IAAM Safety and Security Task Force
Best Practices Planning Guide
Arenas, Stadiums, Amphitheater

Introduction
Public assembly facilities around the world host the largest mass gatherings of people on a regular basis, and thus are considered possible targets of terrorism and social disorder. Safety and security measures, though prevalent in most venues, are now more overt in nature and extensive in options, but must repeatedly be reviewed and evaluated for circumstantial/situational conditions.

Following the September 11, 2001 terrorist attacks on America, the International Association of Assembly Managers (IAAM) formed the Safety and Security Task Force (SSTF) to conduct research and to assess and develop an ongoing series of Safety and Security Protocols. These protocols will include "best practices," position statements and training materials on issues related to safety and security at public assembly facilities.

IAAM President Lionel Dubay, director of the Stephen C. O'Connell Center at the University of Florida, formed the SSTF under the leadership of Chair Frank Poe, CEO, Birmingham Jefferson Convention Complex, and Vice Chair Larry Perkins, CPP, Assistant General Manager, Raleigh Entertainment & Sports Arena. Complete SSTF membership, mission and charges for the task force can be found in **Exhibit I.**

A result of the successful formation of the task force, IAAM established the Center for Venue Management Studies as a source for distribution of information on pertinent industry issues. The first installment of Safety and Security Protocols, Best Practices Planning Guide, developed by the task force and released by the Center, focuses on procedures to be used at sports/performance venues such as arenas, stadiums and amphitheaters. Additional protocols, such as planning guides for convention centers and performing arts venues as well as emergency preparedness and crisis communication will be developed in subsequent months. Also to be released by the Center includes information on venue architectural issues and position statements on concealed weapons laws.

The following Best Practices Planning Guide for safety and security at sports/performance venues comprises several documents that aid in assessing risk factors and determining terrorist threat levels. A checklist is also provided that can be utilized in the formulation safety/security plans at public venues for any given event or related activity.

Venue management should adopt a planning process that includes the following steps:
- Assess risk factors
- Determine threat levels

- Develop and implement the safety/security plan

Assessing Risk Factors and Threat Levels
Many governmental agencies have taken steps to establish command structures and communications plans to advise the public concerning terrorist threats in the new environment. The suggested range assumes a system using a five-level structure of threat—Red (Severe), Orange (High), Yellow (Elevated), Blue (Guarded), and Green (Low). See **Exhibit II.**

In light of the new threats, the IAAM Safety and Security Task Force recommends that facilities establish contingency plans based on levels of threat. A decision tree is useful in establishing threat levels. Though based in part on terrorist threat conditions as defined, the decision process is applicable in other national and international contexts and for situations that contain threats not associated with terrorism.

Most venues have emergency plans, event plans and other planning procedures to establish and implement safety/security practices. Even in cases without terrorist threat, venues may face other serious threats, such as crowd behavior, natural disasters, etc. To that end, risk factors must be evaluated for each event, regardless of program. A list of common risk factors can be used for determining safety/security plans for any particular event.

IAAM's Suggested Risk Levels
The Safety and Security Task Force recommends a four-tiered system for establishing threat levels at venues. The following table provides an explanation of the general issues and illustrates the corresponding relationships between a five tier Governmental Alert System and venue threat levels.

GOV'T RATING	RISK LEVEL	VENUE THREAT	Security Measures	ACTION STEPS
Severe		Cancel	Secured	"Lock-down" patrol of perimeter restricting all access.
High	4	Maximum	Gov't Control	National law officials / security agencies screen public and control
Elevated	3	Elevated	Restrictive	May involve regional or local law officials with "pat-down" measures.
Guarded	2	Moderate	Protective	Limited Access to venue with screening precautions implemented.
Low	1	Minimum	Routine	No primary factors of concern exist outside normal routine measures.

SSTF Event Decision Tree

Analysis to Determine Security Level and Measures for an Event

On a daily basis the manager of a public assembly facility is required to make decisions concerning safety and the level of security in and around his or her facility. In order to determine the level of security necessary to protect life and property, the facility manager or event manager must consider and evaluate many factors related to an event. Some factors, that must be considered, are whether the event is open to the public, the number and nature of attendees, whether senior government officials will attend the event, the general profile of the event, the country and specific location of the facility, any applicable laws and of course any information and recommendations from law-enforcement officials. With the increased threat of terrorism and the general decrease in private or public funding, managers must weigh or balance the risks and take security measures that substantially reduce or eliminate security risks. Therefore, in order to assist the manager in the security planning process, the IAAM SSTF has developed a general list of considerations to determine the level of security planning required for an event. For the purposes of simplicity, we have created four levels of security planning. Level #4 is the maximum security possible followed by Level #3 which includes a high level of planning and measures. Level #2 includes a moderate level followed by Level #1 which is the minimum level of security for an event. You may determine that your facility requires Level #1 measures in one area and Level #3 measures in another of area of the facility. Please note that the following is provided to you only as factors to consider in your security analysis and does not in any way adequately assess the security risks or the security measures that should be taken for any specific event or facility.

Level #4 Security Measures (High Degree of Security Risks)

Level #4 is the highest level of security measures and may involve the United States Secret Service, the Federal Bureau of Investigation (FBI) and other national or international law enforcement and public safety agencies controlling the security at the event. For national security purposes, Level #4 requires strict measures that severely limit access to the perimeter of the facility prior to and during the event. Each employee, contractor and patron is screened for weapons and other prohibited items through magnetometer checkpoints. Suggested security measures may include all of the security items listed in the SSTF Best Practices.

a) The event is considered a “special event” under the U.S. Homeland Security Act or is an equivalent event in your country.
b) The U.S. Secret Service is required to protect a participant or certain event attendees.
c) The event requires coordination and participation by national, regional, state and local law enforcement and public safety officials.
d) Local and State Law enforcement officials cannot carry weapons into the secure perimeter.
e) The event is most likely open to the public.
f) The event is a highly public event with thousands of patrons and may include participants or patrons from other countries.
g) The event otherwise presents a severe or high degree of security risks.

Level #3 Security Measures (Elevated Degree of Security Risks)

Level #3 is the second highest level of security measures and may involve the Secret Service, the Federal Bureaus of Investigation (FBI and other national or international law enforcement and public safety agencies on a limited basis or for specific security concerns. Level #3 requires strict security measures that severely limit access to all or part of the facility prior to and during the event. The facility or event manager controls the remaining areas of the facility. Each patron (and possibly contractors and

employees) is screened for weapons and other prohibited items through magnetometer checkpoints. Suggested security measures may include the security items listed in the SSTF Best Practices Guide. The following are some characteristics of a Level #3 event:

a) The event requires coordination and participation by national, regional, state and local law enforcement and public safety officials.
b) The event is most likely open to the public.
c) The event may be televised nationally or regionally and will most likely attract government officials as patrons and speakers.
d) The event is a highly public event with thousands of patrons and may include participants or patrons from other countries.
e) The event may attract patrons that carry weapons.
f) The event may attract patrons that abuse alcohol or drugs.
g) Law enforcement assessed the event as having a high degree of security risks.

Level #2 Security Measures (Guarded Degree of Security Risk)

Level #2 is the third highest level of security measures and may involve regional, state and local law enforcement and public safety agencies. Level #2 requires moderate security measures that may limit access to the facility prior to and during the event. The facility or event manager controls the security of the facility. Each patron is screened or patted down for bottles, cans and other prohibited items through entry checkpoints. Suggested security measures may include the security items listed SSTF Best Practices Guide.

a) The event may require coordination with regional, state and local law enforcement and public safety officials.
b) The event is televised nationally or regionally and may attract government officials as patrons and speakers.
c) The event is a highly pubic event but does not generally include foreign participants or patrons.
d) The event may attract patrons that abuse alcohol or drugs.
e) The event has not been identified by law enforcement as having any particular threat outside the customary or ordinary event (sporting, theatrical, musical or convention) that takes place often in your area or country.
f) Law enforcement may have assessed the event as having a moderate degree of security risks.

Level #1 Security Measures (Low Security Risk)

Level #1 is the minimum amount of security Measures for an event. This event does not require the higher levels of security planning or security measures. An analysis of the event, the number of attendees, location, television coverage, if any, the invited guests, presents no primary factors of concern outside the normal concerns for security after September 11, 2001. All the events not classified in the other levels fall into this Level. Suggested security measures may include the security items listed in the SSTF Best Practices.

a) The event is a regional or local event that, based upon the number of attendees, the nature of the event and invited guests, presents a minimum security risk; or
b) The event is not televised or is only televised locally and
c) The event does not include government officials; or
d) The event otherwise presents only a minimum degree of security risks.

This Decision Tree provides a method to determine security level based on the IAAM "Best Practices" Safety and Security Guide for Arenas, Stadiums, and Amphitheaters. The IAAM SSTF has identified four levels of threat, requiring appropriate safety and security measures. Level #4 is the high security possible followed by Level #3, which includes an elevated level of threat, Level #2 with guarded level of threat followed by Level #1, which is the minimum level of threat of safety/security for an event.

Using the decision process questionnaire, facility/event management can determine the risk factors and what levels of threat are possible. Outcomes may vary by venue due to location, design, proximity relationships, and other profile factors not included in this document.*

Questions. Circle answer (yes / no) to guide decisions.

Has the Government issued a "Severe Condition" warning?

No ¯ Yes ® Management should implement Level 5 Security Practices..

Has the Government issued a "High Condition" warning?

No ¯ Yes ® Management should implement Level #4 measures.

.

Has the Government issued a "Elevated Condition" warning?

No ¯ Yes ® Management should implement Level #3 measures where applicable.

Has the event been classified by the Government as a "Special Event?" (In the U.S., the Office of Homeland Security designates certain events, primarily those with the U.S. President and/or high government officials attending, as "Special Events" under Secret Service control.)

No ¯ Yes ® Management should implement Level # 4 measures.

Do any event guests or speakers require Government protection?

No ¯ Yes ® Management should implement Level #3 measures.

Will any senior government officials or international officials be attending the event?

No ¯ Yes ® Have specific and credible threats been received by the event organizers or police?

¯ Yes ® Management should implement Level #3 measures.

Is the event being broadcast nationally or internationally?

Yes® Management should consider implementing Level #3 measures.

Have specific and credible threats been received by the event organizers or police?

No ¯ Yes ® Management should implement Level #3 measures.

Will the event otherwise attract national or international attention? Consider event history.

No ¯ **Yes ®** Have specific and credible threats been received by the event organizers or police?
¯ **Yes ®** Management should implement Level #3 measures.

Are there any high profile elements/situations or icons existing in nearby proximity to the venue?

No ¯ **Yes ®** Management should implement Level #2 measures.
Have specific and credible threats been received by them?
¯ **Yes ®** Management should implement Level #3 measures.

Does event attract a mix of market demographics that are diametrically opposed?

No ¯ **Yes ®** Management should implement Level #2 measures.
Is there a history of violence among the participants?
¯ **Yes ®** Management should implement Level #3 measures.

Will the event attract patrons that abuse drugs or alcohol?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to prevent abuse of drugs or alcohol.

For sports events, does the event attract patrons with intense rivalries?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to limiting conduct, such as preventing abuse of drugs or alcohol.

Are patrons inclined to storm the field of play or rush the stage at performance?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to prevent risks.

Are patrons inclined to throw objects?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to prevent risks.

Does the seating configuration include festival seating?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to provide adequate barricades, trained peer security, and medical services.

Is alcohol being served?

No ¯ **Yes ®** Level #2 event - Special precautions must be made to prevent alcohol related incidents.

Do patrons/fans tend to customarily gather early or socialize (tail-gate) at venue prior to the event?

No ¯ **Yes ®** Level #2 event - Special precautions must be taken to monitor and control crowd behavior.

Has there been a National Weather Service warning issued?

No ¯ Yes ® Level #2 event - Special precautions must be taken for emergency response. See Emergency Planning and/or Crisis Management.

Does the event present any other security or safety risks?

No ¯ Yes ® Management should consider specific risks and take protective security and safety precautions.

If none of the above applies to the event, use IAAM SSTF Level #1 minimum safety and security measures.

*** Please note that the Decision Tree is provided to you only as factors to consider in your security analysis and does not in any way adequately assess the security risks or the security measures that should be taken for any specific event or facility.**

Key:

- **Bullets indicate suggestions for when to implement Security Procedure. These are only general guidelines. All decisions must be made in light of your particular circumstances.**

IAAM SAFETY & SECURITY TASK FORCE
BEST PRACTICES PLANNING GUIDE

Arenas - Stadiums - Amphitheaters

Risk Levels				Security Procedures
1	2	3	4	
				1. Coordination with Outside Agencies
				Venue Management should designate employees to consult with representatives of appropriate public safety agencies:
			●	A. Local area (county, state, province, etc.) and national law-enforcement agencies (e.g., police, FBI, ATF, Secret Service)
●	●	●	●	B. Fire departments and hazardous materials response units
		●	●	C. Emergency management agencies
		●	●	D. Local elected public officials
	●	●	●	E. Emergency medical services
●	●	●	●	F. A group of individuals from each of these entities or groups should be identified to participate in assessing risks, conducting vulnerability assessments and fully developing all components of venue security procedures. These plans should address preparation, response, communication and recovery. The group should meet well in advance of the first event and schedule follow-up meetings with specific individuals as needed.

Risk Levels				Security Procedures
1	2	3	4	
	●	●	●	G. All agencies are encouraged to work together under the leadership of a primary individual who will coordinate security and communication efforts. It is recommended that these individuals form a security committee inclusive of representatives from all appropriate agencies.
				2. Persons with Disabilities
●	●	●	●	A. Review the applicable facility plans (e.g., Americans with Disabilities Act).
●	●	●	●	B. Ensure that measures taken do not compromise requirements pertaining to persons with disabilities.
				3. Venue Events
	●	●	●	A. Inspect all bags, including equipment bags and other containers of persons entering the venue.
	●	●	●	B. Require each licensee, organizer, team, etc. to provide a pass list, certified by management, of all representatives who will enter the venue.
		●	●	C. Venue management and lessees will not issue credentials to non-essential personnel or other persons.
	●	●	●	D. All event employees, media, contractors, exhibitors and vendors must wear IDs issued by management. All temporary employees, contractors, vendors, media and visitors should be issued daily passes that correspond to the "color of the day." Passes should not be issued until verification from their point of contact within the venue has been established. All passes should be returned to security upon exiting.
		●	●	E. Photo IDs "must" be worn at this level of 'heightened' security.
		●	●	F. No persons other than authorized user personnel and guests should be permitted in the dressing rooms, i.e. players, performers, spouses, coaches, media, staff, cleaning, maintenance, catering, etc.
		●	●	G. Artists and team members should not bring guests, other than immediate family, a significant other or friend into the back-of-the-house areas.
				4. Staffing Coordination
●	●	●	●	A. Identify the representatives of the agencies that will be involved in addressing preparation, response, community and recovery (see above). Develop a key-contact sheet listing the names and telephone numbers of these individuals.

Risk Levels				Security Procedures
1	2	3	4	
●	●	●	●	B. Determine any other individuals to be included in the communication loop. Develop a key contact sheet listing the names and telephone numbers of the emergency preparedness individuals involved in the response to any emergency situation in connection with the event, including cell and pager numbers.
●	●	●	●	C. Designate individuals who, in the event of a specific, viable threat, will make the final decision regarding cancellation of the event, evacuation of the venue, etc.
●	●	●	●	D. Develop a written evacuation plan. Rehearse the evacuation plan.
			●	E. Implement as needed two command centers in your venue: a main command and auxiliary. All agencies should be represented in the command post including facility management. An off site command center, at least two miles from the venue, must also be established.
			●	F. Create a direct communications link between facility management and the command post.
			●	G. Establish communication with a second command post located away from the venue site.
●	●	●	●	H. Determine how to handle bomb threats or other threatening/suspicious telephone calls. These procedures must be in writing.
●	●	●	●	I. Review venue and local incident response plans. Include coordination of medical response units.
●	●	●	●	J. Establish a time prior to doors opening to clear all persons from around gate positions and ensure these areas are ready to receive guests.
		●	●	K. Augment uniformed officers and private security officers as the situation warrants.
	●	●	●	L. Conduct a visual inspection of the venue, both inside and outside. Specially look for suspicious packages and other items.
		●	●	M. Prohibit vehicles from pausing or stopping in the perimeter (as defined by law enforcement and venue management), except for monitored, designated drop-off areas.
			●	N. Determine whether it is necessary to have a “hostage team” and/or a “SWAT team” available.

Risk Levels				Security Procedures
1	2	3	4	
		●	●	O. Inspect all buses (team, performers, contractors, etc.), then provide police escorts for them where applicable.
●	●	●	●	P. Review plans for handling protests or demonstrations both inside and outside the venue (Have a definitive policy in place for each).
				5. Coordination with Promoters/Organizers
●	●	●	●	A. Meet with promoter/organizers and artist security representatives prior to event to review special needs and security requirements.
●	●	●	●	B. Signs must be posted and clearly readable at doors listing items that are not allowed inside the venue.
●	●	●	●	C. No information on internal security measures should be released to the press. This is a precaution so as not to "tip off" the perpetrator.
		●	●	D. Promoters, artists, organizers, management, government, and teams will not issue credentials to non-essential persons.
				6. Deliveries
		●	●	A. Limit or prohibit all vendor vehicles during events.
	●	●	●	B. All deliveries should be accepted only at the designated receiving area. They should be documented and drivers should sign a delivery log.
		●	●	C. All drivers and driver's helpers should have a government or other official entity issued photo ID (such as a driver's license) and should be issued a daily color-coded credential, which must be collected upon exit.
		●	●	D. Implement a system for inspecting items delivered to the facility. After deliveries have been inspected, label the packages, cartons, crates, etc. so others will know they have been approved.
		●	●	E. Prohibit vehicular use inside the facility during the event.
				7. Venue Personnel
		●	●	A. Conduct background checks on all personnel to the extent possible.
●	●	●	●	B. Designate and limit access points and persons actually required to be on site.
●	●	●	●	C. Review with appropriate personnel the venue's plan for handling emergencies.

Risk Levels				Security Procedures
1	2	3	4	
●	●	●	●	D. Brief all personnel as to response procedures in the event of an emergency.
●	●	●	●	E. Supply all ushers and security with flashlights, if applicable, (e.g., night and indoor events).
●	●	●	●	F. All venue personnel must be on the lookout for anything out of the ordinary (persons, objects, actions, containers, vehicles, broken doors and air vents, etc.).
			●	G. Only authorized personnel with picture IDs should be allowed access before the start of event (also see section 3, item E above). Management must approve all other personnel, such as concessionaires, ushers, etc. prior to having access to the facility.
●	●	●	●	H. Designate a pre-approved entrance for all concessionaires, gatekeepers, ushers, and cleaning personnel.
●	●	●	●	I. Educate all appropriate staff on proper procedures for checking suspicious packages and heighten their overall perception of their surroundings.
●	●	●	●	J. Schedule training sessions with Event Staff and review training manual. This must cover all types of responses to specific emergencies. Evacuation mock drills should be done with employees and appropriate public safety agencies, if possible. It is incumbent that all employees attend any training sessions called no matter how long they have been working at the facility.
				8. General Public Entrance to Venue
●	●	●	●	A. Post signs, use external public-address systems and/or megaphones to inform event guests and others of bag-checking and prohibited-items procedures.
		●	●	B. Designate an area away from the venue for inspection of prohibited items (bags, packages, persons, etc.). This task may be accomplished at the perimeter fence, bottom of steps, etc. A clear zone may also be established for this purpose.
		●	●	C. Establish line control by using rope, stanchions or barricades to move event guests in single-file to and through each turnstile.
		●	●	D. Establish separate entrances for individuals who are carrying bags, if possible. This will allow for more expedient checking of those carrying items at the other doors.

Risk Levels				Security Procedures
1	2	3	4	
		●	●	E. Open venue doors earlier than normal. This will allow security ample time to check for prohibited items. Guests should be informed of this extra time and encouraged to arrive at the venue earlier.
●	●	●	●	F. Establish security control for pass out and return, i.e., re-inspect guests returning, restrict guests to a specific area outside the venue with control, do not allow non-guests near established smoking areas, etc.
		●	●	G. Prohibit pass out and return.
		●	●	H. The venue should be searched by security and secured at a designated time prior to the start of an event where possible.
	●	●	●	I. Venue management should take into consideration the type of event, past history, request of the artist, team management, organizers, etc. and current world climate when making decisions on when pat-downs and visual searches are conducted.
				9. Lockdown
●	●	●	●	A. Venue management should determine the length of time before and after the event to require credentials for admittance to the venue by individuals, (e.g., venue staff, exhibitors, contractors, competitors, officials, organizers, fans).
				10. Media
		●	●	A. Procedures for checking media bags through a visual search or the use of metal detectors must be determined by venue management.
		●	●	B. A media plan must be developed for heightened security events to specify credential requirements, press congregation/coverage/conference areas, and a specific spokesperson to keep media informed as required. Advance notice of the plan must be distributed.
				11. Metal Detectors
		●	●	A. Conditions must be determined and procedures established as to when individuals entering the facility will be subject to metal detectors (either wands or gates).
		●	●	B. Procedures must be established for the use of metal detectors and provisions for same if not owned.

Risk Levels				Security Procedures
1	2	3	4	
				12. Parking and Perimeter
		●	●	A. If possible, establish an outer perimeter for keeping unticketed and unauthorized individuals away from the venue.
		●	●	B. If possible, establish an outer perimeter with concrete barriers at strategic locations to keep unauthorized vehicles away from the venue.
		●	●	C. Distribute prohibited items and procedures information flyers at the parking entrances to educate guests and others.
		●	●	D. Establish 24-hour security at the perimeter beginning one or more days prior to the event.
		●	●	E. Inside the perimeter, permit only necessary parking (e.g., workers, authorized persons, venue personnel and media with passes, etc.)
		●	●	F. Inspect all vehicles entering the perimeter including players, performers and all other authorized vehicles. This may include a visual check of the interior with the dome light illuminated, truck and mirrored underside. Consider marking the vehicle to indicate it has been inspected.
			●	G. Prohibit all vehicles from parking inside the perimeter and/or loading dock areas.
		●	●	H. Determine the feasibility of creating additional emergency exits.
●	●	●	●	I. Working with local authorities, establish evacuation routes for pedestrians and vehicles.
		●	●	J. Review security around air vents. Inspect air intake units and know how to shut off air circulation system.
		●	●	K. Install vehicular impedance bollards at the ramps leading to the concourse and at any other entrances to the facility, if necessary.
		●	●	L. Temporary parking adjacent to the venue on the day of an event should be prohibited. Any other parking areas to be prohibited should be clearly marked.
		●	●	M. In parking areas controlled by the venue, all vehicles without proper identification should be parked at least 100 feet (30 meters) from the building.
●	●	●	●	N. Ensure proper exterior illumination of parking areas and perimeter, and that the external PA system is working and audible.

Risk Levels				Security Procedures
1	2	3	4	
			●	O. All team/performer/organizer buses should be restricted to a designated area and should be monitored 24 hours a day, 7 days a week.
●	●	●	●	P. All exterior garbage receptacles must be emptied as close to event time as possible and periodically checked throughout the event and do not bring outside trash inside venue.
	●	●	●	Q. Particular vigilance must be exercised in the parking areas (especially public areas) that are adjacent to the venue structure.
●	●	●	●	R. All exterior garbage/trash receptacles should be sealed. and inspected regularly.
				13. Prohibited Items
●	●	●	●	A. Establish specific dimensions for bags that are acceptable to be brought into the venue and publicize the dimensions
		●	●	B. Media, team, performer, exhibitor, etc. Inspect all bags and once inspected, tag it to identify it as having been checked.
●	●	●	●	C. If a security alert warrants, all bags should be prohibited.
		●	●	D. Prohibit backpacks, waist packs, purses, coolers, and other items deemed by management to be inappropriate and/or a safety hazard.
	●	●	●	E. If the situation warrants, prohibit all still cameras, audio and video recorders, televisions or any other devices with batteries into facility hosting events. Note: Credentialed media may carry devices necessary for their work and security personnel must inspect those devices. One or two media entrances should be designated for the event.
●	●	●	●	F. Develop a list of prohibited items that includes all bottles, cans, food and other containers except in cases of medical needs of guests.
●	●	●	●	G. Instruct all patrons to dispose of all prohibited items prior to entering the venue.
●	●	●	●	H. If possible, intercept parking lot patrons who are carrying bags and other items that are contrary to policy and ask that these items be returned to their vehicles prior to seeking admittance.

14. Public Relations				
Risk Levels				**Security Procedures**
1	**2**	**3**	**4**	
●	●	●	●	A. Notify public of specific measures affecting them (e.g., items not permissible inside the venue, gate-opening times, plans for use of metal detectors or physical searches), although it is not necessary to publicize all specific measures you will take.
		●	●	B. Post fliers and signs at hotels and other places where guests may gather; signs and public address announcements in and around the venue; media releases; mailings to ticket-holders; and fliers distributed at the box office and ticket agencies.
●	●	●	●	C. A similar announcement should be made as patrons are entering the venue: "Please be advised that our venue has instituted increased security measures and extra vigilance that may cause you some delay. We apologize for any inconvenience you may experience. We can assure you that your safety is always our first concern and we thank you for your patience and cooperation."
●	●	●	●	D. Identify individual(s) authorized to speak on specific emergency preparedness issues.
●	●	●	●	E. Direct all media inquiries to a designated spokesperson.
	●	●	●	F. When given the opportunity, conduct interviews with the media regarding security issues to advise the general public to be cognizant of their surroundings and to let management know of anything unusual.
				G. In the event of a crisis, adhere to the following guidelines:
●	●	●	●	1. Notify all appropriate personnel immediately.
●	●	●	●	2. Convene immediate meeting of crisis coordination team and gather as much information as possible.
	●	●	●	3. Venue management should be available as or with the spokesperson.
●	●	●	●	4. Venue management, with the help of the crisis team, must formulate a statement as soon as possible that can be issued to the media quickly. A prompt response is of the utmost importance but factual information is first priority. [A quick media announcement can be that factual and up-to-date information will be available at (estimate time)]
●	●	●	●	5. In a crisis, it is better to have a media conference as opposed to just a written statement.

Risk Levels				Security Procedures
1	2	3	4	
●	●	●	●	6. At the media conference discuss the facts and do not speculate; let the media know if you don't have an answer; let the media know you are working with the appropriate agencies and will provide answers as soon as possible; keep answers conversational but brief; provide appropriate expressions of remorse and condolences if there are personal injuries and/or loss of life; reinforce positive actions; do not respond to statements allegedly made by third parties, unless it's a security or privacy issue then so state and; avoid saying to the media "no comment."
●	●	●	●	7. Coordinate efforts with organizer, promoter, artist, or team management. It is imperative that all speak as one voice.
●	●	●	●	8. First, formulate a plan of action, and following the initial media briefing, re-assemble the crisis team to update your plan.
●	●	●	●	9. Do not respond to inquiries regarding actions or decisions of other entities such as police, fire, rescue, and governmental concerns.
				15. Sweeps & Bomb Threats
	●	●	●	A. Work with local law enforcement agency to determine whether it is necessary to conduct a bomb sweep prior to an event; if so, lock-down the facility after the sweep.
		●	●	B. Use canine teams to sweep the venue on the day of the event.
		●	●	C. Building bomb sweep should be completed at least one hour prior to the doors opening, depending on the size of the facility and should be as empty as possible.
●	●	●	●	D. The venue should be equipped with "track and trace." Upon receipt of a bomb threat, the phone operator should immediately look at the caller ID display and note the time the call came in.
●	●	●	●	E. Switchboard personnel must have available at all times a copy of the "Bomb Threat Checklist and Reporting Procedure."
●	●	●	●	F. Ensure proper emergency communications procedure is in place in case of an incident.
				16. Miscellaneous
●	●	●	●	A. Determine who should receive copies of written security plans, keeping the list to a small group on a "need-to-know" basis.

Risk Levels				Security Procedures
1	2	3	4	
	●	●	●	B. Consider prohibiting “standing room only” as the situation warrants.
●	●	●	●	C. Compile a list of the telephone numbers and venue locations for the event promoters, producers, tour managers, convention organizers, and other key decision-makers.
		●	●	D. Require credentialed individuals to show photo identification along with the proper credentials to enter the venue.
●	●	●	●	E. Make a facility checklist for all areas of the venue, including mechanical rooms, generators, emergency broadcast systems, air in-take ducts, emergency vehicles, evacuation routes, stairwells, keys systems, etc.
●	●	●	●	F. Create a pre-event readiness checklist, event checklist and post event checklist.
		●	●	G. Work with the proper authorities to determine whether to restrict air space above the venue.
●	●	●	●	H. Work with local utilities personnel to ensure the integrity of power and telephone services.
●	●	●	●	I. Review emergency light and essential electrical power back-up systems to ensure that they are operational; secure transformers.
		●	●	J. Inspect vents and air-intake systems for hazardous materials and secure appropriately.
●	●	●	●	K. Secure stairwells leading to the catwalk for security purposes.
●	●	●	●	L. Establish an air contamination prevention and control program.
				17. Overnight Security (Non-Event)
	●	●	●	A. Venue should be locked during non-event hours. There should be at least two (2) entrances available for entry during normal business hours. The main door to the administrative area should be unlocked during office hours and locked once the offices close. Additional entrances should have a buzzer system or similar device (if not staffed) for patrons, delivery personnel, etc. to notify personnel inside facility that they are outside.
		●	●	B. An overnight guard should be considered (during the hours staff is not on duty) for grounds security year round and most importantly when there is a perceived or specific threat.

Risk Levels				Security Procedures
1	2	3	4	
●	●	●	●	C. Security should wear clothing that designates them as associated with the building.
			●	D. Local law enforcement agencies should patrol the area as arranged with facility management.
		●	●	E. A well-trained security person should be on duty after hours. This person is charged with checking the facility by making periodic walk-throughs, manning a security camera, maintaining logs of all activities, etc.
				18. Event Security
●	●	●	●	A. Establish safe staffing levels (depending on the type of event) with the promoters of various events based on information communicated between all parties.
●	●	●	●	B. Influencing factors should include size of event, type of event, past history, demographics of guests, and availability of alcohol, etc.
		●	●	C. Increase the utilization and visibility of uniformed law enforcement in parking lots and inside the facility.
		●	●	D. Increase the utilization of undercover law enforcement personnel in parking lots and inside the venue.
●	●	●	●	E. The name of the on-site uniformed law enforcement command officer should be provided to venue management.
				19. Liability Issues
●	●	●	●	A. Venue management, along with personnel, should be aware of legal issues that may arise. Being a public entity, consent to check inside packages, purses, bags, etc. may be required prior to the search being made.
●	●	●	●	B. No bottles, cans, etc. (items that could be used as projectiles) should be allowed inside.
				20. Technology
		●	●	A. An updated security system should be in operation at all times. The back of the building should be monitored 24 hours a day, 7 days a week, 365 days per year.
		●	●	B. A log of persons entering the building kept on a daily basis.
		●	●	C. Security cameras should be stationed inside and outside the venue.

Risk Levels				Security Procedures
1	2	3	4	
		●	●	D. Alarms should be placed on all doors, if possible.
●	●	●	●	E. Venue should be connected to a local security company.
●	●	●	●	F. All safety and security systems including PA system override, fire/smoke alarms emergency generators and lighting systems should be checked at least once a month.

EXHIBIT I
IAAM Safety And Security Task Force

Membership:
Frank Poe – Chair, CEO, Birmingham Jefferson Convention Complex; Larry B. Perkins, CPP – Vice Chair, Assistant General Manager, Raleigh Entertainment & Sports Arena; Milton Ahlerich, Senior Director of Security, National Football League; Doug Arnot, Salt Lake Organizing Committee for Olympic Winter Games of 2002; Horace Balmer, Senior Vice President, Security, National Basketball Association; David Bevans, General Manager, San Jose McEnery Convention Center; Dennis Cunningham, Vice President, Security, National Hockey League; Gregory A. Davis, Director, The Cajundome; Mickey K. Farrell, Director of Facility Operations, Raymond James Stadium; Jay S. Green, CFE, General Manager, Phoenix Civic Plaza; Steven G. Hacker, CAE, President, Intl. Association for Exposition Management; Kevin M. Hallinan, Sr. Vice President, Security and Facility Management, Major League Baseball; Robert J. Hunter, CFE, Senior Vice President & General Manager, Air Canada Centre; Patrick Leahy, Vice President/Venue Operations, Clear Channel Entertainment; Richard A. Martin, Principal, HOK Sports Facilities Group; Cory Meredith, President/CEO, Staff Pro, Inc.; Donna Noonan, VP for Div. I Women's Basketball, NCAA; Thomas S. Paquette, ComCast/Spectacor; Joe Psuik, III, Convention Center Director, San Diego Convention Center; Dan N. Saunders, Jr., CFE, Managing Partner, Global Image Concepts; Cliff N. Wallace, CFE, Managing Director, Hong Kong Convention & Exhibition Centre; Robyn L. Williams, CFE, Director, Portland Center for the Performing Arts; Turner D. Madden, Esq., Legislative Counsel, IAAM; and Dexter King, CFE, Executive Director, IAAM.

Mission:
The IAAM Safety and Security Task Force is to review current industry crisis management practices. Specific emphasis will be given to guest, tenant and physical asset security/safety/terrorism and other appropriate aspects of public assembly facility emergency management. Upon completion of the data collected, the IAAM Safety and Security Task Force will prepare "best practices" recommendations that can be incorporated in all aspects of IAAM professional development, educational, and public information programs.

Charge:
- Identify and prioritize potential issues of security and safety to include data collection.
- Collect and compile data, policies, and procedures specific to crisis management plans, protocols, and other activities currently in use by IAAM members.
- Develop and publish through IAAM material reflecting "best practices" in the area of security/safety/terrorism and crisis management for submission to the IAAM Board of Directors by July 2002.
- Generate "white papers" on procedures relative to security and safety topics to be distributed to IAAM members and the general public through print and electronic distribution. Collect safety tips and write pertinent articles and news stories for the IAAM Newsletter, IAAM Facility Manager magazine, or other related publications.
- Review and recommend benchmarks and guidelines to help venue managers in revising and updating security and crisis management plans.
- Serve with the ICMC as a resource to assist other program elements such as ICMC, ICCC, PAFC, district meetings, Oglebay School, Senior Executive Symposium, Stadium Managers, UVMC/Annual Conference, and AMC in recommending program topics, panelists, and speakers on the subject. Also

serve as a resource to the Body of Knowledge Task Force, Professional Development Committee and Ad Hoc Associate Committee.

- Work in concert with the Research Task Force to identify potential research projects to benefit our members and the industry, as well as possible funding sources.
- Identify, develop and build partnerships with other like-minded organizations and/or agencies, including law enforcement, public safety, and industry partners (IAEM, PCMA, ASAE, ASIS, IAPCO, professional sports, etc.) that will improve communication, programming, professional development, training, and the general body of knowledge related to crisis management for public assembly facilities.
- Coordinate its activities through the International Task Force to secure data in support of development of "best practices" procedures and "white papers." Identify potential programming material, training aids and online information exchange that could be utilized by and through member organizations of World Council for Venue Management (WCVM). Develop a long-term program for information exchange/networking regarding matters of crowd management/security/safety for public assembly facilities, and in support of IAAM responsibilities as WCVM Secretariat.

EXHIBIT II

the White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
March 12, 2002

Gov. Ridge Announces Homeland Security Advisory System

The Homeland Security Advisory System will provide a comprehensive and effective means to disseminate information regarding the risk of terrorist attacks to Federal, State, and local authorities and to the American people.

As part of a series of initiatives to improve coordination and communication among all levels of government and the American public in the fight against terrorism, President Bush signed Homeland Security Presidential Directive 3, creating the Homeland Security Advisory System (HSAS). The advisory system will be the foundation for building a comprehensive and effective communications structure for the dissemination of information regarding the risk of terrorist attacks to all levels of government and the American people.

The Attorney General will be responsible for developing, implementing and managing the system. In conjunction with the development of this new system, the Attorney General will open a 45-day comment period in order to seek the views of officials at all levels of government, law enforcement and the American public. Ninety days after the conclusion of the comment period, the Attorney General in coordination with the Director of the Office of Homeland Security -- will present a final Homeland Security Advisory System to the President for approval. The Homeland Security Advisory System will provide the following:

National framework for Federal, State, and local governments, private industry and the public. There are many federal alert systems in our country -- each tailored and unique to different sectors of our society: transportation , defense, agriculture, and weather, for example. These alert systems fill vital and specific requirements for a variety of situations in both the commercial and government sectors. The Homeland Security Advisory System will provide a national framework for these systems, allowing government officials and citizens to communicate the nature and degree of terrorist threats. This advisory system characterizes appropriate levels of vigilance, preparedness and readiness in a series of graduated Threat Conditions. The Protective Measures that correspond to each Threat Condition will help the government and citizens decide what action they take to help counter and respond to terrorist activity. Based on the threat level, Federal agencies will implement appropriate Protective Measures. States and localities will be encouraged to adopt compatible systems.

Factors for assignment of Threat Conditions. The Homeland Security Advisory System will provide a framework for the Attorney General, in consultation with the Director of the Office of Homeland Security, to assign Threat Conditions, which can apply nationally, regionally, by sector or to a potential target. Cabinet Secretaries and other members of the Homeland Security Council will be consulted as appropriate. A variety of factors may be used to assess the threat. Among these:

- Is the threat credible?

- Is the threat corroborated?
- Is the threat specific and/or imminent?
- How grave is the threat?

Unified system for public announcements. Public announcements of threat advisories and alerts help deter terrorist activity, notify law enforcement and State and local government officials of threats, inform the public about government preparations, and provide them with the information necessary to respond to the threat. State and local officials will be informed in advance of national threat advisories when possible. The Attorney General will develop a system for conveying relevant information to Federal, State, and local officials, and the private sector expeditiously. Heightened Threat Conditions can be declared for the entire nation, or for a specific geographic area, functional or industrial sector. Changes in assigned Threat Conditions will be made when necessary.

A tool to combat terrorism. Threat Conditions characterize the risk of terrorist attack. Protective Measures are the steps that will be taken by government and the private sector to reduce vulnerabilities. The HSAS establishes five Threat Conditions with associated suggested Protective Measures:

Low Condition
Green

Low risk of terrorist attacks. The following Protective Measures may be applied:

- Refining and exercising prepla nned Protective Measures
- Ensuring personnel receive training on HSAS, departmental, or agency-specific Protective Measures; and
- Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

Guarded Condition
Blue

General risk of terrorist attack. In addition to the previously outlined Protective Measures, the following may be applied:

- Checking communications with designated emergency response or command locations;
- Reviewing and updating emergency response procedures; and
- Providing the public with necessary information.

Elevated Condition
Yellow

Significant risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Increasing surveillance of critical locations;
- Coordinating emergency plans with nearby jurisdictions;
- Assessing further refinement of Protective Measures within the context of the current threat information; and
- Implementing, as appropriate, contingency and emergency response plans.

High Condition
Orange

High risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Coordinating necessary security efforts with armed forces or law enforcement agencies;
- Taking additional precaution at public events;
- Preparing to work at an alternate site or with a dispersed workforce; and Restricting access to essential personnel only.

Severe Condition
Red

Severe risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

- Assigning emergency response personnel and pre-positioning specially trained teams; Monitoring, redirecting or constraining transportation systems;
- Closing public and government facilities; and
- Increasing or redirecting personnel to address critical emergency needs.

Written comments may be sent to: Director, Federal Bureau of Investigation, Homeland Security Advisory System, Room 7222, 935 Pennsylvania Avenue, N.W. Washington, D.C. 20535. Comments may also be submitted electronically to: HSAScomments@fbi.gov

---

Return to this article at:
http://www.whitehouse.gov/news/releases/2002/03/20020312-1.html

Exhibit III
Resource List

BOOKS

Avery, William. Emergency/Disaster Guidelines & Procedures for the Sport, Leisure & Entertainment Industry. Orlando, FL: Systems Safety Management, 1996.

Berlonghi, Alexander. *The Special Event Risk Management Manual.* Dana Point, CA: Alexander Berlonghi, 1990.

Bombs and Bomb Threats. New York: Marsh & McLennan, 1995.

Emergency Planning Guidebook: A Blueprint for Preparing Your Building's Response. Washington, DC: Building Owners and Managers Association International, 1994.

Emergency Procedures for Employees with Disabilities in Office Occupancies. Public No. FA154. Emmitsburg, MD: United States Fire Administration, 1995.

Exercise Design Course: Guide to Emergency Management Exercises. SM#170.2. Washington, D.C.: Federal Emergency Management Agency, June 1984.

Guide to Health, Safety and Welfare at Popular Concerts and Similar Events. UK Government Bookstore. ISBN 0113410727. Phone: 011 44071 873-9090.

Kaplan, Audrey, et al. *Emergency Preparedness in the Built Environment.* Houston: International Facility Management Association, 2001.

NFPA 101 Life Safety Code & Handbook. 2000 Edition. Quincy, MA: National Fire Protection Association, 1994.

NFPA 1600: Disaster Management. Quincy, MA: National Fire Protection Association, 1995.

Murray, Edward. *Considerations for Fire and Life Safety in Stadium/Arena Complexes.* Miramar, FL: Miramar Fire-Rescue Department, 1994.

Pauls, Jake. Movement of People: *Fire Protection Handbook.* Quincy, MA: National Fire Protection Association, 1986.

Physical Security Guidelines. Washington, DC: Federal Bureau of Investigation Bomb Data Center.

Schmidt, Donald L. *Emergency Response Planning: A Management Guide.* New York: Marsh & McLennan, 1994.

IAAM VIDEO TRAINING PROGRAMS

Managing the Crowd. 18 minute VHS video and Instructor's Guide and Resource Manual. Item #08-049

Emergency Planning at Public Assembly Facilities. 17 minute VHS video and Instructor's Guide and Resource Manual Item #08-044

*Safety Awareness at Public Assembly Facilities***.** 20-minute VHS video and Instructor's Guide and Resource Manual. Item #08-043.

INTERNET WORLD WIDE WEB RESOURCES

http://training.fema.gov/EMIWeb/crslist.htm
Includes free instruction and resources on *Special Events Contingency Planning for Public Safety Agencies*, IS-15

http://www.fema.gov/library/lib07.htm
An excellent publication that can be downloaded is *Emergency Management Guide For Business & Industry*

http://www.crowdsafe.com
A website dedicated to improving crowd safety at music events worldwide.

http://www.cdc.gov/niosh/emres01.html.
Emergency Response resources from the National Institute for Occupation Safety and Health.

http://recovery.ifma.wego.net/?p=1464
Links development by International Facility Management Association.

http://www.ifmaseattle.org/links.html
Extensive links development by Seattle chapter of International Facility Management Association.

http://www.iacvb.org/iacvb/resource_center/resource_content_view.asp?maction=LIST&mresource_id=16&mkey=
Resources and links on crisis management developed by International Association of Convention and Visitors Bureaus.

http://www.packing.org/states.jsp
Good site for researching security issues related to concealed weapons laws.

