



2008

# Protective Measures Guide for U.S. Sports Leagues



UNITED STATES TENNIS ASSOCIATION



For Official Use Only

# **PROTECTIVE MEASURES GUIDE FOR U.S. SPORTS LEAGUES**

## **WARNING**

This document is **FOR OFFICIAL USE ONLY (FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

2008

## Table of Contents

Introduction.....	1
Potential Threats.....	2
Terrorist Objectives.....	2
Threat Streams.....	3
Available Protective Measures.....	4
Implementation of Protective Measures.....	5
Routine Non-Event Protective Measures.....	5
Facility Emergency Action Plans.....	11
Command Post/Unified Joint Operations Center.....	12
Protocols for Event Threat Assessments.....	14
Personnel.....	15
Cyber Security.....	17
Deliveries/Mail.....	17
Event Day Operations: Perimeters.....	19
Event Day Operations: Signage.....	24
Event Day Operations: Gate Access and Management.....	25
Event Day Operations: Personal Searches.....	26
Event Day Operations: Credential Procedures.....	28
Event Day Operations: Food and Beverage.....	29
Event Day Operations: Aviation.....	30
Event Day Operations: Team/Officials Security.....	31
Event Day Operations: Miscellaneous.....	33
Areas of Special Concern.....	34
Special Considerations for Adjacent Facilities.....	34
After-Action Reviews.....	35
Appendix A: Acronyms.....	36
Appendix B: Codes, Regulations, Standards, and Guidelines.....	37
Appendix C: References.....	38

## Table

1 Homeland Security Advisory System Alert Levels.....	5
---	---

FOR OFFICIAL USE ONLY



## Introduction

Reducing the Nation's vulnerability to acts of terrorism by protecting critical infrastructures and key assets from attack is a core homeland security mission. Accomplishing this mission entails building and fostering a collaborative environment in which the private sector and Federal, State, and local governments can better protect the infrastructures and assets they control.

This guide provides an overview of protective measures designed to assist sports teams and owners/operators of sporting event facilities in planning and managing security at their facilities. It provides examples of successful planning, organization, coordination, communication, operations, and training activities that result in a safe sporting event experience.

This guide is a compilation of information obtained directly from the following sports leagues' security guides:

- Major League Soccer
- National Association of Stock Car Auto Racing
- National Basketball Association
- National Football League
- National Hockey League
- United States Tennis Association

Additional information was obtained from the International Association of Assembly Managers' (IAAM) *Best Practice Planning Guide for Arenas, Stadiums, and Amphitheaters*; an August 2005 draft document on Major Special Events from the U.S. Department of Justice's Office of Community Oriented Policing Services; *Counter Terrorism Protective Security Advice for Stadia and Arenas*, prepared by the United Kingdom's National Counter Terrorism Security Office; and Department of Homeland Security (DHS) reports on *Common Vulnerabilities*, *Potential Indicators of Terrorist Activity*, and *Protective Measures*.

Photographs and drawings were provided by the National Football League, Major League Baseball, and the National Association of Stock Car Auto Racing.

The following should be noted regarding the suggested protective measures in this guide:

- These suggestions are based on practices that may be employed by sports league facilities across the Nation. The need and ability to implement them at any specific facility and event will vary.
- These measures are intended for guidance purposes only; they are not a requirement under any regulation or legislation. In addition, because of the wide variety in the types of sports league facilities and in the size, composition and profile for particular events, not all suggested protective measures will be reasonable or applicable.
- These suggestions should not be viewed as a complete source of information on protecting sports league facilities. Sports teams, facility managers, and local security personnel should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

- These measures can be implemented for normal sporting events taking place under the Yellow, Elevated Alert Level in the Homeland Security Advisory System (HSAS). (See Table 1.) Higher alert levels may require more restrictive measures.

This guide discusses protective measures for pre-event, Event Day, and post-event activities, and offers information on other special considerations. Recommendations are grouped into the following categories:

- Routine Non-Event Protective Measures
- Facility Emergency Action Plans
- Command Post/Unified Joint Operations Center
- Protocols for Event Threat Assessments
- Personnel
- Cyber Security
- Deliveries/Mail
- Event Day Operations: Perimeters
- Event Day Operations: Signage
- Event Day Operations: Gate Access and Management
- Event Day Operations: Personal Searches
- Event Day Operations: Credential Procedures
- Event Day Operations: Food and Beverage
- Event Day Operations: Aviation
- Event Day Operations: Team/Officials Security
- Event Day Operations: Miscellaneous
- Areas of Special Concern
- Special Considerations for Adjacent Facilities
- After-Action Reviews

## Potential Threats

Protective measures are employed in response to various threats in order to:

- Increase awareness among facility and event managers and law enforcement agencies,
- Reduce vulnerabilities of sporting event facilities and their respective critical assets (e.g., team members, spectators),
- Enhance the defense against and response to an attack, and/or
- Better prepare event staff and supporting public safety entities to respond to and resolve incidents.

As such, it is important to understand terrorist objectives and the types of threats that exist against our Nation's critical infrastructures and key assets, which include sporting events.

## Terrorist Objectives

In general terms, terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence in government leadership. Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts, and these casualties can occur both at the targeted facility and in the surrounding area. Damage or destruction of the facility can be intended to shut down or degrade the operation of the facility or to cause the release of hazardous materials to the surrounding area. Disruption of the targeted site without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these items to other uses or to reap financial gain from their resale. Theft of

information can be intended to acquire insight that is not public information, gain data that can be used in carrying out attacks, or both.

## Threat Streams

Terrorists have a variety of weapons and tactics available to achieve their objectives, and they have demonstrated an ability to plan and conduct complex, simultaneous attacks against multiple targets. Attacks can be carried out by individuals, by small teams of a few perpetrators, or by larger groups acting in a coordinated fashion. Some threat streams (i.e., categories of potential threat) are described below.

- ***Improvised Explosive Devices***

An improvised explosive device (IED), or “homemade bomb,” can be constructed of commonly available materials, construction explosives (e.g., dynamite), or stolen military-grade explosives. Unprotected or accessible ammonium nitrate and fuel oil (ANFO) that is stored at many sports facilities may provide an opportunity for assembling an IED on-site. An IED can also be carried into a facility by an individual (e.g., a suicide bomber) or can be deposited in an unnoticed location for detonation by a timer or by remote control. Vehicle-borne IEDs (VBIEDs) are loaded into a car or truck or onto a motorcycle. The vehicles can then be parked close to the facility and placed where large numbers of people gather, or they can be driven through barriers and then detonated. VBIEDs are much larger and more dangerous than IEDs, and they are currently the most common means of attack throughout the world.

- ***Chemical Attack***

Chemicals can be exploited or used by terrorists as a weapon. Industrial chemicals can be transported by truck or by railroad to an area near a facility or large gathering of people then dispersed by means of explosives. Chemical warfare agents (e.g., sarin, VX) are another weapon of concern. Although not readily available, they have been procured and used by terrorists.

- ***Biological Attack***

Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of the potential for mass casualties and the exhaustion of response resources. The most notable instances are the 1995 sarin gas attack on the Tokyo subway, which killed twelve people, and the letters containing anthrax that were mailed out in the United States in 2001, killing five people. Biological agents can be dispersed into the atmosphere (e.g., via crop-dusting aircraft); can be introduced into a facility through its heating, ventilation, and air-conditioning (HVAC) system; or can be spread by contact (e.g., through contaminated letters delivered by mail). A biological attack may involve colorless and/or odorless agents, and symptoms of exposure may be undetected for days or weeks afterwards.

- ***Nuclear/Radiological Attack***

Weapons-grade nuclear material is relatively difficult to obtain. However, some sources of nuclear and radiological material are more readily available and/or easily delivered. Radiological materials include radioactive material from a variety of sources, such as medical or industrial equipment. In radiological dispersion devices, often called “dirty bombs,” these materials are attached to an explosive to create a wide area of contamination. All these materials can be introduced into a facility either directly (e.g., by spreading them on surfaces where people will have direct contact with them) or through the HVAC system.

- ***Aircraft Attack***

Both commercial and general aviation aircraft can be hijacked and used to deliver attackers, explosives, or hazardous materials to an area or facility. The aircraft themselves can also be used as weapons.



- ***Maritime Attack***  
Ships and boats of various sizes can be used to deliver attackers, explosives, or hazardous materials. The vessel itself can also be used as a weapon.
- ***Cyber Attack***  
Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Information can be altered, corrupted to render it unusable, or stolen. Information systems can be attacked with the intent of overloading the equipment (e.g., denial-of-service attacks).
- ***Sabotage***  
The disruption, damage, or destruction of a facility through sabotage and the introduction of hazardous materials into the facility are of concern. Sabotage can be perpetrated by employees or by outsiders.
- ***Small Arms Assault***  
Small arms, including automatic rifles, grenade launchers, shoulder-fired missiles, and other such weaponry, can be aimed at people (e.g., shooting of civilians) or at facilities (e.g., stand-off assault from outside a perimeter fence).
- ***Arson***  
Intentional fires can be set by using highly flammable materials (e.g., gasoline) tossed into a facility. Accelerants that promote the spread and intensity of a fire can be applied beforehand and then ignited. Arson is a threat both during and after normal business hours.

## Available Protective Measures

Protective measures include equipment, personnel, training and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

<b><i>Devalue</i></b>	Lower the value of a facility to terrorists; that is, make the facility less interesting as a target.
<b><i>Detect</i></b>	Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.
<b><i>Deter</i></b>	Make the facility more difficult to attack successfully.
<b><i>Defend</i></b>	Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

There are many different protective measures available for deployment at sports facilities and events and in the areas surrounding the event (i.e., buffer zones). Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or threat stream. In addition, some may be sustainable and address long-term strategic needs, while others may be implemented in the short-term as responses to specific information or elevated threat levels. In general, applicable protective measures can be grouped into several broad categories based on alert levels, as shown in Table 1. In addition to these generally applicable measures, some protective measures are specifically oriented toward a particular sports league's infrastructure.

## Implementation of Protective Measures

Some protective measures are designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as “baseline countermeasures.” Others are implemented or are increased in their application only during times of heightened alert.

The implementation of protective measures at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners need to coordinate and cooperate with local law enforcement, emergency responders, and State, local, and Federal government agencies with regard to what measures to implement, how extensive they should be, and how long they should be carried out in order to maximize security while staying within the bounds of available resources.

To assist in the decision process, DHS has developed the color-coded HSAS to communicate with public safety officials and the public at large so that protective measures can be implemented or expanded to reduce the likelihood or impact of an attack.

**Table 1: Homeland Security Advisory System Alert Levels<sup>1</sup>**

Alert Level		Description
Red	SEVERE	Severe, imminent risk of terrorist attack
Orange	HIGH	High risk of terrorist attack
Yellow	ELEVATED	Significant risk of terrorist attack
Blue	GUARDED	General risk of terrorist attack
Green	LOW	Low risk of terrorist attack

When available intelligence allows, the HSAS alerts are supplemented by information on the threat stream(s) most likely to be used by terrorists. This information may or may not be very specific, may or may not identify geographic areas of concern, and may or may not offer a time period when attacks might be expected. This level of uncertainty is inherent in dealing with terrorist threats and must be factored into decisions on committing resources to the implementation of protective measures.

In addition to the HSAS, some infrastructure owners, industry associations, and information sharing and analysis centers have developed their own alert classification schemes tailored to specific critical infrastructures or key asset segments (i.e., IAAM’s *Best Practice Planning Guide for Arenas, Stadiums, and Amphitheaters*).

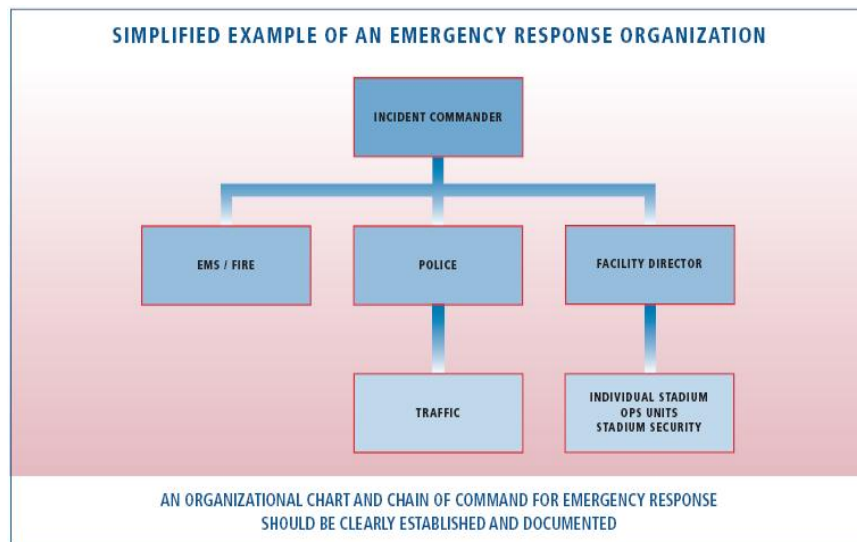
## Routine Non-Event Protective Measures

In this time of elevated security awareness, owners of facilities that attract large crowds of the general public such as sporting events must be responsible for assessing their specific facility vulnerabilities and practicing prudent risk management and mitigation measures. This assessment is an ongoing process that produces various plans and programs that are implemented throughout the year, while other plans and programs are implemented for specific sporting events. The activities described below should be considered for inclusion in the sport facility’s protective measures baseline.

- The facility should designate an experienced employee as Security Director/Incident Commander to lead day-to-day security matters and emergency-related activities.

<sup>1</sup> Table 1 is intended to be illustrative rather than comprehensive.

- Conduct threat analyses, vulnerability assessments, consequence analyses, risk assessments, and security audits of the facility and surrounding area on a regular and continual basis. Include assessments of other activities and operations in the vicinity (e.g., airports, chemical plants, government buildings, pipelines, rail lines) to determine whether they may present increased security risks to the facility.
- Develop a Facility Emergency Action Plan that is reviewed periodically and revised as needed. The Facility Emergency Action Plan should address event preparation, incident response (e.g., bomb threats, mechanical problems, structural problems, fire, suspect package or vehicle, isolated attack, catastrophic large scale attack, unauthorized entry into facility, and power failure), evacuation or shelter-in-place, communications, and recovery. This plan should be developed in concert with the facilities public safety entities. It should include a signature page for all entities involved.
- Create a Command Post (CP) or Operations Center (OC) location within the facility in order to manage the security and safety aspects of sporting events occurring on the premises.
- Utilize an Incident Command System (ICS) with a Security Director/Incident Commander to coordinate local resources in response to a critical incident at the facility. The ICS should be integrated with the Command Post and should utilize the Facility Emergency Action Plan to carry out its responsibilities. For major incidents, the Incident Commander (IC) will be a public safety official.



(Photo courtesy of National Football League)

- Establish the capability to collect and interpret available threat intelligence from local, State, and Federal agencies. Facility owners and operators, through a partnership with various law enforcement and intelligence contacts, should maintain constant awareness of current threat conditions and available intelligence information.
- Establish procedures, as part of the Facility Emergency Action Plan, to implement additional protective measures as the threat level increases. Also establish procedures for returning to lower security levels as the threat decreases. Utilize the ICS to alert local law enforcement and emergency responders of the protective measures being implemented at the facility.

- Evaluate crime in the area surrounding the facility. Continually monitor the activities around the facility, and record any suspicious or unusual activities. Follow up on any such occurrences with the relevant authorities (e.g., Joint Terrorism Task Force (JTTF)). Create a program through the ICS that allows the facility's security organization to share information and concerns to the proper local authorities.
- Evaluate the impact of the sporting event on the surrounding area. Businesses and homeowners may be impacted by crowds and the closure of streets. Owners of retail stores, restaurants, and other small businesses should know what to expect during an event. Discuss potential problems, and review the law about alcohol service to intoxicated individuals. Meet with businesses to explain protective measures activities associated with each sporting event and to obtain input from the surrounding community.

- Install internal and external cameras (digital) with pan, tilt, zoom and monitoring capability covering all vulnerable areas. Assess camera coverage and recording capabilities. Make footage available to local law enforcement partners.



(Photo courtesy of National Football League)

- As part of the ICS, develop and sign a memorandum of understanding with local jurisdictions that clarifies the legal authority of assisting government agencies to enforce the law in the lead agency's jurisdiction, and enumerates the commitment of assisting government agencies in providing personnel and equipment. The memorandum should state when and where other government agencies' officers should arrive and the specifics of their assignments; it should also clarify any compensation for labor costs, expenses, and equipment incurred by the assisting government agencies.
- As part of the ICS, identify roles and responsibilities for the emergency services and law enforcement personnel working at each event (e.g., law enforcement will maintain order and traffic management; fire/rescue will perform fire inspections, rescues, and deal with hazardous materials; Emergency Medical Services (EMS) will perform medical care and transportation; county and State emergency management will coordinate crisis requirements and resource needs; and the Federal Aviation Administration (FAA) will control aviation activities). The National Incident Management System should be utilized as a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management. The FBI will provide IC for terrorist incidents and weapons of mass destruction support.
- The facility Security Director should maintain and/or develop positive working relationships and key contacts with local law enforcement and other government services, including local police, fire and EMS departments, the Federal Bureau of Investigation (FBI), the United States Secret Service, and additional emergency management agencies.

- Integrate hospitals into the Facility Emergency Action Plan in order to provide critical information to these primary health care facilities on anticipated threats to and attendance of sporting events. In some cases, hospitals may set up mobile clinics at a sporting event to assist in treating heat stroke, intoxication, and minor injuries.
- Check the status of all emergency response equipment and supplies on a regular basis and prior to an event. Have emergency supply kits located in areas where employees can have ready access to them. Through the ICS, provide adequate security for emergency response equipment, facilities, and personnel. Do not leave emergency vehicles or equipment unattended or unsecured.



(Photo courtesy of National Football League)

- Hold a routine meeting including the sports league, team management, facility owners/operators, and public safety agencies prior to an event to review special needs, protective measure requirements, roles and responsibilities. Review lessons learned from past events to know what worked, what didn't, and how those lessons could impact future events.
- Identify potentially incompatible communications equipment being utilized among the various agencies involved in event security prior to an actual event, and ensure that different frequencies can be routed through a common communications matrix or via hand-held radios employed by all participants. Consider implementing a Unified Joint Operations Center (UJOC) to collocate and centralize all communications (e.g., voice, data and video).
- Conduct regular exercises with facility employees to test the security and emergency response plans, to ensure that adequate resources are available to implement the plans, and to verify that all operating units can implement their responsibilities according to the plans. Through the ICS, conduct regular exercises with law enforcement and emergency responders to familiarize them with the facility and its security and emergency procedures. Conduct at least one emergency drill prior to or early in the sports league season.
- Inspect and test all safety and security systems, including the PA system override, prior to the sporting event season and at least once a month during the season, or more frequently if required by code.
- Perform a pre-event site survey in an effort to identify areas of unauthorized access; try to minimize the total number of access points to the venue. Block access points on the facility property that are not being utilized with "Jersey-type" concrete barriers; install signage stating that the area is not a means of access and that spectators should report to the next available access



(Photo courtesy of National Football League)



point. During the event, however, ensure that egress points have personnel posted and remain unlocked for evacuation purposes.

- Identify key roles and responsibilities for the facility and event staff. Fill those roles with experienced personnel. Prepare an Organization Chart that explains the roles and responsibilities of all facility personnel (i.e., security, emergency medical services facility operations, concessions, communications, parking, seating). Develop and provide personnel with Post Orders for each position.
- Provide sufficient employees for year-round facility security, twenty-four hours a day and seven days a week.
- Create a program that will require employees to check their own work areas on a daily basis for anything that seems out of the ordinary. This type of check is known as a “white level search.” The best people to identify unusual occurrences are the people that work in that area every day.
- Encourage employees to report any suspicious activities. Emphasize during training that all reports (including false alarms) will be taken seriously and regarded as a contribution to the safe running of the sports facility. Include Tour personnel if the facility conducts public tours.
- Develop and maintain administrative procedures to ensure that uniforms worn by security personnel, event staff, concessionaires, etc., which could be utilized to compromise access controls are properly safeguarded.
- Establish a secure perimeter (i.e., buffer zone) around the facility with limited and controlled vehicle and people access points. Limit access control gates to one or two on Non-Event Days.



(Photos courtesy of National Football League)

- Create a vehicle parking system, and allocate parking areas for specific aspects of facility activities (i.e., players, employees, visitors). Patrol facility to ensure that there are no unauthorized vehicles or personnel on the grounds. Do not allow unauthorized vehicles to remain overnight, and limit public access to the greatest extent possible. Be alert for any suspicious activities, and collaborate with police to conduct periodic, unscheduled police patrols around the facility. Keep familiar vehicles close to the facility, and limit access of unknown vehicles to a distance away from the facility. If necessary, work with local law enforcement to close public streets that are adjacent to the facility and re-route traffic away from the facility. Search vehicles entering the inner perimeter of the facility.
- Issue badges with photograph for regular employees, event staff, vendors, and subcontractors.

Design photo identification to incorporate different levels of access into various parts of the facility (i.e., service level, locker rooms, heating, ventilation, and air conditioning (HVAC) intakes). Identify, log in and out, and issue self-expiring day passes to all authorized visitors. Escort visitors with appropriate department employees. Refuse entry of visitors who are not authorized, and send them away from the facility.

- On Non-Event Days, have visitors and contractors sign in and out when entering and leaving the facility. These records could be useful later if needed. On Event Days, have staff, vendors, and contractors sign in and out.



(Photos courtesy of National Football League)

- Through the ICS, share critical information about the facility (e.g., floor plans, location of emergency equipment, notification and contact lists) with local law enforcement and emergency responders. At the same time, restrict access to sensitive venue data and information (e.g., building plans; mechanical, electrical, fire, and life safety systems).
- Secure and protect with locks and/or tamper proof seals all HVAC, mechanical, electrical panels, gas and fuel systems, and centralized beverage (i.e., beer and soda) dispensing rooms. Test backup utility systems annually or in compliance with local codes to ensure that they are properly maintained and functional.
- Protect the controls for critical systems (i.e., lights, fire doors, elevators, escalators, sprinkler systems, public address (PA) system, closed circuit television (CCTV), and land line phone systems) against outside intrusion by installing passwords, firewalls, and exception logging/tracking software. Test intrusion systems on a regular basis.
- Store flammables, combustibles, fertilizers, and other potential products or chemicals that can be used as components for explosive devices in secure and separated areas, preferably off-site. Regularly monitor the safeguarding of any products and/or chemicals that must be stored on-site, and handle all materials in compliance with State regulations.
- Keep facility clear of clutter and debris. Store all equipment and materials in an orderly manner.
- Do not place propane tanks under or adjacent to structural supports or sensitive areas.
- Develop procedures for shutting down the facility in case the threat is deemed too serious to continue an event.
- Prepare a Business Continuity/Disaster Recovery Plan for the facility.

- Review insurance coverage and recovery requirements periodically as part of the overall risk management program.
- Consider having at least one employee obtain a Federal security clearance.
- Do not place dumpsters under structural supports or sensitive areas (i.e., entrances/exits for team members and spectators). Dumpsters should be locked when not in use. Regularly monitor and empty all dumpsters and trash receptacles.



(Photos courtesy of National Football League)

## Facility Emergency Action Plans

Prepare a Facility Emergency Action Plan as part of the facility's ongoing protective measures.

- Coordinate the Facility Emergency Action Plan with local, State, and Federal emergency management authorities. Include protocols for event delays, cancellations, incident response (e.g., partial or full evacuation, relocation, or shelter-in-place), communications, and recovery. Address the needs of people with special needs (e.g., physical disabilities, non-English speaking).
- Keep copies of the Facility Emergency Action Plan and all response documents in redundant locations. Ensure that the plans are protected from unauthorized disclosure.
- In coordination with local, State and Federal emergency management authorities, identify the chain of command (i.e., decision makers) through the ICS. Each sporting event should have an ICS document that clearly identifies who has the authority to make decisions relative to man-made or natural incidents. This authority includes such actions as halting the event, dealing with the containment of a contaminant within the facility, evacuating the facility, relocating individuals, or coordinating shelter-in-place. The Security Director will discuss information and proposed courses of action with various stakeholders (e.g., sports club, facility owner, State and local governments) in an effort to achieve a unity of effort and a consensus regarding the approach taken.
- Determine the need for personal protective equipment for employees (e.g., toxic material detectors, breathing apparatus). Purchase and store equipment for ready use in the event of an incident.
- Include contact numbers for personnel identified above and give sequence of notification. This information may be provided in an appendix to the plan and updated at least annually and/or when changes are made.

- Develop flow charts showing the means of communicating decisions and information from the top decision maker down to the ticket holder. Describe the primary and backup communication systems (e.g., phones, radios, and jumbo screens).
- Ensure that relocation areas for evacuation situations are accessible and secure. For shelter-in-place situations, ensure that the facility is adequately stocked with food, water, and supplies to accommodate the number of people who might need to use them.
- Ensure that plans are developed for securing the facility in the event of a full evacuation and for ensuring that the facility is safe for re-occupancy.
- Develop a plan and timeline for conducting emergency drills and training exercises. The training scenarios and drills should test the ICS's decision-making process, primary/secondary communications and emergency use of the PA and video systems. Update all plans as needed and submit to each Sports League's Security Office.
- Determine the feasibility of creating additional emergency exits. Working with local authorities, establish evacuation routes for pedestrians and vehicles.
- Ensure that employees are familiar with the protocol and procedure for shutting off utility services (e.g., electricity, natural gas) during emergency situations.
- Prepare an Emergency Medical Plan as part of the Facility Emergency Action Plan. Include clear procedures for a catastrophic event, requiring primary and secondary triage. Designate triage and transport sites. Identify and secure emergency routes in and out of the facility (in the context of local area emergency plan). Each county throughout the US is required to have a Mass Casualty Plan in place that has been coordinated with the facility.
- Develop audio and video scripts (i.e., public address announcements) for specific emergency announcements, including but not limited to natural disasters, weather, bomb threats, and other potential disasters.
- Do not release information on internal security measures to the press. Establish a single voice to deal with the media.
- Ensure that security measures do not compromise spectator safety.



(Photo courtesy of National Football League)

## Command Post/Unified Joint Operations Center

A Command Post (CP) / Unified Joint Operations Center location should be established for each sporting event in order to manage the security and safety aspects of the event. The CP/UJOC protective measures described below should be considered for activation during a sporting event.



- Provide a secure area in the UJOC designated for decision makers. It may be beneficial to have monitors in the CP with feeds to monitors in the incident room. The UJOC should be close enough to be part of the solution, but not so close that it becomes part of the problem.
- Utilize the ICS to coordinate resources in response to a critical incident.
- Consider designating an area for a forward CP that has a view of spectators and the playing field.



(Photo courtesy of National Football League)

- Ensure that everyone working within the CP/UJOC understands the protocol and resulting chain of command for handing an issue over to the relevant government/public safety department(s).
- Staff the CP/UJOC with the following: Security Director, potential Incident Commander(s), police, fire/EMS, facility management (operations and security), club representative, private security, media representative if the event is televised, and FAA (or direct line) personnel. The UJOC should be designated the meeting place for the “Threat Assessment Team” should an emergency occur.
- Designate the UJOC as the backup to the CP in the event the forward CP has to be evacuated. Locate the backup outside the facility with good communications and sufficient employees/equipment to serve as a CP. A mobile police command vehicle may be considered.
- Ensure that reliable communications with backup systems are in place and tested. Include an outside line; facility extension phones; police, fire/emergency medical technician radios; fire, intrusion, and panic alarms; ring downs and contact with home team public relations; control tower or the owner's box. There must be reliable communications (e.g., hand-held two-way radios) between the CP and the PA/video employees in order for the CP/UJOC to authorize and direct the broadcast of emergency scripts and messages. Consider establishing a 911 consol in the UJOC to receive and dispatch all calls within the immediate vicinity.
- Ensure that the CP/UJOC has the capability to override the facility PA system and video scoreboards. Prepare announcements and displays for various potential incidents.



- Initiate a trap and trace capability on all CP/UJOC phones. Provide telephone operators with relevant checklists and forms to fill out in the case of threatening phone calls. Training should be given to staff members that will be working in such positions.

## Protocols for Event Threat Assessments

The threat assessment protective measures described below should be considered for use at the facility.

- In coordination with local, State and Federal Public Safety authorities, establish a “Threat Assessment Team” for each event, consisting of (as appropriate) a representative from local police, fire, and EMS departments; a facility management representative, and a sports league representative. Designate a person to be “In Charge” or the “Incident Manager,” as appropriate to the situation.
- Identify the most logical event threats (e.g., bomb, person with firearms, chemical/biological agent, suspicious packages/letters, threats made against a specific person).
- Establish a Threat Response Protocol for both Event Day and Non-Event Day situations.
- Provide checklists and training to phone operators dealing with phone threats. Install caller identification and/or coordinate phone call trap capability with the phone company for publicly accessible numbers.
- Ensure that all incoming threats, whether telephonic or via other mediums are properly recorded and preserved.
- Threats received at other facilities that are connected to or co-located with the sports facility (i.e., train or subway station, another sport facility) should also be reported to the Incident Manager.
- Specify persons to be notified and the order of notification. Ensure that the notification list remains current by updating annually and/or when contact changes occur. Establish a monthly or quarterly exercise to test recall procedures.
- Clearly establish protocols for investigating and reporting a given threat or suspicious package on both Event Days and Non-Event Days. The person receiving the initial threat should only communicate it to the appropriate supervisor for action. Immediately notify law enforcement if a threat is found to be credible.
- Develop policies and procedures for dealing with hoaxes and false alarms so that they will not unduly burden the facility’s operations. Determine how bomb hoaxes and genuine threats may be differentiated successfully, as well as how to communicate the awareness of possible harm without creating alarm that could add to the impacts (e.g., a stampede).
- Designate a Public Information Office to respond to the media and the general public in the event of an incident to speak with a single voice. Develop policies and procedures to advise them of the situation and diffuse rumors and panic.

- Establish a “Security Awareness Campaign” through information provided on the facility’s Web site, team mailings, and signage in the facility to reach out to the patrons to encourage reporting of suspicious activity to the nearest usher, event staff, security guard, or law enforcement officer.
- Develop procedures for shutting down/evacuating the facility in the event that a threat is deemed too serious to continue a sporting event on the premises.

## Personnel

Personnel that are properly screened, trained, and equipped constitute the primary element of a successful security program. The protective measures described below should be considered for use.

### Employees

- Establish a comprehensive employee background screening and training program for all facility personnel and venue concessionaires. Employee screening should be updated regularly and reviewed by the facility’s Security Director. Conduct more detailed checks on those who will have access to critical or restricted areas. Develop a list of disqualifying factors that can be used to reject an individual. Personnel background screening should be reviewed by the facility’s Security Director/Incident Commander every two (2) years to ensure the suitability for his or her position.
- Incorporate security awareness and appropriate response procedures for security situations into employee training programs. Include the following in the training:
  - Standard Operating Procedures in the security and emergency response plans that are to be used for different types of incidents,
  - Maintaining alertness to and recognizing situations that may pose a security threat (e.g., suspicious persons, persons without proper employee identification, persons carrying unusual packages, unattended vehicles and packages, strange odors or liquids),
  - Contact and notification protocols for suspicious situations and emergencies,
  - Caution in providing facility information to outsiders,
  - Procedures to provide for the safety of employees during a security incident, and
  - Roles and responsibilities.
- Maintain up-to-date security training with regular refresher courses. Maintain records of employee training that has been completed.
- Provide an adequate level of security supervision and oversight for employees. Be alert to suspicious activities by employees (e.g., working irregular hours, attempting to access restricted areas, carrying unusual packages).
- Review the personnel files of recently terminated employees to determine whether they pose a security risk. Take appropriate actions to mitigate the risk.
- Ensure that employees understand and accept the need for security measures. Emphasize the fact that security is a responsibility for all employees, not merely for security experts or professionals. Make it easy for employees to raise concerns and/or report their observations.

### **Contractors, Vendors, Temporary Employees**

- Provide security information and training to all contractors, vendors, and temporary employees at the facility. Advise them to be alert to suspicious activity or items, and train them on how to report such incidents.
- Require contractors, vendors, and temporary employment agencies to certify that their personnel meet the security and background standards that are consistent with contractual requirements.
- Review cash handling procedures with vendors/concessionaires.

### **Security Force**

- Maintain an adequately sized, equipped, and trained security force. Ensure that adequate security personnel are on duty or on call in the event of an incident. Consider employing local law enforcement personnel on a part-time basis to supplement the facility's security force. Determine the availability of security force reinforcements that would be deployed during heightened threat conditions. Conduct rigorous background checks on security force personnel.
- Provide additional security measures (e.g., body guards) to VIPs and high-profile visitors. Coordinate plans and communication procedures to ensure safe arrival, attendance, interviews, and departure for special persons and their support staff, which may involve working with contract, State, and Federal protection authorities.
- Coordinate security force operations with local law enforcement and, as needed, with State and Federal agencies (e.g., FBI, DHS, and the JTTF).
- Develop a procedure and location for detaining and questioning persons exhibiting suspicious behavior and/or violating security regulations. Train security force in appropriate methods for handling such people.
- Conduct regular drills and exercises with security forces in coordination with local, State, and Federal emergency management authorities. Involve local law enforcement and other agencies as appropriate.
- Alter the appearance of security force personnel (e.g., changing uniforms, vests, plain clothes) to disrupt terrorist planning. Dispatch plainclothes security employees inside and outside the facility and parking area.
- Develop a security force schedule that includes both regular and random patrols.
- Arrange for security force and/or law enforcement vehicles to be parked randomly outside critical facility assets.
- Provide personal protective equipment (e.g., respirators, body armor) to security force personnel as appropriate.

## Cyber Security

The protective measures described below should be considered for use to address information and computer systems security.

- Develop and implement a security plan for computer and information systems hardware and software. Design and implement a secure computer network architecture.
- Ensure that all operating software is regularly updated. Software providers are continually addressing security vulnerabilities in their software. The resulting fixes or patches are typically available for downloading on their Web sites.
- Regularly test the computer security measures (e.g., audits, penetration testing).
- Install and maintain up-to-date cyber security techniques (e.g., firewalls, virus protection, spyware protection encryption, user authentication) and software patches. Monitor computer systems regularly to detect any patterns of probing, hacking, or intrusions. Work with your Internet service provider to address multiple points of entry and implement protective measures against attacks (e.g., denial-of-service attacks). Keep current on the latest cyber security threats, incidents, and defensive measures.
- Provide training on cyber security policy, procedures, responsibilities, threats, and incident reporting to all employees that use the facility's computer system. Immediately cancel access for terminated employees.
- Control physical access to information technology facilities (e.g., computer rooms). Install locks and access controls to allow only authorized personnel to enter. Provide communication capabilities to allow rapid reporting of incidents.
- Thoroughly test all applications that involve the handling of sensitive information for potential vulnerability to compromise.
- Back up all information and store it in a secure location, preferably off-site.
- Regularly review the facility's Web site to ensure that no sensitive information is being provided. Delete any information from the facility's Web site that might aid an adversary in planning an attack.
- Immediately report all intrusions or denial of service to the FBI.

## Deliveries/Mail

The protective measures described below should be considered for use to address delivery of mail/materials to the facility.

- Position security vehicles or other physical barriers in such a manner as to prevent vehicular forced entry into the loading dock area.
- Limit daily or weekly delivery times. Schedule all deliveries through a single entrance.

FOR OFFICIAL USE ONLY

- Make Event Day deliveries the exception, not the normal routine. Schedule as many deliveries as possible for days/times when a sporting event is not in progress. Schedule the delivery of hazardous materials during times of non-occupancy (e.g., overnight).
- Require all delivery vehicle drivers and helpers to produce photo ID and sign in at a control point.
- Accept deliveries by appointment only, and require authorization by the appropriate facility supervisor. Reserve the right to inspect or reject any delivery. Require check-in and receive delivery by person expecting it. Do not leave deliveries unattended on the loading dock.



(Photos courtesy of National Football League)

- Escort the delivery vehicle to any other areas within the facility where a delivery is made. Contact routine facility vendors, and introduce a Self-Certification Program to facilitate deliveries and shipments.
- Keep a record of each vehicle, driver, and helper(s) entering and leaving the secure area by use of a log or permit system. Identify driver and helper(s) by photo identification. The facility Security Director should retain the delivery records.
- Search vehicles when they exit the facility to ensure that no theft has occurred.
- Inspect all large items brought into the facility, and retain the right to search any bags or parcels brought into the facility. Provide security guards at all checkpoints for assistance and deterrence purposes.
- At no time should any vehicle be unescorted or left unattended. Upon departure, the driver will check out at the security control point. Inform the Security Director/Incident Commander of all expected deliveries on Event Days.
- Process mail off-site, if possible. Facilities used for mail processing should have independent HVAC systems and alarms.
- Train mail room personnel to recognize suspicious mail and packages, and what procedures to follow.
- Consider providing protective equipment (e.g., gloves, respirators) to mail room personnel. Develop and rehearse evacuation procedures, which should include designating a Washing Facility where contaminated staff can be isolated and treated.



## Event Day Operations: Perimeters

Access control to the facility is an important protective measure utilized during sporting events. It is important to control vehicles and individuals outside the facility, inside the facility, and in restricted or playing/racing areas. Access control is implemented in terms of three perimeters (i.e., outer, middle, and inner). Responsibilities for implementing the perimeter protective actions will be defined by the ICS.

### *Outer Perimeter*

A secure outer perimeter (i.e., buffer zone) of at least 100 feet should be established around the facility to the maximum extent and when possible. This outer perimeter is used to deter vehicle traffic, but not necessarily pedestrian traffic. It often encompasses the facility's property boundary, but this differs for each facility. The outer perimeter may include the facility's parking lots and, in the case of motor speedway events, the camping areas.

The protective measures described below should be considered for use throughout the outer perimeter during a sporting event.

- Temporarily block off roads and streets adjacent to the facility, where feasible.



(Photos courtesy of Major League Baseball)

- Reinforce areas that are vulnerable to forced vehicle entry with substantial barricades (e.g., Jersey barriers, reinforced concrete decorative planters, bollards and / or large trucks or buses). This is especially true for inner perimeter areas such as racing facilities.
- Ensure that all parking lot attendants and security personnel are fully informed of and trained in security policies and Emergency Evacuation Procedures.
- Monitor parking areas to ensure that EMS and fire vehicles and personnel have unimpeded access to and from the facility.
- Increase the presence of uniformed law enforcement and facility security employees within the outer perimeter, supplemented with “undercover” personnel.



(Photo courtesy of National Football League)



(Photo courtesy of Major League Baseball)

- Utilize marquees and electronic message boards to communicate protective measures procedures, restrictions, prohibited items and evacuation routes to the patrons entering the facility.
- Use the PA system to communicate patron security instructions. Use signage and handout materials, if necessary, to supplement instructions as patrons park or walk up to the facility. Consider printing security guidelines on tickets or including guidelines in the materials sent to season ticket holders and dispensed during box-office sales.
- Post signs outlining security procedures at all “park and ride” or shuttle pick-up points, other mass transportation locations and parking lots.
- Ensure that security personnel and parking attendants advise arriving patrons to dispose of bags/coolers or other prohibited items before entering the facility.
- Remove all unauthorized or unidentified vehicles within the defined outer perimeter area at least two (2) hours prior to the event.
- Where underground parking is utilized. On game days, all vehicles capable of carrying 5,000 pounds of concealed weight should have the contents of the vehicle inspected by the security staff prior to entering the underground parking area.
- Inspect and label all vehicles allowed inside the 100 foot outer perimeter. If it is not possible to create the 100 foot secure area around the facility, identify vulnerable areas and identify the possible threat. Utilize employees’ vehicles as barriers. When creating the outer perimeter secure, an area to ensure public access for disabled patrons, fire lanes, and emergency vehicles.
- In unusual circumstances where the facility has inside parking, search each vehicle and screen its occupants. The use of trained canine (Bomb Dog) teams is suggested under these circumstances, as well as trunk searches and the use of undercarriage mirrors. Prohibit the sale of daily parking permits.
- Ensure that parking areas are properly illuminated and patrolled at least 1 ½ hours before the event.
- Ensure that the external P.A. system is working and audible.

### ***Middle Perimeter***

The middle perimeter is the first level of access control for persons and their possessions. This perimeter is secured so that no one without a pass/ticket or credential is permitted entry through protected gates or doors.

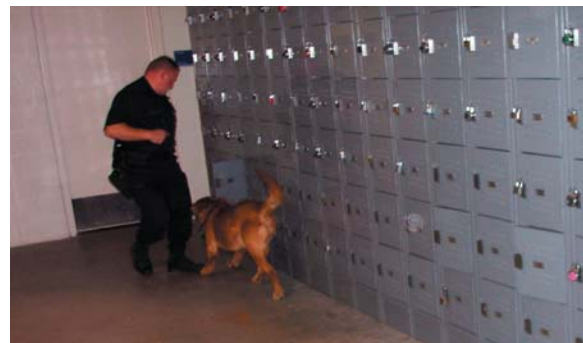
At motor sport facilities, the middle perimeter usually encompasses the outer ring of the racing surface and the stands. Unlike other major sporting events, it is also the first line of defense for vehicle access.

The protective measures described below should be considered for use throughout the middle perimeter during a sporting event.

- Prior to opening the access control gates to the public, all departments should physically check their areas of responsibilities and inform the security command center when they are ready to open. If there is any reason why the access control gates cannot be opened to the public at the posted time, the Security Director should be informed immediately. The person responsible for the security and safety of the facility should be the one who authorizes the opening of the access control gates to the public.
- Ensure that all exterior doors have non-removable hinge pins, no exterior hardware or protective plate coverings on the locks, and no plates covering gaps between the door and its jam.
- Conduct a complete and thorough inspection of the facility immediately after the home team takes control of the facility. Pay particular attention to restrooms and garbage receptacles. Secure gates and lock down the facility (i.e., remove all unauthorized vehicles and personnel) to create a secure middle perimeter. Identify inspected vehicles with a visible permit or sticker. Conduct this inspection 1½ hours prior to the event, and, if possible, utilize “bomb dogs” and trained personnel using a grid search technique.



(Photos courtesy of National Football League)



- Assign responsibility for conducting facility inspections to the employees who are most familiar with the facility and can quickly identify what is missing, out of place, or otherwise suspicious.

- Inspect all HVAC, mechanical and gas/fuel/cooking systems, and other critical systems. Protect them with locks and/or tamper proof seals. Assign security to safeguard any vulnerable systems, including air intakes that are located inside and outside the inner perimeter. Know how to shut off air circulation systems. If local fire codes allow, consider installing a central emergency shut-off switch for the HVAC system.



(Photo courtesy of National Football League)

- Check and inspect broadcast/media vehicles that arrive before or on Event Day. The broadcast company should forward a list of all personnel requiring access into the facility during set-up and event periods. Upon entering the facility, broadcast personnel are to identify themselves with a photo ID and be issued a facility credential. All broadcast bags are to be checked by security, cleared, and tagged. Broadcast vehicles should be located in a designated, secure compound with its own perimeter. A security officer should be deployed 24/7 in the area of the broadcast/media compound while the media is present at the facility. Entry to the media area should be controlled, and all media persons should be credentialed.



(Photo courtesy of National Football League)



(Photo courtesy of Major League Baseball)

- Establish access control gates for all vehicles, employees, event staff, police, media, and competitors. Ensure that event personnel IDs are screened and verified prior to admittance into the facility. Search and tag all vehicles. Limit access to those individuals that are necessary to put on the event (i.e., club employees, relevant facility employees, Event Day employees, public safety officials, event officials, league officials, media, and participating teams). All individuals entering through the access control gates are subject to a personal search as well as a search and tagging of any work-related equipment. Event Day personnel who do not require a bag to perform their function will not be allowed to enter with a bag. Remove all refused bags from the facility.
- Employ protective measures (e.g., fencing, bollards, enclosures) around exposed utilities (e.g., transformers, natural gas lines, water valves, telephone switch boxes) to protect them against attack and damage.





(Photos courtesy of Major League Baseball)

### ***Inner Perimeter***

For team sport events, the inner perimeter contains the players' locker rooms, benches, playing surface/racetrack, infield, and garages/pits.

For motor sport facilities, the inner perimeter includes the track surface and the infield. The size of this perimeter varies from track to track, potentially including camp grounds, helipads, vendors, fuel stations, garage areas, and pits as well. At motor sport venues, the inner perimeter contains all high-level government officials, competitors, sponsors, entertainers, and event officials. No one should be permitted in the inner perimeter without proper credentials and identification.

The protective measures described below should be considered for use throughout the inner perimeter during a sporting event.

- Allow only patrons with tickets, credentials/badges/passes/wristbands or coaches/players/teams in the inner perimeter. Credential Boards that display credentials/badges/passes/ wristbands for the event should be created and given to the security employees for access enforcement.



(Photo courtesy of NASCAR)



(Photo courtesy of Major League Baseball)

- At motor sport facilities, specifically authorize and thoroughly search all vehicles prior to entry. Provide pull-over lanes for inspection of suspect vehicles.



- Ensure that the pits and garage areas of motor sport facilities have additional check and access points where people attempting to enter are carefully screened. It is recommended that the garage area be swept for explosives by bomb dogs before opening. Prior to loading the garage, it is recommended that race haulers should be screened by bomb dogs before unloading.



(Photo courtesy of NASCAR)

- Security guards and/or event staff should be present where there is access to the playing fields, courts, tracks, and rinks. Each team security manager and facility Security Director will determine the number and location (i.e., bench area, end lines, family member's area) of security guards and/or event staff that will be on the playing fields, courts, tracks, and rinks.
- Each team security manager and facility Security Director will determine the responsibilities and actions to be taken by security guards and event staff during event time-outs, half-times, player and/or coach altercations, and player/fan altercations.

## Event Day Operations: Signage

Signage is essential to the orderly conduct of an event. The signage protective measures described below should be considered for use during a sporting event.

- Ensure that ample, prominent signage lists Point of Contact information for facility security personnel and provides guidance on responding to and reporting suspicious activities.
- Ensure that signage in the parking/camping areas lists prohibited items and identifies acceptable containers that may or may not be carried into the facility.
- Ensure that signage is provided throughout the facility that identifies current location relative to the exits, since most people will not be familiar with the facility. During an emergency, spectators frequently become confused as to their location in relation to the exits, and vital response time is lost.
- Ensure that signage clearly marks what type of access is allowed through a particular area. Signage is also recommended for directing delivery trucks to their appropriate destination and checkpoint.
- Ensure that signage is clearly visible at all pedestrian and vehicular access gates, and indicates that entrance to the facility is conditional upon compliance with all established screening and facility policies.
- Ensure that emergency exits are clearly marked to allow for a smooth flow of patrons exiting the facility.

## Event Day Operations: Gate Access and Management

The gate access and management protective measures described below should be considered for use during a sporting event. Responsibilities for implementing the gate access and management actions will be defined by the ICS.

- Train security employees in proper inspection procedures and identification of suspicious items. Train, equip, supervise, and provide security personnel with all of the tools necessary for them to complete their mission. Written responsibilities and duties (Post Orders) for each position (one dual-sided page maximum) should be available that link job function to the overall protective measures and safety program. Emergency instructions or cards that link job function to the Facility Emergency Action Plan should also be available for each position.
- Hiring and training of security personnel should be in accordance with State and local requirements. Several States require that security personnel be screened and trained in order to be licensed. Recommended training includes first aid, CPR, crowd management, drug awareness, emergency response, and defensive techniques. Practical exercises in facility-specific evacuation and sheltering-in-place plans should also be taught to security personnel. Consider providing security awareness and training programs to non-security employees (e.g., food service personnel).
- Post uniformed police officers at each gate to observe suspicious behavior (e.g., individuals looking for weakest security) and to backup searchers. Encourage police to be visible and among the crowd. Inform police officers of the facility's procedures for screening individuals entering the facility.
- Create a policy that identifies any item that is forbidden within the facility. Prohibit coolers, large backpacks, large bags, explosives, and weapons. Use a template at each public access control gate to show allowable package size. Ensure that owners of restricted items dispose of (but not abandon) them in order to gain entrance to the facility.



(Photos courtesy of National Football League)



- Publicize the list of prohibited items and the inspection policy. Send policy notices in advance to season ticket holders and to mass transit system operators. Post signage and distribute leaflets at the facility, at satellite parking areas, and at logical transit sites. Use loop announcements and employees at key locations to provide information concerning allowable/prohibited items.
- Designate an entrance for all concessionaires, gatekeepers, ushers, and cleaning personnel.

- Ensure that an adequate number of employees are available at the access control gates to efficiently handle security checks.
- Consider opening all main access control gates at the same time. Keep ticket collection responsibilities separate and distinct from security responsibilities. Conduct security checks and/or personal searches for prohibited items prior to ticket collection. Use tables for bag/purse searches and instruct staff not to reach hands into bags; patrons should be instructed to move items around inside of their bags instead.



(Photo courtesy of National Football League)



(Photo courtesy of Major League Baseball)

- Install CCTV equipment at all access gates that can be monitored from the CP/UJOC in order to provide a more comprehensive view of the venue and to ensure that digital images are available for use should an incident occur.
- Create a regular maintenance program to ensure that the CCTV system is meeting operational requirements. Try to avoid having to conduct CCTV maintenance during an event.

## Event Day Operations: Personal Searches

Personal searches may include visual inspections, pat-downs, metal detectors, and/or inspection of items brought into the stadium. Facility management as well as individual sports teams should take into consideration the type of sporting event, the teams/event participating, past event history, team requests, and current world climate when making decisions regarding personal and visual searches.

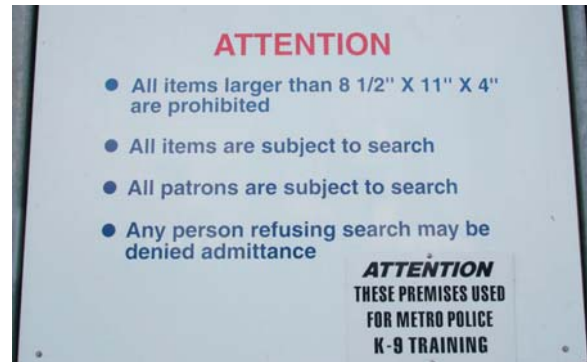


(Photos courtesy of National Football League)



The protective measures for personal searches described below should be considered for use during a sporting event. Responsibilities for determining the appropriate personal search procedures and implementing those procedures at events should be defined by the ICS. Facility management should be prepared to implement heightened personal searches in the event that security conditions change, such as DHS elevating the Homeland Security Alert level.

- Determine conditions and develop procedures regarding when individuals entering the facility will be subject to personal searches, including whether searches will be conducted randomly or on a mandatory basis for all individuals entering the facility.
- Develop procedures for the use of any metal detectors, pat-downs, and/or bag inspections.
- Develop procedures for personal searches of small children and disabled patrons.
- Train security inspection employees on the proper procedure for conducting personal searches.
- Deploy obvious signage informing patrons that they are subject to search as a condition of entry into the facility. Provide audio announcements over available external PA systems. Post notice of search procedures on the facility and/or sports team's Web sites.
- Provide notice of the search procedure at ticket sale locations, within season ticket mailings, and on ticket faces.
- Deploy security personnel in front of the facility access control gates to conduct personal searches of patrons prior to ticket taking and admittance into the facility.
- Inspect all items allowed into the facility, and visually inspect outer clothing.
- Designate locations adjacent to access gates where personal searches will take place.
- When screening with magnetometers or portable metal detectors (i.e., wands), visually inspect any item that activates the detectors.
- Ensure that standard inspections are also applied to full-time employees, event staff, and the media. Assign team staff members to identify all players, coaches, team members, and employees who enter the locker rooms and other restricted team areas.
- Institute a policy that male employees will search male patrons, and female employees will search female patrons.
- Establish separate lines at entrances for individuals who are carrying permissible bags, if possible, in order to allow for more expedient checking of those patrons who are not carrying items.



(Photo courtesy of National Football League)





(Photo courtesy of National Football League)



(Photo courtesy of Major League Baseball)

- After inspection, apply color coded tags to all media and employees bags allowed into the facility. The color-coded tags should be changed for each event, and all previous tags must be removed from the bag before affixing the current color-coded security tag.
- Refuse entry to the facility to individuals who decline to be searched.
- Utilize the ICS to address incidents where dangerous prohibited items (e.g., weapons) are discovered.
- Establish procedures for incidents where non-dangerous prohibited items (e.g., noise makers) are discovered.

## Event Day Operations: Credential Procedures

The protective measures for credential procedures described below should be considered for use during a sporting event.

- Devise credential systems that indicate the following:
  - Areas of access / Event function
  - Areas of sensitivity (e.g., protective measure needs, facility needs, event needs, media needs, and financial control needs)
  - Purpose of activity on facility premises (e.g., media, concessions, security)
- Design and color code credentials (“color of the day”), and ensure that they are substantially different from those used during prior seasons. Provide a hologram or other protection on the credential to reduce the potential for counterfeiting.
- Conduct roster checks on all personnel employed during an event.
- Require written requests for credentials (including media) prior to the event. Require those designated to pick up credentials to do so in person using photo IDs.



(Photo courtesy of Major League Baseball)



- Maintain a record of persons issued credentials for control purposes. The entry criteria into restricted areas of the facility should be agreed upon in advance. When necessary, a supplementary credential (e.g., a wristband) can be issued to an individual for access to a particular event or area of the facility. Sequentially number credentials for control.
- Ensure that all event employees, media, contractors, team members, and vendors wear IDs issued by the facility management. All temporary employees, contractors, and vendors should be issued daily passes that correspond to the “color of the day.” Do not issue passes until receiving verification from a point of contact within the venue. Ensure that passes are returned to security by all persons exiting the facility. Identify all individuals who do not return passes, and alert security personnel.
- Issue photo credentials to all regular Event Day teams, staff, and media. Regular facility employees may be allowed to use their everyday credentials on Event Days.
- Require that credentials be worn at all times and clearly displayed. Require all team bench staff (except for players in uniform) to wear an event credential. To assist with access control, display credential boards/access documentation guides at all access control points.
- Train access control personnel in credential recognition, access, and resolution of problems.

## **Event Day Operations: Food and Beverage**

The food and beverage protective measures described below should be considered for use during a sporting event.

- Ensure that all food concessions are reasonably secure.
- Inform food distributors before deliveries are made that any box, package, or container that is open, or appears to be tampered with, will be refused.
- Notify food distributors and local law enforcement of actual or suspected tampering incidents.
- Inspect packages and containers for tampering. If tampering is suspected, a supervisor should be notified, the incident documented, and the delivery refused.
- Conduct background checks on all food service employees and potential applicants. Supervise food service employees during the preparation and distribution of food. Train all food service employees on emergency procedures. Establish emergency procedures regarding recalled food and the immediate closing of concession stands.
- Inform food service managers and/or supervisors of the possibility of food contamination. Train food service managers and supervisors in methods to prevent and identify food contamination. Food service managers and/or supervisors should monitor food deliveries.
- All food and beverage deliveries should be recorded with the date, time, vehicle registration number, and company name. Obtain identification information from the person(s) making deliveries.

- Place portion-control packages in a location that is highly visible and readily monitored. All condiments in food courts should be individually packaged and not offered in bulk. If not, food toppings such as onions, relish, peppers, etc., should be supplied directly to patrons by concession food servers. Open and accessible items are subject to having contaminants easily introduced.
- Have a defined alcohol policy for facility concessionaires. This policy should contain guidelines with respect to:
  - Beverage limits per customer at point of sale,
  - Serving size restrictions,
  - Checking of photo identification for age-appropriate verification,
  - Cut-off times for alcohol sales,
  - Guest Services personnel training program regarding alcohol management,
  - Signage/PA announcements on alcohol policy, and
  - Arena policy on intoxicated patrons

## Event Day Operations: Aviation

Aviation may be a major consideration during some events. There may be “flyovers” by military aircraft, parachute drops by military units, use of airplanes and/or blimps for media coverage, and actual take-offs and landings by helicopters next to or within the outer perimeter.

The aviation protective measures described below should be considered for use during a sporting event. Responsibilities for implementing aviation protective actions will be defined by the ICS.

- Involve the FAA when planning and conducting any on-site events that include aviation activities. The FAA is required to issue a Special Notice pursuant to 14 CFR Section 99.7, which states that “commencing one hour before the scheduled time of the event until one hour after the event, all aircraft and parachute operations are prohibited at or below 3,000 feet within a three nautical mile radius of any stadium having a seating capacity of 30,000 or more people in which a Major League Baseball, National Football League, National Collegiate Athletic Association Division One football, or major motor speedway event (NASCAR Nextel Cup series and INDY Racing League) is occurring.” Operators of aircraft within the temporary flight restriction area must obtain a waiver from the Transportation Security Administration.
- Obtain copies of Pilots Certificates, Medicals, Insurance, and Part 135 certificates listing aircraft that are to be flown with “n” numbers listed. Ensure that these copies are available in the CP.
- Request that the FAA conduct a mandatory meeting for all pilots one day prior to commencing event flights. Provide printed copies of mandatory routing, checkpoints, and communication frequencies at the meeting. Use a sign-in sheet to ensure compliance.
- Request that the FAA establish and assign holding patterns for inbound aircraft to avoid traffic overload when the aircraft will be landing within the facility (e.g., on the infield of a racetrack), and establish a staging area within three miles of the facility.
- Require two-way communications between aircraft approved to land at the facility and air traffic control before the pilot reaches the first assigned checkpoint preceding the facility’s outer perimeter. Require the same once the pilot is ready to take off for departure from the facility.

## **Event Day Operations: Team/Officials Security**

Particular protective measures should be put in place to ensure the safety and well-being of event officials, teams, and event participants. If an incident requires immediate evacuation, both the visiting and home teams, as well as event officials, should be escorted to a pre-determined, secure location by facility security personnel. The designated location should be communicated by the facility to the League Security Office at the beginning of each season. Any change will require additional notification. The protective measures described below should be considered for use to address team/officials security.

### ***Security of Event Officials***

- Ensure that the event officials are identified by photo ID prior to entry into the facility. Their bags should be searched and tagged. All old stickers and tags must be removed prior to placing any new inspection tags on bags. Their vehicles are subject to screening and search procedures.
- Post a security guard at the officials' locker room. Ensure that their personal property is guarded. Unauthorized people should not be permitted to interfere with the officials. Escort the officials into the event.
- Ensure that canopies or other protective devices are in place to protect the officials from patron contact or from objects thrown by the crowd.
- Escort officials to their vehicles for departure from the facility.

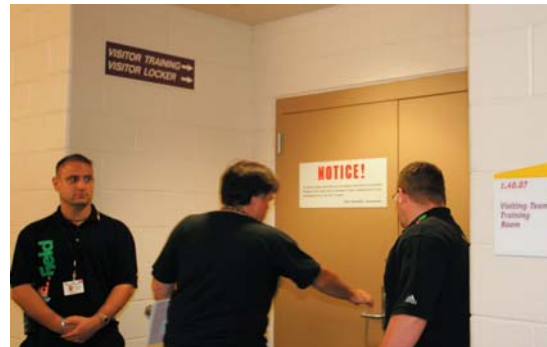
### ***Visiting Team Locker Room and Security Responsibilities***

- Assign responsibility to the designated team security person for ensuring that all visiting team, staff, and traveling party carry-on bags and luggage have been inspected and tagged.
- The equipment manager and/or his staff should supervise the unloading and loading of the visiting team's equipment truck. Lock and/or secure the loaded truck with a tamper-proof seal.
- Require bus companies to provide the identity of their drivers. Security personnel and/or escort officers should inspect buses and confirm the identities of the drivers. Buses should be locked, and the drivers should remain with the buses in a secured area. Post a security officer in that area, if necessary.
- Provide security personnel either from the facility or from the visiting team to escort the visiting team between the buses and the visiting team's locker room.
- Issue credentials to all team staff to be worn inside the facility during warm-ups and the event. Players/officials in uniform are the only persons not required to wear a credential.
- Ensure that the visiting team locker room areas are clear of any unauthorized personnel and sufficiently staffed with visible security personnel.
- Post a member of the visiting staff at the locker room door to visually identify team players, staff, and other authorized personnel.

- Canopies or other security devices should be in place to prevent fan contact and/or objects that might be thrown from the stands.
- A sufficient security presence should be in place behind and around the visiting team during the event to prevent contact between fans and players. Any fan behavior (e.g., profanity; throwing objects; threats directed at players, coaches, or officials) should be addressed immediately by security. Written or verbal warnings to cease such behavior should be directed to the errant fan(s). Failure to comply may be cause for relocation, removal from the facility, or arrest.

### ***Home Team Locker Room and Security Responsibilities***

- A designated team person should confirm that all player and staff bags have been inspected and tagged.
- Issue Event Day credentials to team staff to be worn during the event. Players and officials in uniform are the only exception. Non-uniformed players should be provided with an Event Day credential to wear during the event.
- Post a person representing the home team at the locker room door to visually identify team players and staff entering the facility.



(Photos courtesy of National Football League)

- The equipment manager and his staff should supervise the loading of the equipment truck, which should be locked and/or secured with a tamper-proof seal. The identity of the truck and any bus driver should be confirmed.
- Ensure that the team locker room areas are clear of any unauthorized personnel and sufficiently staffed with visible security personnel.
- Canopies and/or other security devices should be in place to prevent fan contact and/or objects that might be thrown from the stands.
- A sufficient security presence should be in place behind and around the visiting team during the event to prevent contact between fans and players. Any fan behavior (i.e., profanity; throwing objects; threats directed at players, coaches, or officials) should be addressed immediately by security. Written or verbal warnings to cease such behavior should be directed to the errant fan(s). Failure to comply may be cause for relocation, removal from the facility, or arrest.

## Event Day Operations: Miscellaneous

The miscellaneous protective measures described below should be considered for use during a sporting event. Responsibilities for implementing the miscellaneous protective actions will be defined by the ICS.

- Prior to the opening of the facility to the public, convene a meeting between the facility's Security Director or authorized representative and the sanctioning league and/or team security representatives, referees, and any League Security personnel to discuss procedures; potential player, fan or team rivalry issues; emergency response procedures; emergency egress; and/or any unique concerns pertaining to the event.
- Dedicated advanced life support ambulances should be on site and staffed by qualified medical technicians. All ambulances, unless responding to an emergency at the facility, must be inspected before entering the facility perimeter. A backup ambulance or procedure should be in place in the event that the primary unit has to leave the facility to transport a patient to the hospital. Drivers must remain within close proximity to their emergency vehicles at all times.
- Periodically empty trash receptacles during the event. Utilize clear plastic bags for all trash receptacles.
- Do not refill propane tanks during an event when the facility is loaded with spectators.
- Designate secure smoking areas. Establish inspection procedures for patrons entering and leaving the smoking area. Do not allow non-patrons near established smoking areas.
- Areas where special equipment (e.g., Zamboni, golf carts, half-time equipment, emergency response vehicles) is stored for use during the event should be secured and accessible only to authorized personnel with the appropriate credentials.
- Test backup equipment (i.e., generators, communications equipment) before the event.
- Security, emergency response, and public safety personnel can be exposed to blood through needle sticks and other sharp injuries, mucous membrane, and skin exposure. Facility management and employees are urged to take advantage of available engineering controls and work practices to prevent exposure to blood and/or other body fluids.
- Supply all ushers and security employees with flashlights for indoor, outdoor, and evening events.
- During sporting events thousands of dollars in cash may be collected at ticket booths and concession stands. In many instances, the law enforcement organization overseeing security at the event is also responsible for protecting cash collections. This protection includes securing the cash from external robbery and from employee theft or loss. Frequently, a central bank exists for cash turn-in. Special attention should be afforded this bank to include uniformed officers and CCTV coverage. Regular armored car pickups should occur to reduce more than one day's revenue remaining on site.
- Coordinate efficient exit flow for vehicles. While traffic arriving at an event may be staggered over a period of one to eight hours, nearly all event spectators attempt to exit the parking areas at the same time once the event is over. Some people may leave the event having consumed too much alcohol. Sitting in heavily-congested traffic for a long period of time may contribute to road



rage, which could contribute to accidents, disruptive behavior, etc. Facility and security employees should monitor parking lots associated with the facility and part of the “outer perimeter” to ensure timely and safe exiting from the event.

- Employ the same level of concern for unauthorized entry into the facility while spectators are exiting. Ensure that adequate security and event staff members are present to deal with the large crowds exiting the facility all at once, and that they pay particular attention to those individuals wishing to enter the facility at the end of an event.

## Areas of Special Concern

There may be areas within the outer perimeter of the facility that need special protective measures beyond the general guidelines provided in this guide. Protective measures for these areas of special concern may be developed through consultation with the facility, the sports league involved, and appropriate law enforcement organizations.

Some examples include the following:

- Tailgate activities in designated areas, and
- Motor Sport Facilities, including
  - Speedway Pits,
  - Speedway Garage Area Enclosure,
  - Speedway Competitor Motorcoach Area Compound, and
  - Speedway Campground.

## Special Considerations for Adjacent Facilities

The ICS should determine if sporting event facilities may be impacted by other facilities that are located within close proximity of the venue or that have operations occurring nearby to the sporting event facility. The development of a Facility Emergency Action Plan should involve, whenever possible, a designated representative from each nearby facility in order to address potential impacts that those facilities’ activities may have on an event, the spectators in attendance, or the sporting event facility. Options that may mitigate risks during an event should be explored (e.g., delaying movement of hazardous materials on event days).

Sporting event facilities may:

- Be within a short distance of civilian or military airports or their flight paths;
- Be within close proximity to a hazardous materials processing facility;
- Be Adjacent to railroads that transport hazardous chemicals;
- Fall within the inundation area of an upstream dam; or
- Fall within a 20-mile radius of a nuclear reactor.

If the ICS determines that an adjacent facility or activity poses a threat to the sporting event facility, the event facility manager should ensure that all Federal, State, and local emergency management and regulatory agencies, as well as the sporting event facility employees, have a clear understanding of evacuation or shelter-in-place procedures and resources that would be needed if an incident occurs at an adjacent facility.

The impacts of an incident or unauthorized release from nearby facilities should be documented.

## After-Action Reviews

An ICS After-Action Review is an important component of the emergency security and safety process. This review should critique what activities and/or incidents occurred during a sporting event, and how well the protective measures and safety functions were implemented. It should also include an assessment of what worked well, what could be improved upon, and what lessons were learned.

The After-Action Review should incorporate verbal discussions, written reports from the event, any arrest reports, complaints, video of the event, and interviews with key individuals (i.e., facility managers, sports league, competitors, security, and media representatives).

Lessons learned should be identified in the report, and a list of recommendations should be compiled for implementation. When planning begins for the next event, previous After-Action Reports should be reviewed for utilization of lessons learned and implementation of recommendations.

For a one-day event, the After-Action Review should occur within 48 hours of the event's completion. If the event extends over multiple days, it may be advantageous to conduct a review at the end of each day's activities to allow for the benefit of making mid-course adjustments during the event.

Provide the After-Action Report to all agencies and organizations that participated in the protective and safety measures of the event. At the conclusion of this process, any applicable recommendations from the report should be incorporated into the Facility Emergency Action Plan in preparation for the next event.

## Appendix A

### Acronyms

CCTV	Closed Circuit Television
CP	Command Post
CPR	Cardiopulmonary Resuscitation
DHS	Department of Homeland Security
EMS	Emergency Medical Services
IC	Incident Commander
ICS	Incident Command System
IED	Improvised Explosive Device
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
HSAS	Homeland Security Advisory System
HVAC	Heating, Ventilation, and Air Conditioning
IAAM	International Association of Assembly Managers, Inc.
ID	Identification
OC	Operations Center
PA	Public Address
UJOC	Unified Joint Operations Center
UCS	Unified Command System
VBIED	Vehicle-Borne Improvised Explosive Device
VIP	Very Important Person

## Appendix B

### Codes, Regulations, Standards, and Guidelines

The following list provides examples of available resources that address protective measures.

Occupational Safety and Health Administration

Environmental Regulations

Fire Codes

Seismic Safety Codes

Life Safety Codes

Transportation Regulations

Zoning Regulations

Corporate Policies

Sports Leagues Policies and Guidelines

Special Events Planning Guides

- Federal Bureau of Investigation
- United States Secret Service

Professional organization standards and guidelines

- ASIS Risk Assessment Guideline
- IAAM Best Practices Planning Guides

State Homeland Security Guidelines

Department of Homeland Security

- *Incident Communications Emergency Reference: A Guide for Communications Professionals*
- Common Vulnerabilities, Potential Indicators of Terrorist Activity, and Protective Measures Reports for Stadiums, Arenas, and Speedways
- Vulnerability Identification Self-Assessment Tool available for stadiums, arenas, and speedways.

## Appendix C

### References

- *Best Practices for Stadium Security*. The National Football League. 2002.
- *Best Practice Planning Guide for Arenas, Stadiums, and Amphitheaters*. International Association of Assembly Managers. 2003.
- Connors, Edward. *Planning, and Managing Security for Major Special Events: Guidelines for Law Enforcement*. The Institute for Law and Justice. Alexandria, 2007.
- *Counter Terrorism Protective Security Advice for Stadia and Arenas*. National Counter Terrorism Security Office (UK).
- Ingersoll Rand Security Technologies. *Security and Safety Guideline Reference Manual, Version 1.0*. NASCAR, Inc. 2006.
- *Recommendations for Arena Security*, revised. National Hockey League. 2005.
- Rodriguez, Michael J. *Security Procedures Manual*. U.S. Tennis Association. National Tennis Center, 2005.
- *Team Security Survey*, updated. Major League Soccer. 2006.



