

In the event of an evacuation, venues will be reliant on front-line staff to successfully guide patrons through the evacuation. Expert opinion is that during an evacuation fans will be fairly attentive to direction from ushers and stadium staff, and that this willingness to follow direction

is even stronger when patrons are used to receiving direction from staff during a normal event. It is ***recommended*** that venues place staff in positions to assist patrons needing to move throughout the venue. It is ***recommended*** that if these staff members are not security personnel that they still receive briefings and training on procedures for an evacuation. A venue might measure how much direction takes place during a normal event by sending in "secret shoppers" to report back on interaction with stadium personnel. However, not all staff will remain at their posts during some incidents. It is suggested that venues consider conducting anonymous surveys of staff to understand the impact of potential staffing reductions during incidents that match the threats identified in the risk assessment.

End of event stadium clearance offers a good approximation for what a venue evacuation might look like. It is ***strongly recommended*** that venues maintain statistics on end of event clearance time, in order to estimate how quickly an evacuation might be possible. For an even more advanced analysis of its preparations, it is ***suggested*** that a venue might study how well stadium employees and patrons react if an exit is closed or normal stadium egress is hindered in some limited manner (e.g. temporary construction or malfunction) and assess the impact on clearance time.

It is also possible that an incident inside a venue might be intended to lure people out of the venue mass, since it is then easier to inflict mass casualties on a crowd in unscreened, open areas outside of a venue. To limit this risk, it is ***recommended*** that a venue monitor major egress routes for anomalies throughout an event. Furthermore, this risk can be factored in when making the decision to evacuate the venue. Large crowds leaving a venue pose a risk even during normal end of event venue clearance. It is ***recommended*** that a venue coordinate with local authorities, especially transit agencies, to be sure that crowds can disperse quickly in both evacuation and normal end of event scenarios. It is also ***recommended*** that a venue monitor and sweep outside areas where large numbers of fans are likely to congregate or pass through after an event. The sweeps are designed to look for suspicious individuals, vehicles, and packages.

Questions	Metric
Are evacuation and shelter-in-place plans in place?	Y/N
What percentage of fans have a basic knowledge of stadium evacuation procedures?	%
How long would an evacuation of a capacity crowd take?	#
How long would a shelter-in-place of a capacity crowd take?	#
How often are employees trained on evacuation procedures?	Freq.
How often are evacuation drills conducted?	Freq.
Are staff positioned within the stadium to assist with fan movement during the event?	Y/N
How many times are secret shoppers given directions by stadium employees on their way to their seats?	#
On average, how many minutes after the end of an event is the stadium cleared?	#
Are exits closed (or other obstructions introduced) to study this impact on stadium clearance time?	Y/N
Are there assurances in place that emergency vehicles and personnel can reach the stadium during an evacuation?	Y/N
Is there a procedure in place for determining if an evacuation is necessary?	Y/N
Are egress routes monitored for potential security risks?	Y/N
Does the stadium coordinate with local authorities to assure quick dispersal of stadium patrons from the area around the stadium either during an evacuation or at the end of an event?	Y/N
Are evacuation routes identified?	Y/N
What are the roadway capacities of the evacuation routes from the stadium?	#
Does the venue implement traffic management plans pre and post-event?	Y/N
Are evacuation procedures communicated to fans during or before an event?	Y/N
How many minutes of air-time are given on the message boards to evacuation procedures? How many minutes before the start of an event are these procedures last mentioned?	#,#

Open Ended Question	Anticipated Response
Describe the resources available on-site to support implementation of the evacuation plan.	Resource Description

5.4.3 Planning

There is a natural tension between developing plans for specific threats, and treating incident management more holistically. Specific plans might be in place for any of the following: bomb threat, fire, earthquake, utility outage, CBRN (chemical, biological, radiological, and nuclear), lightning, active shooter, IED, vehicle-borne IED, medical emergencies, or more. Each of these threats may require specific responses. It is ***strongly recommended*** that a venue develop a comprehensive evacuation plan. It is ***strongly recommended*** that a venue prioritize development of specific incident plans based on their potential threat as identified in the risk assessment. At the same time, it is impossible to plan for the details of all possible events, so it is ***recommended*** that in combination with specific response plans a venue develop a set of general response principles that can then be applied to whatever incidents do develop it is ***strongly recommended*** that a venue use tabletop exercises as a way to test and develop incident management plans. Proper incident management preparation involves coordination with outside groups such as local law enforcement, fire, and OEM, and it is ***suggested*** that a venue consider involving these groups in any tabletop exercises it develops.

It is ***strongly recommended*** that venues participate in tabletop exercises with quantifiable metrics of performance. Any weaknesses that are discovered as a result of the tabletop exercise can be used to improve the security plan. It is ***strongly recommended*** that tabletop exercises be as realistic as possible. For example, in a previous chapter, we recommended randomly excluding participants from the exercise and splitting participants into separate groups in order to simulate real-world possibilities.

It is ***strongly recommended*** that the security management of a venue include venue management in incident response planning. It is ***recommended*** that venue managers are prepared for what to say and do publicly in an emergency. It is also ***recommended*** that security at a venue advise

venue management, which is usually civilian, how to interact with outside agencies in the event that these agencies must come in and take over command of venue security. This preparation can include briefings presenting what might occur during various scenarios.

It is ***suggested*** that venues consider the development of procedures to follow when planning for unique events that may require increased security. These unique events may alter the overall risk assessment and therefore may require different response capabilities should an incident occur. These special event procedures will include notifying staff and stakeholders of changes to any response plans. Such plans may include changes to the incident command system and leadership changes under these events. For example, a venue may conduct a championship game in which the league inserts itself into the incident command structure at high levels, which would be unusual for regular season games. Venue staff including non-security personnel may be affected and confused by the communication chain-of-command due to changes in security protocols. These events may even escalate to National Special Security Event (NSSE) designation in which the United States Secret Service takes the lead on security operations, and other federal agencies lead core functions such as intelligence, counter-terrorism, disaster management and recovery.

Questions	Metric
Are plans in place for handling elevated security events?	Y/N
How often are plans reviewed with agencies with added responsibility for special events?	Freq.
Are security procedures documented should outside entities need to take control?	Y/N
Is speed of response tested during tabletop exercises (or other venue incident response preparedness drills)?	Y/N
Is venue management consulted with respect to incident management planning?	Y/N

Open Ended Question	Anticipated Response
What additional agencies are involved in plans for special events?	List of agencies

5.5 Operations: Key Points

- A clear response plan will ensure venues not only address mitigation via security operations to reduce risk, but also will address the mitigation of consequences as a result of an incident.
- Security is often implemented using a layered approach.
- Perimeter control needs to balance safety and security.
- The outer perimeter of every venue is connected to the area transportation network, and this connection point may provide the initial opportunity for the venue to start reducing its risk.
- A network of Closed Circuit Television (CCTV) cameras can be used to support monitoring and response.
- A 100 foot stand-off distance may be expanded to incorporate moving vehicles and may be supplemented by or implemented under a Buffer Zone Protection Plan (BZPP).
- Coordination with the transit operating agency that intersects with the outer perimeter is critical.
- There are three common methods of patron screening: pat-down, wanding, and magnetometer.
- A venue must balance security concerns for patrons inside the venue with concerns about security for patrons outside the venue, specifically those waiting in a queue to enter the venue.
- Bags pose an especially large threat as a container to deliver an IED.
- Middle and inner zone security can include sweeps performed at regular or randomized intervals.
- Cameras are frequently utilized within the middle and inner security zones.
- Media personnel require dedicated access and screening due to their broad access credentials and media equipment such as cameras, laptops, wiring, and large bags; items that are restricted to general access patrons.
- All vehicles requesting access to a loading dock at the venue must undergo thorough screening.
- Clearly defined areas and access points limited to security personnel are important for inner zone security.

- Ensure the safety of all persons within the inner perimeter by addressing all possible intrusion paths discovered in the venue's vulnerability analysis. Terrorists may utilize various points of attack including food contamination, mail delivery, service repairs and others.

- Response refers to all activities that are involved in mitigating the damage created by a terrorist attack. In order to be effective, incident response must be a process that is trained and drilled clearly and consistently.
- Shelter-in-place, partial and complete evacuations are responses to incidents that might be considered by a venue.
- Specific plans might be in place for any of the following threat scenarios: bomb threat, mail bomb threat, fire, earthquake, utility outage, hazardous material, CBRN (chemical, biological, radiological, and nuclear), civil unrest, plane crashes, active shooter, IED, vehicle-borne IED, medical emergencies, and others.

5.6 Recommendations – Chapter 5 Operations

Chapter 5 – Operations	
Strongly Recommended	Section
Specific "zones" or concentric rings be established, for which there is a reasonable expectation that a certain level of security can be maintained within the zone.	Intro
Training and exercises focus on [response operations] as part of the venue's training plan.	Intro
Security tactics be implemented prior to, during, and after people access [parking] lots or structures.	5.1.1
Security tactics include assigning staff to [parking] areas who are able to relay information to the command center.	5.1.1
Vehicles parking within 100 feet of the venue structure be checked utilizing a detailed vehicle security screening process.	5.1.1

Any public transportation systems that intersect the outer perimeter be addressed by venues in their security plans.	5.1.2
Venues develop and implement a vendor and service provider security protocol to ensure only those cleared to pass through the outer perimeter can do so.	5.1.3
Venues employ at least one of the following methods of patron screening: pat-down, wanding, or magnetometer.	5.2.1
Venues employ training and random tests of patron screening staff to mitigate [inconsistent or poor performance].	5.2.1
Venues limit the possibility of magnetometers acting as an obstruction during an evacuation.	5.2.1
Venues also screen bags upon entering stadiums.	5.2.1
Venues estimate queue length at patron screening lines in order to assess the risk to patrons waiting in line to enter the stadium.	5.2.1
All vehicles requesting access to a loading dock at the venue undergo thorough screening.	5.2.2
Deliveries to be allowed only if scheduled in advance.	5.2.2
The contents listed on the submitted and vetted manifest be reconciled with the contents of the vehicle or truck at the time of delivery.	5.2.2
The previously submitted and vetted driver's license of the delivery person match that of the person making the delivery.	5.2.2
All broadcast camera transfer cases either be removed to the broadcast truck, or secured and locked.	5.2.3

All media trucks and vehicles that are permitted to enter the premises of the venue be thoroughly inspected.	5.2.3
Cameras be placed along the outside perimeter of the venue and at key vantage points within the [middle] zone that grant a view of the crowd, including queues and entrances.	5.2.4
Each sports venue incorporates into its security plan operational protocols for the purposes of sweeping by trained security staff.	5.2.5
Regularly scheduled sweeps build upon incentive-based training scenarios so as to leverage continuity between exercise and practice.	5.2.5
Pre-event sweeps include protocols to ensure that rooms, the merchandise and concession warehouse, and other venue spaces are properly swept as part of the pre-event process and/or response to a bomb threat.	5.2.5
Venues have cameras installed that provide coverage for all major and minor areas within the venue – including blind corners, and that venues have the ability to store copious amounts of digital videotape footage captured by the cameras.	5.3.1
All sports venues perform manned sweeps before every event to look for suspicious items including signs of equipment tampering.	5.3.2
Sweeps [of the inner security zone] incorporate a random check of food vendor product as it is unloaded from the vendor truck to the product storage within concession areas.	5.3.2
All sports venues draft a plan that clearly defines areas and access points for all personnel within the hierarchy.	5.3.3
Venues draft proper signage indicating to patrons which areas within the inner zone they can access and which they cannot.	5.3.3

Venues use credentialing to assist in limiting employee and patron access to appropriate areas.	5.3.3
Color coding on credentials be used to delineate clearly the access levels of an employee, and that a photo also be present on the ID to ensure its use by the rightful owner only.	5.3.3
Venues implement mail-handling security policies based upon guidance by the United States Postal Service.	5.3.4
Every venue has an incident response plan, at minimum formalizing in writing the existing unwritten plans.	5.4.1
Incident response plan policies and procedures to be drilled regularly.	5.4.1
Government agency best practices to be incorporated into [the venue's] incident response plans as appropriate.	5.4.1
Evacuation and shelter-in-place plans to be a core component of the security incident plans developed to support response capabilities.	5.4.1
A plan for handling the possibility of mass fatalities to be developed.	5.4.1
Venues develop procedures and metrics for quickly determining whether an evacuation is necessary.	5.4.2
Venues maintain statistics on end of event clearance time, in order to estimate how quickly an evacuation might be possible.	5.4.2
Venues prioritize development of specific incident plans based on their potential threat as identified in the risk assessment.	5.4.3
Venues develop comprehensive evacuation plans.	5.4.3
Venue use tabletop exercises as a way to test and develop incident management plans.	5.4.3

Venues participate in tabletop exercises with quantifiable metrics of performance.	5.4.3
Tabletop exercises be as realistic as possible.	5.4.3
The security management of a venue includes venue management in incident response planning.	5.4.3
Recommended	
Some assigned staff [in parking areas] include patrols of trained security or law enforcement personnel.	5.1.1
Patrols [in parking lots] be on foot and visit locations in random order.	5.1.1
All [parking] lots be surrounded by physical infrastructure such as fences, trees or walls, and that a network of Closed Circuit Television (CCTV) cameras be used to support monitoring and response.	5.1.1
Vehicles be kept at least 100 feet away from the facility whenever possible.	5.1.1
Venues use clear garbage cans with clear liners and have security personnel check them regularly during an event.	5.1.1
All vendors provide a list of personnel and their vehicles, plate numbers, and other information for verification.	5.1.3
Access for mail, deliveries, and non-essential repairs be cut off well in advance of the event start time.	5.1.3
Some method is employed to lessen the risk that a bag could be used as a container to deliver an IED.	5.2.1

Simulation and modeling be used to understand and project variations in screening, and in patron behavior.	5.2.1
Venues attempt to modify fan behavior to reduce queue lines and track the success of various [incentive] programs.	5.2.1
Venues set and meet queue size goals.	5.2.1
Vehicle screening includes a survey of the vehicle undercarriage as well as of the vehicle contents including the trunk of any vehicle and both the inside and cab of the truck or trailer.	5.2.2
Delivery vehicles to be screened for explosives using the K-9 unit if one is available.	5.2.2
Delivery vehicles to be swiped for the detection of explosive materials if no K-9 unit is available.	5.2.2
The screening of media trucks includes a survey of the vehicle's contents.	5.2.3
Cameras [placed in the middle security zone] to be monitored at the command center.	5.2.4
All personnel monitoring the cameras to be trained in how to detect suspicious activity and behavior.	5.2.4
Cameras to be trained on key air intake and electrical delivery systems so as to help harden security against the introduction of chemical or biological agents into the system or disrupting venue power.	5.2.4
The plan [defining areas and access points for all personnel within the hierarchy] corresponds to key-card level access, if such a system is in place.	5.3.3

Certain venues with unique footprints and appropriate budgets incorporate alarm systems that trigger when unauthorized entry is made through access points within the inner zone.	5.3.3
Smart card technology be used, since this technology can assist in tracking employee movements and monitoring for suspicious behavior.	5.3.3
Venues review the protocol concerning who gets what kind of credentials and how those are verified.	5.3.3
Venues establish food security policies which address the entire supply chain beyond just the inner security zone.	5.3.4
Venues try to minimize the number of decisions that are not predetermined.	5.4.2
Testing of [evacuation] procedures be done via tabletop exercises, and also that plans be developed in consultation with public partners.	5.4.2
Venues use the tools at their disposal to prepare fans for potential evacuation before the start of an event.	5.4.2
Venues place staff in positions to assist patrons needing to move throughout the venue.	5.4.2
If these staff [those assisting patrons needing to move] are not security personnel they still receive briefings and training on procedures for an evacuation.	5.4.2
Venues monitor major egress routes for anomalies throughout an event.	5.4.2
Venues coordinate with local authorities, especially transit agencies, to be sure that crowds can disperse quickly in both evacuation and normal end of event scenarios.	5.4.2
Venues monitor and sweep outside areas where large numbers of fans are likely to congregate or pass through after an event.	5.4.2

Venues develop a set of general response principles that can then be applied to whatever incidents do develop, in combination with specific response plans.	5.4.3
Venue managers be prepared for what to say and do publicly in an emergency.	5.4.3
Security at a venue advise venue management, which is usually civilian, how to interact with outside agencies in the event that these agencies must come in and take over command of venue security.	5.4.3
Suggested	
Some of [the staff assigned to parking lots] to be in plain clothes to allow for their integration into parking lot activities without drawing the attention of suspicious persons and that some of them be trained in behavioral assessment.	5.1.1
Vehicles parking [more than 100 feet] away from the structure [also] be checked utilizing a detailed vehicle security screening process [in addition to vehicles within 100 feet].	5.1.1
Venues consider integrating license plate reader devices at parking access points to identify potential threats.	5.1.1
Venues with larger budgets devoted to security development consider the following pilot program on a small scale: Set up target vehicle parking areas in which vehicles in high risk of drawing criminal activity or identified by intelligence reports may be located in sight of parking lot staff. Alternatively, staff may be assigned to monitor vehicles if parking in these target areas is not possible.	5.1.1
Visiting teams be inspected off-site [for sports events].	5.1.3

Venues located near airports and venues having established flight takeoff or approach paths over them coordinate with airport officials and the Federal Aviation Administration to see if alternative paths are available during event-day operations.	5.1.4
A venue consider using a combination of methods in patron screening in order to take advantage of the value of the most effective screening techniques, and the speed of alternative techniques.	5.2.1
Venues consider rotating staff in and out of the busiest and most stressful patron screening jobs.	5.2.1
Guidelines to limit the size of bags be established, taking into account the needs of patrons along with the venue risk assessment.	5.2.1
Venues provide incentives for those coming without bags, for instance moving those patrons to faster-moving inspection lanes.	5.2.1
Venues consider employing more patron screeners and/or training screeners more thoroughly to maximize their effectiveness and speed.	5.2.1
Venues consider developing incentives [for patrons] to arrive earlier and/or arrive at less busy gates.	5.2.1
Venues consider employing a patron screening strategy that is responsive to queue size; for example switching procedures or randomizing procedures if the size gets too large.	5.2.1
Venues consider cutting off access to a gate if the queue size at the gate gets too large.	5.2.1
Venues study and potentially pilot a program for expedited screening of season ticket holders and other trusted patrons, possibly patterned after the TSA PreCheck program.	5.2.1

Media personnel be screened separately in order to allow a careful and attentive screening of equipment and credentials.	5.2.3
Venues may wish to consider a separate entrance for media personnel access.	5.2.3
A combination of devoted camera and positioned security personnel at key intakes or electrical stations be deployed.	5.2.4
The venue consider moving cameras from time to time, perhaps using randomized placement.	5.2.4
Venues consider utilizing a software tool that can identify unattended bags.	5.2.4
Venues with either mutual aid agreements or the appropriate budget might consider the use of local law enforcement bomb or K-9 units to perform sweeps for the venue.	5.2.5
Certain venues also consider investing in their own K-9 unit for both scheduled and random sweeps prior to the event.	5.2.5
Venues consider incorporating camera facial recognition software if budget and threat determination warrant the expense.	5.3.1
Venues make temporary credentials substantially different from one event to another.	5.3.3
Venues implement simple policies including thoroughly securing food and ice storage areas and conducting in-house health inspections in addition to the locally required inspections, while more in-depth policies may include strict procedures for inspecting food containers prior to opening to ensure tampering did not occur.	5.3.4

Venues consider conducting anonymous surveys of staff to understand the impact of potential staffing reductions during incidents that match the threats identified in the risk assessment.	5.4.2
Venues study how well stadium employees and patrons react if an exit is closed or normal stadium egress is hindered in some limited manner (e.g. temporary construction or malfunction) and assess the impact on clearance time.	5.4.2
Venues consider involving outside groups such as law enforcement, fire, and OEM in any tabletop exercises they develop.	5.4.3
Venues consider the development of procedures to follow when planning for unique events that may require increased security.	5.4.3

Appendix – Chapter 5

This appendix provides significant additional details on security operations and incident response. The security operations information has sections related to General issues, and issues specific to the three security layers (Outer Zone, Middle Zone, and Inner Zone). Additional information on patron screening techniques and metrics is presented in the Patron Access section. The incident response information is organized into sections on Evacuation and Planning.

General

- DHS Best Practices for Active Shooter, Bomb Threat, Area Searching, and Area Sweeps can be used to create standard operating procedures for the venue. These Best Practices create layers of security and response considerations by venue staff that, if adopted, enhances the security profile of the venue.
- All implemented technologies can be incorporated into an overall maintenance program to ensure all equipment used for security purposes maintains its level of reliability.
- An understanding and description of the failure rates or strength ratings can be maintained for each technology. For example, how much force causes bollards to fail? What is the optimal

distance between bollards? How often do CCTV cameras fail? How often do access control devices fail to send an alarm? Are camera images clear enough to identify persons?

- In addition to inherent technology vulnerabilities, the environment and humans may also cause variations in technology reliability. These issues also can be identified. For example, access control technologies may have increased false alarms when it rains. This situation could raise the number of staff required to monitor CCTV camera feeds.
- All deliveries and services can be scheduled outside of event-day operations when possible. This includes trash collection, mail delivery, armed guard services and repair services. Vendors and service providers can display proper credentials.
- Venues might consider using PO Boxes and conducting mail inspection at a separate facility.
- Vehicle checks may include bomb-sniffing dogs, undercarriage mirrors, trunk checks, staff observing occupant behavior, requiring parking passes, requesting tickets be shown, inspecting tailgating equipment, etc.

Outer Zone

- Randomized patrols may be necessary as set patrols can be monitored by terrorists.
- Plans can clearly mark the various security zones used by the venue.
- Develop pre-event checks for the outer zone to ensure areas are secure prior to opening the parking lots.
- Implement physical measures that would reduce or eliminate cascading effects due to devices exploding at adjacent infrastructures to mitigate consequences and reduce risk. Physical measures include installation of blast resistant walls and windows within a public transit station on site, increasing the thickness of concrete walls between infrastructures, etc.
- Venues might consider utilizing a site away from the venue to conduct vendor delivery vehicle checks.
- Resources focused specifically on parking: The DHS First Observer program was created with a specific component geared toward major sport venues and the parking services industry operating at those venues. As noted in the First Observer program, the parking industry is recognized as one of the top emerging threats of terrorism. The program introduces the First Observer acronym, "OAR" (Observe, Assess and Report). Additionally, the training includes, "The Fatal Five," (Firearms, Knives, Package Bombs, Vehicle Bombs, Chemical /

Biological and Radiological / Nuclear) and "Seven Signs or Signals of Terrorism."

Middle Zone

- New technology exists that may allow for cameras and or sensors to be placed in fixed or mobile sites that can detect unattended bags.
- Some venues found that establishing their own K-9 unit is cheaper over the long run than paying for temporary resources.
- Venues may consider exit lane access control systems. These systems may allow for staff to be assigned elsewhere while ensuring patrons or persons do not enter/re-enter the venue during egress.

Inner Zone

- Venues may consider purchasing mail screening technologies that are capable of handling large packages.

- Visitors who require access to areas requiring authorization may be assigned a security detail to ensure they accomplish their purpose and leave the area when complete. Examples of such visits include equipment repair within the command center, media filming at the loading docks, etc.

- Access control systems may include varying levels of access and credentialing.

- DHS has provided a number of useful suggestions for developing and implementing credentialing procedures. See "Sports Venue Credentialing Guide," Department of Homeland Security, May, 2012.

Patron Access

- In general, a patron screening strategy is only as effective as its effectiveness at its weakest times. Terrorists might try to enter the venue during the times of worst screening effectiveness, and the threat is heightened when terrorists can easily predict when a screening strategy will be the weakest.
- To reduce the queue outside of gates, venues may try modifying patron behavior by

directing crowds to shorter lines at the same or different gates, implementing incentive programs such as pre-event entertainment, free or reduced cost for food and drink, opening gates to ticket holder groups at varying times, implementing communication technologies in the parking lots to announce or show wait times by gate, banning pre- event activities, banning bags, etc.

- DHS has provided a number of useful suggestions for developing and implementing bag search procedures. See "Sports Venue Bag Search Procedures Guide," Department of Homeland Security, May, 2012.
- Venues might consider tracking the confiscated items caught by each screening method. Such data can help in understanding the success rates of different security tactics.
- If a venue utilizes randomization in patron screening techniques, then a good measure of effectiveness is the distribution of patron screening techniques when they are most skewed to the least effective techniques.
- When testing patron screening effectiveness, the tests can occur at different times in order to investigate if screening is more effective or more likely less effective, closer to the start of an event.
- Venues might consider using simulation software to help guide their decision making process when it comes to patron screening. Such software can help answer questions such as:
    - Under strategy A, how long will lines get?
    - Under strategy B, when will the queue clear?
- Throughput is likely dependent on weather, event time, crowd demographics and other factors. By creating a database with throughput information along with these factors, a venue might be able to predict what throughput will be like, and adjust staffing and patron screening decisions accordingly.
- Queue size is somewhat difficult to measure directly, but not all that hard to estimate fairly accurately in the following way:
    - A venue may have employees stand in line and measure how long it takes to get to

the front of the line. The venue may also keep track of how many patrons enter through each gate each minute. The venue may then combine this information to determine queue size. For example, if (at a specific gate) at 12:40 it takes 3 minutes to reach the front of the line, and throughput was 150 persons at 12:40 and 12:41 and 200 persons at 12:42, then the size of the queue at 12:40 was roughly 150+150+200=500 people.

TSA Pre-Check Program

The Pre-Check program offers airline passengers (typically frequent flyers) the opportunity for expedited screening including no shoes, belt, jacket, liquids, or laptop removal required. To qualify, passengers must pass a background check (including finger printing and in-person enrollment) and pay an up-front fee of $85 for a five-year term. For an eligible passenger, TSA embeds information in the bar code of the passenger's boarding pass, and the passenger may be directed to an expedited screening lane at selected airports.

While a program for season ticket holders and other trusted patrons analogous to the TSA Pre-Check program seems desirable, there is not a simple mapping to stadium security screening. For one thing, event tickets, unlike airline tickets, often change hands (in many cases multiple times) between the original purchaser and the ultimate user/patron. This means that some sort of authentication step would be required, e.g. patron's identity authenticated at the entrance gate via driver license check, a database lookup, or biometric technology. The time taken by this extra step could exceed the time saved by expedited screening. It is also not clear whether participating patrons could completely forgo screening (pat-downs, wanding, or magnetometer checks), or just have access to a shorter queue. In any case, the TSA Pre-Check and other similar programs initiated by Customs and Border Protection may evolve in such a way that sports venues ultimately can pattern trusted patron programs after them. Alternatively, venues might find other ways in which to shorten the inspection time required for trusted patrons, thus shortening inspection time overall.

Magnetometers

Magnetometers pose a risk as an obstruction during an evacuation. A venue might consider the following steps to mitigate this risk:

- Remove the magnetometers once the event has begun and most patrons are in the venue.

- Put magnetometers on wheels to facilitate moving them. If a magnetometer is on wheels, a step underneath the magnetometer can be used to ensure that a patron's entire body, including shoes and feet, must pass through the area screened by the magnetometer.

- Tape down electrical cords around the magnetometers so that patrons do not trip on them. This is important for general safety, not just for evacuation planning. Alternatively, battery powered magnetometers might be used.

- Plan what to do with magnetometers in the event of an evacuation occurring while a large number of patrons are still entering the venue. Train staff to implement this plan quickly, and make sure that front-line staff will be informed of an evacuation order as soon as possible.

Incident Response:

Evacuation

- Fan awareness of evacuation procedures, or at the very least the priming of fans to mentally prepare for the possibility of an evacuation, is important. A venue could try different methods of informing fans of emergency evacuation procedures before or during an event. They could then use post-event online surveys to gauge the effectiveness of different methods. These measures of effectiveness could then be used by security to argue for the importance of airing a message about emergency procedures (e.g. put security information on message boards close to the start of an event).

- Secret shoppers can test the amount of direction and guidance provided by ushers and security personnel when arriving at the venue and travelling to one's seat. Fan surveys on usher interaction can also give an indication of performance. As noted in the chapter, this pre-event guidance can be important in establishing a relationship that could be useful during an emergency evacuation.

- Data on event clearance times can be stored and analyzed to notice trends. Differences based on weather, event time, etc. can be noted. These differences can then be used by

decision makers when deciding whether to evacuate. When making evacuation decisions, it is important to know what an evacuation might look like, not for an average event, but for an event of the type currently taking place.

- Cameras or properly placed personnel can identify bottlenecks in patron flow out of the stadium.

- Modeling software can be used to simulate an evacuation. This software can be used to estimate how long it takes to clear the venue, and to identify potential bottlenecks. The model can be validated by checking model output with the actual reality of what occurred at the end of events. Once validated, the model can be used to answer various questions using "what if" scenarios that can help in security planning decisions. For example, the model could help at least estimate answers to questions such as:
  - If Gate C is closed, how much longer would an evacuation take?
  - If the concourse is widened by 5 feet, how would this affect evacuation times?
  - How long would an evacuation take with 20,000 fans? 25,000 fans? 30,000 fans? Etc.

- The use of modeling software and real-life observation can be extended to areas outside of the venue proper to predict where fans might congregate or bottlenecks might occur outside the venue during an emergency. These are areas that can then be monitored during an event.

- Especially for venues where a large number of fans use public transportation, a MOU might be developed with local public transportation detailing evacuation plans. Drills can be run to determine potential performance. For example, for a venue near a city train line, it could be tested how quickly trains can be directed to arrive at the station to remove fans without prior warning. This is somewhat different from the everyday scenario where extra trains might be allotted, but the time at which these trains will be needed can be predicted by paying attention during the event.

- Venues are encouraged to develop a comprehensive transportation standard operating procedure (SOP) to address not only evacuation of the venue but to ensure egress of parking lots as well.

Planning:

- Protocols can be developed for incidents that will occur from time to time at the stadium and could turn into a more serious incident. For example, one protocol could be the procedure for identifying a suspicious package.
- If the response is too drastic to these serious but not yet emergency scenarios, security runs the risk of potential threats not being reported to security or not being dealt with according to protocol. On the other hand, if the response is not serious enough, security runs the risk of jeopardizing safety.
- Incident Response Plans can be developed in coordination with some key stakeholders including first responders such as bomb squads, law enforcement, fire and medical services, etc. to ensure plans meet requirements, fit into local response plans and address the necessary activities for proper response.

Chapter 6 – Training and Evaluation

Introduction

Training and exercise planning covers the types of training required for all staff. This includes first responders who staff the venue and potentially local jurisdiction law enforcement, fire services, and medical teams that may be called during an emergency. Venue security and guest services staff may be in-house or contracted from a provider outside of the venue. Standards and procedures for training and quality evaluation may differ between in-house staff and contract staff. Training also includes patron training on topics such as evacuation procedures, screening processes, and other venue management issues.

Questions	Metric
Have you outlined staff types or security team roles so as to better plan training and exercises?	Y/N

Have you considered differences in training standards between in-house and contracted staff?	Y/N
Have you implemented patron training programs to better prepare them for action during emergencies?	Y/N

6.1 Exercise and Education

6.1.1 In-House vs. Contract Staff

The distinction in this chapter between in-house and contracted security personnel is significant for the following reasons. Consistent concerns from security professionals include: a) the quality of guard performance when low-paid guards are used, b) the lack of applicable guard skills even when guards are certified at the state level and working through a contracted service, and c) the ability to ascertain contract guard quality "beyond the contract," i.e. performance beyond the minimum of what is strictly written in the contract. It is prudent to understand the different challenges to assessing and assuring quality between long-tenured in-house security personnel and high-turnover, low-paid, seasonal, and contracted guards. Two other factors also play into this distinction - owners' budget and venue security director's preference. While continued investment into robust quality assurance may be perceived on the part of venue operators as an unnecessary cost, it may be presented to them not merely as a government mandate, but also as a mechanism to help assure value of service. Establishing quality assurance protocols helps venue operators to receive a fair return on investment for their contracted services.

It is ***strongly recommended*** that security managers at sports venues know or be able to access their state's guard certification requirements, especially when hiring contracted security vendors. Venue operators can research security contractors and request documentation regarding their state certification. As part of venue security hiring practices, protocol can be established for purposes of certification verification. In addition, venue operators can request language to be added to contracts with security vendors to allow venues to perform quality assurance checks. These resources apply to both in-house and contracted security.

Questions	Metric
Do you have a program in place to assure certification?	Y/N

Do you know the state requirements for guards?	Y/N
Has your contractor satisfied state requirements for guards?	Y/N
Does your contract specify your right to make quality assurance checks on services provided?	Y/N

6.1.2 Minimum Competency Standards

It is ***strongly recommended*** that the venue Director of Security establish a set of minimum competency standards for security practices. It is ***strongly recommended*** that these minimum standards be applicable to all employees at the venue. It is ***strongly recommended*** that venues establish an introductory tour and assessment for contract guards so as to increase contract guards' familiarity with the venue and its unique features as part of a comprehensive training program (see following section). It is ***recommended*** that various levels of higher proficiency in security procedures be instituted as well. It is ***recommended*** that the positions be clearly defined as to which positions this tiered set of practices applies.

No national standards exist for the training of security guards – each state retains its own requirements. Often, even available quality guard training programs do not offer a curriculum that is appropriate to sport-venue security. Therefore it often falls upon the security director or operations manager to assess whether minimum competency standards are present amongst staff employed at the sports venue. There are a variety of resources for assuring quality minimum competencies. In addition, it is ***recommended*** that security managers consider implementing short (5 minute) refresher training modules for both in-house and contract security on a daily or weekly basis.

Questions	Metric
Are your security guards familiar with the details of your venue?	Y/N
Do you have short re-fresher training modules available to quiz security staff? If so, how often do you run refresher training?	Y/N , Freq.

6.1.3 Training

It is ***strongly recommended*** that training be thought of as a constant activity that helps keep venue staff alert, informed, and engaged through the acquisition of new information. It is ***strongly recommended*** that all venue staff, including security staff, both contracted and in– house, guest services staff, maintenance staff, custodial personnel, parking staff, and food vendors receive some level of training designed by the venue security director. It is ***strongly recommended*** that the training include both an educational component and a testing component. For some staff a practical exam may be appropriate. It is ***strongly recommended*** that the results of training examinations be recorded and maintained as part of employee files. It is ***strongly recommended*** that refresher training sessions be held regularly. It is ***recommended*** that once every six months is an appropriate time course for training refresher courses.

Venue security might want to consider that training may not be sufficient if it is a one-time event during the pre-season for sports venues. The security director or operations manager could attempt to make training an environment where personnel can shine rather than a dry, mind-numbing repetitive exercise. It is ***recommended*** that venue operators consider the following in order to assure their training be both ongoing and dynamic. First, many resources are available to the local security director through federal agencies (see resource recommendations in chapter appendix). Second, mutual aid agreements between the venue operator or security director and local law enforcement can include tabletop exercises that provide benefits for both parties. The venue will be very familiar to local officers who respond to an incident if they have participated in multiple drill scenarios at the venue previously. Local law enforcement will be happy to check-off required annual training modules if training can be done at local venues that provide the "real world" feel so necessary for teachable moments within the scenario. Finally, these coordinated training efforts help to not only establish strong positive ties between the venue and local fire and law enforcement services, but also the relationship can speed up effective coordinated incident management during actual incidents.

It is difficult to assess how effective training is and many people who develop training actually have no background in assessment. Testing and evaluation of the application of training during an actual incident is preferable, but one hopes that this kind of evaluation opportunity never happens. Possible alternative methodologies for assessment include: multiple question tests

following training, secret shoppers to test on the job, supervisor checks during an event, and review of procedures just before an event. Data from patrons might also be used to evaluate training. For example, if training has been conducted on the proper use of force, then the number of excessive use of force complaints could give an indicator of training effectiveness. It is ***recommended*** that a challenge program be used – if an employee sees someone carrying out a procedure incorrectly and reports it, the employee is rewarded. In addition, when an employee notices that another employee has correctly followed procedure, they can also be rewarded for their knowledge and awareness. Another training incentive involves timing how long it takes employees to notice an anomaly (e.g. the sooner an employee spots a hidden bag with a fake bomb, the higher the reward). Financial rewards and other forms of recognition (e.g. a symbol to wear on a uniform) can be used. These and other QA methods can be conducted continuously during the event season as part of the security plan (see Section 6.2). During the pre-season or off-season, venue security directors might be encouraged to reach out to DHS resources so as to help vary or add robustness to training.

Questions	Metric
Does your security plan integrate training as a part of quality assurance?	Y/N
Is your security director aware of federal agency resources available to the venue for the purposes of training?	Y/N
Are the results of training recorded and kept as part of employee files?	Y/N
Are employees rewarded for performance in spotting potential security breaches? If so, what percentage of employees has been so rewarded?	Y/N , %
How long does it take employees to find a hidden fake bomb? Is the length of time to find such a bomb lower than it was a year ago?	#, Y/N
Is local law enforcement involved in tabletop exercises? If so, in what percentage of such exercises?	Y/N , %

6.1.4 Schedule of Training

It is ***strongly recommended*** that pre-season training occur and at minimum include customer service training but ideally also include higher level incident response training for all levels of employees. Federal agency training resources could be tapped for this training if a venue operator is unsure where to get training experts. A main point regarding exercises is that it is a cycle and it can be never ending if it is done correctly. Exercise objectives can be stated as the first step. The goal is for the scenario to fit the objectives. It is ***recommended*** that some exercises endeavor to involve as many players, entities, and partners as possible. There could be a focus on follow-up to exercises for meaningful lessons and continuity. This could be much more valuable than large volumes of exercises checked off a list. After Action Reports (AARs) are very important if used properly and thus AARs are ***strongly recommended***. Some organizations may not want to identify weaknesses or areas for improvement in AARs since they will be documented and could be held against them. If AARs are not used properly, noting deficiencies and then following up with action to improve deficiencies prior to the next exercise or event, the exercise is not useful and it is just a case of going through the motions. It is ***strongly recommended*** that the AAR and discovered weaknesses or areas for improvement be used to help to drive the objectives for the next training exercise. It is ***recommended*** that training be an ongoing process that can be budgeted on an annual basis.

It is ***recommended*** that short, 5 minute, topic training sessions be given 15 minutes prior to an event (just-in-time training) to keep information fresh, in addition to the semi-annual refresher training suggested earlier. It could be that frequency of education and training for entry level employees can be decreased as long as supervisory level training is defined as education plus experience and supervisors are active in propping up the front line. It is ***suggested*** that certain facilities could consider utilizing a steward/apprentice system (see Section 6.2.2). Training frequency might also depend on the frequency of the event (81 games versus 1 event a season). Frequency might also be determined by classification of employee (higher for those whose main role is security, lower for those whose role is less security focused).

Questions	Metric
Does your annual budget contain a line for training?	Y/N
What percentage of your employees is involved in the exercises that use the largest number of employees?	%
What percentage of exercises involves at least 30% of employees?	%
Does your plan have built-in metrics to assess the effectiveness of your training?	Y/N
Do you perform post-event debriefings ("hot washes") with metrics for learning and accountability?	Y/N

Open Ended Question	Anticipated Response
How are After Action Reports (AARs) utilized?	Described use of AARs

6.1.5 Patron Education

It is ***strongly recommended*** that patrons of a venue be educated on emergency procedures prior to the start of each event. Emergency procedure education includes evacuation training and shelter-in-place instructions. It is ***recommended*** that training be in the form of a brief informational video and/or a printed pamphlet describing evacuation routes and instructions for sheltering in place. It is ***suggested*** that venues consider providing additional materials for educating patrons on security screening processes. This approach is particularly valid if the screening process policy has been recently updated and patrons are unfamiliar with the new policy. Educating patrons on the new screening process will aid in obtaining the cooperation, understanding, and patience of the crowd; it may also help to increase fan satisfaction.

Other patron education campaigns of which "see something, say something" is a successful example, help the public become a positive and active component of security. A similar plan can be implemented within sports venues with the added dimension of instructing patrons how to calmly alert venue security about what exactly they have observed. It is ***suggested*** that other areas of venue security can also positively benefit from proper patron education. This includes utilizing signage and the PA system to inform patrons about expected behavior within the venue

as well as what they can expect regarding access point inspections. Venues can also attempt to make patron entry more efficient by educating patrons to arrive early or even to provide incentives to arrive within a particular time range.

Questions	Metric
Do you attempt to educate patrons concerning evacuation procedures? Screening procedures?	Y/N, Y/N
Do you have a way of testing the effectiveness of your patron education techniques? If so, what is the percentage of patrons that retain the information?	Y/N , %

Open Ended Question	Anticipated Response
On what other topics besides evacuation and screening do you try to educate patrons?	Topics for patron education
Which technologies (e.g. PA system, Videos, Signage, Social Media, etc.) are most effective for educating patrons for which purposes?	Discussion of the educational effectiveness of technologies

6.2 Quality Assurance

Quality assurance as applied to security is the systematic maintenance of a desired level of quality in a security plan, component, policy, or technology. It is not enough to choose vetted procedures and technologies at a particular venue; it is also necessary to install quality assurance into the venue's security infrastructure. Security professionals can integrate quality assurance into every aspect of their security plan. Quality assurance maintains and measures the effectiveness of security plans. For example, general maintenance and periodic testing of security equipment are the systematic maintenance components of quality assurance programs. Another process that is part of every QA plan is to specify a system for reviewing various commitments to ensure that they are executed as described in the plan, e.g. did the fire extinguisher contractor check everything per the agreed schedule? Was the vendor's security plan reviewed annually?

It is ***suggested*** that venue operators utilize randomization while applying QA to their security personnel. Random numbers can be useful when attempting to keep the assessment of operations fresh. When we discuss single numbers, a random number is one that is drawn from a set of possible values, each of which is equally probable. When discussing a sequence of random numbers, each number drawn must be statistically independent of the others. Label sections of a venue operation with specific values (e.g. West Gate = 3, upper concourse = 8, media entrance = 17). Then, use a freely available web-based random number generator to generate a value corresponding to the venue section; the result being a random choice of which section to assess for quality during daily rounds. Randomization provides for a more authentic observation of personnel practices but also helps to bewilder potential attackers as to the venue's "normal" operating procedures. It can be a good idea for a sports venue to have a written quality assurance plan in place. Usage of this plan can be increased through familiarity and understanding on the part of venue security and staff via routine practice. In addition, the quality assurance plan can incorporate metrics so as to compare results between QA performance checks.

Questions	Metric
Do you have a quality assurance plan in place?	Y/N
What percentage of the staff is briefed on the quality assurance plan?	%
Is relevant staff quizzed on their knowledge of the quality assurance plan?	Y/N
If so, what percent of quiz questions do they answer correctly?	%

6.2.1 Front-Line Screening

Front-line quality is a significant factor in a venue's security system. Maintaining high quality at this access point can be challenging for venue operators for the following reasons. Pressures acting upon the front line include fan numbers and behavior (surges of potentially unruly fans near the start of event time), lack of investment in the needed number of staff, league pressures to not diminish "the fan experience", and challenges inherent to entry-level or seasonal workers. The following are resources to assure quality in a venue's front line performance. It is ***strongly recommended*** that every sports venue security plan incorporate some form of basic red teaming

to assess their front line personnel. A common and effective tool for front line staff is the use of a wand since it often provides greater assurance than a simple pat-down while also being more budget-friendly than full-body magnetometers. It is ***recommended*** for venues using wands to develop testing protocols for wands and their users including basic strategies for read-teaming. Venues can either develop these testing protocols in-house or in conjunction with their preferred contracted security staff. Venues can consider establishing base-line times to complete an effective wanding, how these times differ due to seasonal varieties of patron clothing, and differences in effective wanding times at different intervals prior to the event (two hours prior versus 15 minutes prior). Establishing relationships with and observing other venue's protocols for wanding may also help increase your staff's effectiveness.

It is ***suggested*** that venues consider introducing protocols to schedule varied forms of in-house search assessments. Quality assessments can be greatly enhanced by establishing protocols to not only observe but also to retrain and correct improper security procedures on the spot. These assessments also provide an opportunity to recognize and reward good performance.

Questions	Metric
Do you perform red teaming at your facility?	Y/N
Do you have protocols in place that work to retrain and correct behavior at the front line?	Y/N
Do you have regularly scheduled and varied exercises in place for assessing quality of in-house search?	Y/N

6.2.2 Auditing via Your Hierarchy

Venues usually have an organizational hierarchy. Perhaps it is ownership, management, security director, security supervisors, and front-line staff. It could also be ownership, operations manager working in conjunction with contracted company's security director, an assistant supervisor, and ushers. An organizational hierarchy can be harnessed to incorporate quality assurance for various levels of responsibility at venues helping to strengthen security practices. Regardless of the particular structure, there are a variety of resources for assuring quality in personnel training by utilizing the installed hierarchy. Having a clearly drawn and readily

accessible organizational chart supports efficient communication and clarifies responsibility for auditing performance, and is thus ***strongly recommended***. In addition, this chart can help to specify the relationships between venue security personnel and any contracted security staff and management. Venues can also establish metrics for supervisors and managers to use when auditing performance by front line staff.

On-going supervision of security staff requires a strong and skilled manager. The security staff manager must be present constantly, and must oversee the activities of security staff whether they are venue employees or contractors. No matter how many good security staff a venue has, without a strong staff manager problems can arise. A good manager will have not only the required training and experience, but will also exhibit strong leadership qualities. It is ***strongly recommended*** that all aspects of the performance of security management (organization skill, supervisory capabilities, leadership) be audited and rewarded appropriately by whomever the manager reports to in the organization.

It is ***suggested*** that venues also consider including a mentor/apprentice program between veteran staffers and new hires. Along with the inherent training benefits of this dynamic comes a useful auditing tool: veterans can assess whether new hires are learning protocol and culture, while new hires can audit their mentors so that their actions match what they preach.

Questions	Metric
Do you have a clear and readily available organizational chart?	Y/N
Does this chart specify the relationship between contract staff and venue operators?	Y/N
Is there a procedure in place for supervisors to audit front-line staff? Is there a procedure for management to audit supervisors?	Y/N
Have you paired veteran staff and younger staff in pseudo apprentice-style relationships?	Y/N

6.3 Training and Evaluation: Key Points

- Establishing quality assurance protocols helps venue operators assess and assure the quality performance of long-tenured in-house security personnel as well as entry-level, seasonal, and contracted guards who may be prone to high turnover.
- The security director or operations manager can assess whether minimum competency standards are maintained by staff employed at the sports venue.
- All venue staff can receive some level of training, designed by the venue security director that includes both an educational component and a testing component.
- Training, including refresher courses and brief "just in time" sessions, is continuous.
- Training frequency might depend on the frequency of events per season or by the security role of the employee.
- If AARs are not used properly, to note deficiencies and follow up with action to improve deficiencies, an exercise may not be useful.
- Patrons of a venue can be educated on emergency procedures such as evacuation and shelter-in-place, on security screening processes, and on ways to become a positive and active component of security.
- Quality assurance maintains and measures the effectiveness of security plans and can be integrated into every aspect of the security plan.
- Resources to assure quality in a venue's front-line performance include basic red teaming, in-house search assessments, and protocols to observe and retrain on the spot to correct improper security procedures.
- Randomization of spot checks can be useful when attempting to keep the performance of front-line staff fresh.
- An organizational chart will help support efficient communication, clarify responsibility for auditing performance, and specify the relationships between venue security personnel and any contracted security staff and management.

6.4 Recommendations – Chapter 6 Training and Evaluation

Chapter 6 – Training & Evaluation	

Strongly Recommended	Section
Security managers at sports venues know or be able to access their state's guard certification requirements, especially when hiring contracted security vendors.	6.1.1
The venue security director establish a set of minimum competency standards for security practices.	6.1.2
Minimum competency standards be applicable to all employees at a venue.	6.1.2
Venues establish an introductory tour and assessment for contract guards so as to increase contract guards' familiarity with the venue and its unique features as part of a comprehensive training program.	6.1.2
Training be thought of as a constant activity that helps keep venue staff alert, informed, and engaged through the acquisition of new information.	6.1.3
All venue staff, including security staff, both contracted and in–house, guest services staff, maintenance staff, custodial personnel, parking staff, and food vendors receive some level of training designed by the venue security director.	6.1.3
Training include both an educational component and a testing component.	6.1.3
The results of training examinations be recorded and maintained as part of employee files.	6.1.3
Refresher training sessions be held regularly.	6.1.3

Pre-season training occur and at minimum include customer service training but ideally also include higher level incident response training for all levels of employees.	6.1.4
After Action Reports (AARs) be used properly, i.e. noting deficiencies and then following up with action (accountability) to improve deficiencies prior to the next exercise or event.	6.1.4
The AAR and discovered areas of weaknesses or areas for improvement	6.1.4
be used to drive the objectives for the next training exercise.	
Patrons of a venue be educated on emergency procedures prior to the start of each event.	6.1.5
Every sport venue security plan incorporate some form of basic red teaming to assess their front-line personnel.	6.2.1
A venue have a clearly drawn and readily accessible organizational chart to clarify responsibility for auditing performance.	6.2.2
All aspects of the performance of security management (organization skill, supervisory capabilities, and leadership) be audited and rewarded appropriately by whomever the manager reports to in the organization.	6.2.2
Recommended	
Various levels of higher proficiency [beyond minimum competency] in security procedures be instituted.	6.1.2
The positions be clearly defined as to which positions this tiered set of [minimum to higher-level] practices applies.	6.1.2

Security managers consider implementing short (5-minute) refresher training modules for both in-house and contract security on a daily or weekly basis.	6.1.2
Once every six months is an appropriate timetable for training refresher courses.	6.1.3
Venue operators consider: Many resources are available to the local security director through federal agencies.	6.1.3
Venue operators consider: Mutual aid agreements between the venue operator or security director and local law enforcement that can include tabletop exercises to provide benefits for both parties.	6.1.3
Venue operators consider: Coordinated training efforts help to not only establish strong positive ties between the venue and local fire and law enforcement services, but also the relationship can speed up effective coordinated incident management during actual incidents.	6.1.3
A challenge program be used – if an employee sees someone carrying out a procedure incorrectly and reports it, the employee is rewarded. In addition, when an employee notices that another employee has correctly followed procedure, they can also be rewarded for their knowledge and awareness.	6.1.3
Some exercises endeavor to involve as many players, entities, partners, and stakeholders as possible.	6.1.4
Training be an ongoing process that can be budgeted on an annual basis.	6.1.4
Short, 5-minute, topic training sessions be given 15 minutes prior to an event (just-in-time training) to keep information fresh, in addition to the semi-annual refresher training.	6.1.4

[Patron] training be in the form of a brief informational video and/or a printed pamphlet describing evacuation routes and instructions for sheltering in place.	6.1.5
Venues using wands develop testing protocols for wands and their users including basic strategies for read-teaming.	6.2.1

Suggested	
Venues consider providing additional materials for educating patrons on security screening processes.	6.1.5
Venues educate patrons by utilizing signage and the PA system to inform patrons about expected behavior within the venue as well as what they can expect regarding access point inspections.	6.1.5
Venues attempt to make patron entry more efficient by educating patrons to arrive early or even to provide incentives to arrive within a particular time range.	6.1.5
Venue operators utilize randomization while applying QA to their security personnel.	6.2
Venues introduce protocols to schedule varied forms of in-house search assessments.	6.2.1
Venues include a mentor/apprentice program between veteran staffers and new hires.	6.2.2

Appendix – Chapter 6

This appendix provides specific resources to potentially incorporate into a sports venue security plan's quality assessment practice. The areas of focus within this appendix include: red teaming, auditing via hierarchies, minimum competency standards, and schedule of training. The

examples given are purely illustrative, and are not intended to be comprehensive.

Red Teaming

- Walk up to front-line member (during a lull) and politely but directly ask them "do you know what you're looking for?" and if there is hesitation on their part, swap them out and re-train or provide a refresher on the spot so as to correct behavior.
- Using your credentials, introduce yourself to a patron a few paces before the front line and ask if you may place a tennis ball inside her purse. Alert your staff that during the next surge of patrons, they are to find this ball. Assess whether they remember to do so *and* whether they can find the item.
- Use a lesser-known employee or local security professional to attempt to enter through a side entrance or "back of the house" to see if their credentials are checked. Be sure to have this actor or yourself record specifically who failed in procedure, how it occurred, and establish an incident report. Speak to the employee immediately to rectify the behavior.
- Inside the venue exercise: Tell the particular security department or individual whom you are interested in assessing that a "white box" has been placed somewhere within the facility and that their job is to find it as quickly as possible. This exercise can also be modified with incentives: the longer it takes the security employee to find the box, the lower the financial reward. This is but one example of strategies that use games to evaluate and improve performance as outlined in other sections of this guide.

Auditing via Hierarchies

- Assign a supervisor to 3-4 ushers or front-line personnel in order to audit their performance and rectify incorrect behavior immediately. This process also can be used to verify that posts are staffed by having the supervisor use deployment sheets. Quizzing ushers or section personnel about who is working in the next section over, why, and what his or her responsibilities are in relation to theirs is also encouraged.
- Crowd managers and venue staff are usually trained to know the locations of emergency equipment such as fire extinguishers, fire hoses, pull stations and defibrillators as well as to know how to use these devices. A supervisor can quiz the staff on the locations and

operation of this emergency equipment.

- League-level random inspections of facility best practices are encouraged. At the venue level, similar random inspections by the on-site security director is also encouraged via the following examples:
    - Randomly choose one of your front-line staff to question what exactly he or she is looking for based on that day's threat profile.
    - Randomly choose one of your supervisors to provide you (from memory) all those employees who are NOT present (may be off-duty) during the particular event.
    - Randomly choose one of your ushers or inside lower-level security personnel to recite from memory who that day is in charge of security and how they would contact them if necessary.
    - Randomly visit the vendors' level of your venue and if you don't see credentials displayed, ask to see their credentials. You can also ask vendors what they would do if they receive food product that has been damaged or tampered with.

- During scheduled tabletops, schedule ownership and corporate managers to participate in scenarios so that they are forced to "take ownership" via participation and knowledge they gain through the experience. This may help them to better understand why investment in certain security practices is warranted.
- Rewarding/Disciplining – while financial rewards are certainly effective in getting lower-ranking staff to perform at a higher or required level, providing them additional responsibilities in conjunction with small financial incentives (e.g. gift card to pro shop) will provide recognition for their good performance.

Minimum Competency Standards

- Coordinate with your contracted security company manager to allow you to randomly "quiz" security company employees regarding details specific to your venue. You are not challenging their basic security competencies, but rather their knowledge of how to apply them to your specific facility.
- Ask your contracted security company manager to provide paperwork detailing guard certification competencies so that you are more familiar with what the guard is expected to already know. Refresh this knowledge applied specifically to your venue operations as

needed.

- Your in-house security staff is expected to be audited on their minimum competencies on a regular basis and can be organized in tiers to reflect your hierarchy. A security director or operations manager needs to audit to ensure that ushers or front-line employees possesses competency (A); area supervisors possess competencies (A+B); and security managers possess competencies (A+B+C). Policy and procedure for auditing the top-ranking security director or operations manager can be established with the help from outside agencies' available refresher or re-training programs on an annual basis.
- Special consideration: If you are fortunate enough to employ an in-house staff composed of either former law enforcement officers or those with some law enforcement training, be sure to implement special re-fresher training modules so that you maximize the value of their experience as training leaders. Also keep these valued resources up-to-date with current techniques and recent intelligence on threats.

Schedule of Training

1. Pre-season training for all in-house staff *or* shorter venue-specific training for contracted security personnel. This training is in addition to the training required by the security company.
2. Pre-event huddle between low-level workers and supervisors. Five to ten minute refresher meetings based on current threat information keeps staff on their toes and keeps it fresh for them on a daily basis.
3. As security directors or their assistant supervisors visit different venue areas, they can stop incorrect procedures, teach proper technique, provide the rationale for the proper technique, and assess whether the lesson has been learned on the spot.
4. Post-event debriefing: key personnel (including local law enforcement and fire services as needed) can participate in post-event debriefings to assess and learn what went correctly and why some things did not go as planned. Security directors are encouraged to ensure the formality of these events so they do not devolve into a situation where no one wants to "point fingers." Accountability is a goal to be maintained, so that lessons can be learned and re-training initiated as needed to correct behaviors.

Recommendations Concerning Specific Critical Resources

Full-time operation and security supervisors are often required to complete the following courses offered by FEMA: Incident Command System (ICS) 100, 200, 700 and 800. The same operation and security supervisors also complete DHS Soft Target Awareness and IED / VBIED Awareness and the DHS Bomb Threat Management program and DHS online Active Shooter programs.