THE ESSENTIAL GUIDE TO SAFETY AND SECURITY

Best Practices for Meeting and Event Planning 2018

Best Practices Guide by Meeting Professionals International

MEETINGS, CONFERENCES AND BUSINESS events are an integral part of American society, representing what is estimated to be a $100 billion per year industry. The development of best practices in safety and security for conference organizers and event management professionals addresses the current need to standardize practices and procedures in event and venue protection. *The Essential Guide to Safety and Security: Best Practices for Meeting and Event Planning* provides a comprehensive overview of important planning components, assessment tools and implementation strategies for safety and security planning and operations at meeting and event venues

owners/operators can review and enhance safety and security plans. *The Essential Guide to Safety and Security* is intended to assist event management teams (event, venue, lodging and transportation), in conjunction with public safety agencies, in developing, implementing and improving their safety and security plans and procedures.

Meeting Professionals International (MPI) recognizes the inherent need for providing effective safety and security for all manner of meetings and events. To promote a consistent methodology for security and safety planning, MPI established an annual Risk Management Conclave. The Conclave brings

together representatives from industry associations, meeting planning departments, event management groups, venue operations, lodging facilities, transportation, audiovisual, entertainment organizations and federal, state and local public safety agencies. These representatives address current safety and security issues, identify solutions and propose future best practices and implementation strategies.
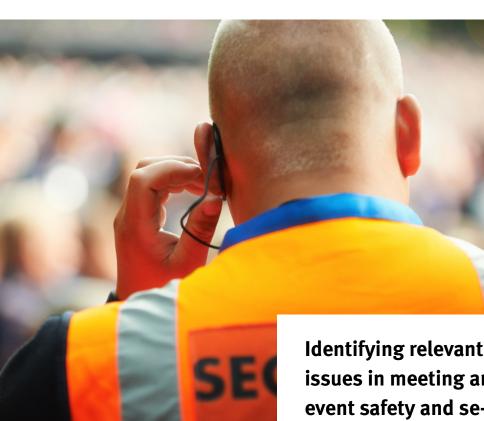
The discussions with security experts at the Conclave—along with personal interviews and a comprehensive review of literature, including existing security plans and operational procedures, government publications such as the SAFETY ACT, academic research reports and published articles—contributed to the formation of these best practices. Based on the literature review, interviews, Conclave discussions and expert vetting, MPI constructed a matrix of guidelines for meeting and event planners to utilize in addressing safety and security issues that potentially affect their business model. Leading experts in the meeting and event industry reviewed the proposed standards—or best practices—and provided feedback on the technical accuracy, relevancy and feasibility of each recommendation.

It should not be assumed that the application of these best practices encompasses all necessary protective measures for event safety and security. Rather, each event, venue and its management should determine appropriate safety and security measures based on their own unique characteristics and specific needs. The purpose of *The Essential Guide to Safety and Security* is to recommend polices, practices and technologies aimed at identifying vulnerabilities, mitigating risk and protecting critical assets. It can be used as a reference for those responsible for the design and development of safety and security plans and procedures.

This is the First Edition of *The Essential Guide to Safety and Security*. Each year, subsequent editions will be developed with input from practitioners, subject matter experts and current academic research.

The best practices in this document are broken up into seven topical areas. The areas covered include:

and lodging facilities.

Addressing the challenges of protecting people, property, information and infrastructure is of significant importance. The threat environment surrounding venues and events with mass gatherings of people is constantly evolving. As a result, security and safety plans should be considered living documents that respond to emerging challenges by integrating and leveraging new resources and information. Identifying relevant issues in meeting and event safety and security is a key component in establishing a standard of continuous improvement by which meeting and event planners, consultants and venue

Identifying relevant issues in meeting and event safety and security is a key component in establishing a standard of continuous improvement by which meeting and event planners, consultants and venue owners/operators can review and enhance safety and security plans.

1. Risk, Threat and Vulnerability Assessment
2. Event Safety and Security Planning
3. People Movement and Management
4. Emergency Action Planning and Crisis

Management

5. Business Continuity, Resilience and Recovery
6. Staff Management/Performance, Training, Coordination and Development
7. Technology/Information Management and Data Security

Following the *Best Practices Guide* are appendices that include a table of abbreviations and a list of individuals who contributed to the development of this document. A list of documents used in the production of this guide is also provided.

While not every best practice set forth will be applicable as written to every event, venue, lodging and transportation, it is applicable as a best practice. Therefore, it should represent achievable organizational goals within a scaled context of the implementation strategies set forth. These best practices are intended to cover the smallest to the largest events, from high risk/threat to low risk/threat, representing vastly different environments.

It is recognized that there is repetition among the topical areas and that is intentional so that comments/items are in context. Also, this guide, in keeping the information in context, is meant to apply to meeting and event organizers, venue managers, lodging facilities and transportation operators. So while a particular item may not be applicable to everyone, it is to one of the aforementioned, which may differ by event. It is a tool featuring industry best practices you can use to guide your assessments, planning, training and exercises.

PURPOSE

To document through professional collaboration the establishment of a living guide, a collection of vetted "best practices" to assist those responsible for safety and security for events of all types and sizes as well as their attendant entities.

DEFINITION

- A "best practice" is a technique or methodology that, through experience and research, has proven to reliably lead to a desired result.

- In practical analysis a "best" or "smart" practice is a clear and concrete behavior that solves a problem or achieves a goal under most conditions.
- A field-tested "best practice" is a program, activity or strategy that, when properly implemented, has been shown to work effectively and produce successful outcomes and is supported to some degree by subjective and objective data sources.

METHODOLOGY (ANNUALLY):

- Identify significant issues requiring solutions with input from steering committees and Conclave sessions.
- Discuss these issues in Conclave sessions to identify all aspects, lessons learned, voids and/or new issues.
- From sessions identify solutions and basis forming best practices.
- Review input, resolve details and collect additional information through literature reviews, research and contributions from subject matter experts.
- Send draft *Best Practices Guide* to Conclave attendees for vetting.
- Aggregate input from Conclave sessions, review, vet and follow up for best practices and formulation into *The Essential Guide to Safety and Security: Best Practices for Meeting and Event Planning*

HOW TO USE THIS GUIDE

Did you know that more than half of meeting and event organizers have no event-specific emergency plan in place? One reason for that is because up until now, no comprehensive set of safety and security best practices for meetings existed. This essential guide, with its nearly 400 reviewed and vetted recommendations of actions you can take, will be an important resource you can use to create emergency action, crisis response, and other safety and security plans for meetings and events.

You will not need every single best practice in this guide for each event, just as a painter never uses all the colors or brushers at her disposal for one single work of art. But,

having access to the depth of information and variety of options that this guide offers will allow you to pick and choose what you need to customize your plans.

Think of this guide as a box of paints. Imagine each topical area is a different color on your palette. Each best practice is a unique shade within that color family. The size of your meeting will determine how you apply that best practice to the canvas of your event.

Always begin your safety and security event management process by reading and following the best practices in the first Topical Area of this guide: Risk, Threat and Vulnerability Assessment.

After you've identified the unique risks, potential threats and vulnerabilities inherent to the event you're planning, the team you're working with, the participants you are gathering together and the event destination, then refer to the Table of Contents (TOC) to look up the specific elements relevant to your event so you know how to build and flesh out your plans, train your staff, and increase the safety and security of the event at hand. Click on the topic of interest to get to that section. When you're done, click on the link next to the page number to return to the TOC.

Predicting and preventing every possible risk is something no one can ever achieve because threats continue to evolve. The existence of *The Essential Guide to Safety and Security* or your ability to use it does not mean that nothing will ever go wrong at your event. But this tool will help you be better prepared to proactively minimize and mitigate the risks that you can, effectively handle the ones that you could not, and help you with your impromptu planning process as the unexpected occurs.

As new threats evolve, we hope you become part of the process of updating this living guide so that it remains the most relevant and essential resource for our industry. Let us know your suggestions for future guides and give us feedback on this one by emailing mpiacademy@mpiweb.org.

TABLE OF CONTENTS

TOPICAL AREA: RISK, THREAT AND VULNERABILITY ASSESSMENT

ASSESSMENTS			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY/ SCALABILITY**
1. A Risk/Threat/Vulnerability (RTV) assessment is one of the most important elements of a comprehensive safety and security plan/program. • Focused on the **venue, transportation, food** and **beverage, lodging** and **events**. • Comprehensive assessment of the risk environment, utilizing an all-hazards approach to identify vulnerabilities, adjust strategies and processes and develop contingency/mitigation plans to address risks and vulnerabilities. • Identify the hazards with the event's activities, locations of the activities and performance of those activities.	Pre-planning, anticipate and preparation. Must know and understand the safety and security risks, threats and vulnerabilities of the operating environment of the venue, transportation, lodging, event and attendees in order to address them through mitigation strategies or acceptance of risk. Without the assessment one cannot effectively develop and implement a security and safety plan. Failure to recognize and respond to risk to health, safety and security may be evidence of either negligence or incompetence in event planning.	Involve event Risk Management and/or security department(s) in this process, if one exists. Insurers may provide resources at no, or minimal cost. NCS4 offers a DHS/FEMA-funded Risk Assessment course. Keep all of your prior assessments.	This should occur regardless of the size of venue or type of event. Scalability is not necessarily a function of size or attendance. The same elements are present for both small and large events/facilities. Scaling comes into play during implementation/ mitigation/acceptance. If you have a static event site (one you use over and over) it will just be a matter of updating after your first assessment. However, if your event location changes for each event, it will be more time consuming. As you return, you will only need to review and update.
2. Create or utilize your risk assessment/crisis management/security team to conduct a Risk/ Threat/Vulnerability Assessment to determine and evaluate vulnerabilities, threats and areas of risk exposure.	A knowledgeable team to assess and address risks, threats, vulnerability, gaps.	Conduct an annual overall assessment as applicable and an event specific one before each event, evaluate and accept, mitigate or make changes as necessary.	Make sure you use qualified personnel to conduct the assessments.

3. Conduct a Risk/Threat Assessment for vulnerabilities for ALL events including a detailed criminal, terrorism, fire, structural, environmental, safety and medical assessment. Take an all-hazards approach. Review the list in the EAP and ensure they include (as applicable):

- Site(s) assessment and environment
- Demographics of attendees
- Number of attendees
- Resources assessment
- Environment/weather assessment
- Historical assessment
- Equipment assessment
- Lodging assessment
- Travel/transportation assessment

Risks and threats exist, but until identified and ranked for mitigation there is a potential for disaster.

In our context, Risk is the possibility of loss resulting from a threat/vulnerability, security or safety incident or event.

Security, safety and health Risk Management is a systematic and analytical process that considers the likelihood that a threat will endanger an asset, individual or function.

Risk =
Consequences x Probability

Break down assessments into three components:

- STATIC – these generally remain fixed with small variations over time, such as: venue, event, surrounding area, attendee type, etc.
- JOINT – this involves working with government organizations, community organizations, utility companies, transportation providers and surrounding neighbors
- DYNAMIC – this involves things that can change quickly, such as adverse weather, demonstrations,
- criminal acts or terrorist acts, etc.

Local DHS Protective Security Advisor (PSA) can assist.

Consider risks/threats as high or low RISK compared to high or low FREQUENCY - compared to high or low IMPACT. Eight common categories of risk to consider:
- Historical - what types of incidents have occurred in the community, at the venue, and other similar events in the area
- Geographic - what could happen as a result of the event's location
- Technological - what could result from a process, system, or equipment failure
- Human Error - what can be caused by a staff error; have they been trained; do they know what to do; and have they been tested on training objectives
- Physical - what can result from design/construction of the venue, utilities, tents, fencing, seating, rigging or staging
- Regulatory – what regulatory issues are there (i.e., laws, ordinances, OSHA, NFPA)
- Environmental – what can result from climate/weather issues (heat, cold, wind, ice, tornado, flooding)
- Business – what can result from bad practices, damage to brand, dissatisfaction of clients/attendees

4. Typical Risk Management cycle includes: • Identify the threats/vulnerabilities • Establish what are the vulnerabilities to address • Identify measures to mitigate, reduce or accept the risk/vulnerabilities • Develop response plans to address risks/threats not mitigated or accepted • Evaluate security/safety measures and exercise mitigation plans	Completeness.	Larger events will be more complex and some smaller events as well, depending on attendee type.	Applicable all size events.
5. Once risks/threats/vulnerabilities are identified and understood, develop a corrective or mitigation plan to address those considered unacceptable or of concern/needing attention. • Identify external resources needed for mitigation and/or response • Coordinate with local community partners and public safety agencies	Deal with risks, threats and vulnerabilities.	This will be part of the basis for the Emergency Action Plan (EAP). There are many governmental and private sector resources available to assist.	This will help you identify the level of scaling required based upon the assessment and need for mitigation or acceptance.
6. Conduct event management meetings prior to each event with sufficient lead time to address Risk Management issues and address mitigation where required.	Planning and preparation is a year-round function.	Events at different venues occur year round, so these meetings should occur for each event. As necessary, schedule weekly or at intervals appropriate for scale of events.	Based upon size, complexity, attendees and RTV assessment will determine depth and frequency of meetings.
7. For repeat events at the same venue, update and disseminate, as required, to key leaders and appropriate components/partners. The same is true for transportation modes used.	Currency and awareness.	Use the last assessment as a starting point to update and build upon.	Do not just assume the results of the last assessment.

ESTABLISH ASSESSMENT TEAM			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY/ SCALABILITY**
1. Establish a "Risk Assessment/Crisis Management Team," consisting of: • Facility/Event – key personnel (internal stakeholders, security, operations, facilities, technology/communications and equipment staff) AND any of the below as applicable based upon event size, components, threat, attendees, weather, geography • Lodging – security, operations, facilities, staff, technology/communications • Transportation – (bus/coach, subway, train, air) mode, operations, security, staff • Audiovisual/staging/rigging provider • Local/state/federal (as appropriate) law enforcement • Fire Department, Fire Marshal, EMS • Emergency Management • Utilities/public works • Include marketing, business affairs, exhibits, maintenance and general manager's office	Effective anticipation and predictability. Be all inclusive; have buy-in and input from subject matter experts. Team approach is essential. Preparedness. Reduces legal liability. Include components as required.	Most appropriate person to head this up is the Event Manager, or consider hiring a consulting team, but they will still need to meet with and interview all the components. If multiple jurisdictions, ensure that they are all included. Having an assessment is better than no assessment at all. Then continue to build upon it.	Smaller events and venues may not have all these resources but put a team together with available resources and personnel. Small events/meetings may mean that the event planner/manager serves this role. The first time will be time consuming, but after developing an outline (much of which is set forth in these best practices), it will go quicker.
2. This team should conduct the risk assessment and prepare a written report as necessary, at least annually, preferably before each event.	This is the beginning of a continuous journey.	The assessment at a minimum should be conducted at each new event/venue and updated at each revisit. All other plans will base their response on this report; it will be a guide as to what needs to be addressed in what order and expenditure.	Essential, regardless of any factors. This assessment once complete should be shared with key stakeholders.
3. As part of the risk assessment, create a team to review social media, monitoring for situational awareness and threatening information.	Monitor and assess threats.	Consider for team make-up: law enforcement, human resources and venue management personnel.	Important for large and risk-adverse events, but relevant for all.

CREATE CHECKLISTS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Create checklists to be used during assessments for the various components of the event/venue. • Review and refresh annually	For completeness and consistency.	These are important and worth the time and effort to prepare. Once complete, continue to use them over and over. They especially help new individuals conducting assessment for the first time. They also serve as an outline for planning.	Applicable to all size events.

CRITICAL ASSETS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Develop a comprehensive profile including detailed lists, staff/attendees and key locations of critical assets with detailed maps/blueprints of each level showing venue/lodging facilities, routes of ingress and egress, location of communication equipment, parking areas, transportation, traffic flow and areas surrounding the venue.	During a crisis it is too late to gather profile information and specific blueprints/diagrams to develop a plan for something that was not previously considered or evaluated.	Catalog and correlate plans to ensure that the Operations Center is notified of changes/modifications to this information, so all documents stay current. Key leaders/designees should have a working knowledge of their areas of responsibility in the assessment.	Applicable to all size events.

LIABILITY COVERAGE

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Event planners/organizers should obtain legal and insurance advice during and based upon the RTV assessment that include the following: • Liability for acts or omissions • Liability for injuries to staff or patrons • Liability toward financial costs associated with your response to incidents • Liability for the effects of an incident(s)	To reduce legal liability and obtain necessary insurance coverage.	In collaboration with insurance provider and legal counsel.	Applicable to all size events. Based upon your RTV assessment, legal counsel and insurance providers can provide you with advice concerning appropriate coverage.

THREAT RESPONSE PROTOCOL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Establish a Threat Response protocol for risks/threats/vulnerabilities identified that need to be addressed prior to the event and for all potential incidents for event day occurrences. Include these in Emergency Action Plan (EAP). • Develop decision trees for each incident type	Accountability. Determine and document what level of risk is acceptable and how to address unexpected issues. For accepted risks, describe why and how they are excepted.	**See Incident Response categories in EAP section.** Assign identified threats, risks and vulnerabilities to appropriate individuals to effectively address.	This affords preplanning that can avert disastrous outcomes for any events.
2. Consider if protective measures and emergency response can be accomplished using your existing resources or, if additional, enhanced resources and capabilities are needed. Identify who has the additional resources, how can they be acquired and pricing.	Adequate qualified staffing.	Resources for information are FBI special event office, local public safety agencies, venue security manager or county Emergency Management agency.	Applicable to all size events.

TOPICAL AREA: EVENT SAFETY AND SECURITY PLANNING

EVENT SAFETY AND SECURITY PLANNING			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY / SCALABILITY**

1. Develop an Event Safety and Security Plan to guide the operations of the event; to establish plans, procedures and guides for supervisors, event/venue staff, volunteers, etc.; and inform public safety partners. This should be based on a Risk/Threat/Vulnerability (RTV) Assessment. **SEE RTVA**.
 	
Should also have a separate Emergency Action Plan. **SEE EAP**.
	Preparation and organization.
	A plan to address reasonably foreseeable risks and threats.
	
	To protect the safety, security and health of your patrons and staff/contractors/volunteers.
	
	Assist staff in effective implementation.
	
	Essential to an effective event.
	
	Reduces legal liabilities.
		The plan should incorporate the following components based upon your Risk/Threat/Vulnerability Assessment as applicable to your type and size:
		• An overview of the RTV
		• assessment
		• Situational/operational awareness
		• Command and control
		  • Venue/event operations
		  • Public safety operations
		• Event management
		  • Disruptions (delay/suspension/change)
		  • Evacuation/shelter-in-place
		  • Cancelation
		• Staging, rigging
		• Audiovisual
		• Insurance coverage
		• Weather planning
		• Event staffing and assignments
		• Load in – load out
		• Intelligence
		  • Collection/sharing
		  • Fusion/analysis
		• Safety and security
		• Fire, EMS and public health
		  • Medical support
		  • Bomb threats/IEDs
		  • Hazardous materials
		• Access Control
		  • Ticketing/credentialing
		  • Pedestrian/vehicular
		  • Prohibited items
		  • Deliveries/waste removal
		• Robbery/theft/cyber protection
		• Investigations
		• Transportation and parking
		• Traffic management
		• Lodging
		• Behavioral issues
		• Public information plan
		• Signage
		• Pre-event agreements
		• Drones/unmanned aerial systems (UAS)
			The complexity of the plan will depend upon the size of the event, attendees and RTV assessment.
			
			The amount of time required for planning will vary depending upon the size, type, location, complexity, duration and RTV assessment. Smaller events a week or two, larger events several months.

POLICY ADMINISTRATION

1. Ensure that event policies are consistent with venue rules, policies as well as local/state jurisdiction laws and ordinances.	Provides guidance for staff on authority levels and the difference between enforcing policy and enforcing law.	Consult with legal counsel and local/state jurisdictions as well as the venue.	Smaller companies may not have access to in-house legal teams. But it will still be helpful to the event organizer to form a cross-departmental group to review the policies internally.

SITUATIONAL AND OPERATIONAL AWARENESS

1. Accessing and sharing information between various event, venue, agencies and organizations may be challenging, but is necessary for developing effective situational and operational awareness.	Effective information sharing through collaboration facilitates prevention and response. Must be "consumable" and "actionable" to be useful.	Set up an email or text group for the appropriate individuals to ensure cross information sharing. Utilize information-sharing software such as Dropbox, Google Drive or Sharefile. Also, set up various communication vehicles before, during and after event to share situational awareness information with staff and attendees.	This is essential for any event or venue regardless of size, but will scale according to event, threat, history and number of entities involved.
2. Train ALL staff and volunteers to be observant and report unusual/out of character or inappropriate activity to their supervisor/OC. Document all training. • Explain examples of unusual behavior and inappropriate behavior for all non-law enforcement personnel • Include traffic/parking personnel, ticket takers, ushers, screeners, food and beverage staff, maintenance staff, stage workers, custodial staff, etc., in this training • Broadcast (using all mediums) "See Something, Say Something" giving them a way and to whom and how they should report	Documented prevention efforts will serve you well should an incident occur and in any litigation. This is essential to engage all parties.	Consider presentations, live or on video, to staff, volunteers and even key attendees prior to and during the event. DHS public service announcement can assist with this. Offer different mediums to report information (i.e. phone, website, text, Twitter or an individual). Front line staff (ticket takers, screeners, parking and traffic personnel, contract security personnel, gate attendants, ushers, concession workers, riggers, venue staff, maintenance workers, etc.) are a great source of intelligence/situational information. Since most work multiple events, they notice what is out of the norm. This training/reinforcement can be conducted at the beginning of the event day.	This can and should be undertaken regardless of event size.

3. Use plainclothes officer(s) who are strategically placed throughout the venue/event to observe and report. • Surveillance and counter surveillance teams are appropriate in external locations as well as within a venue to observe and report • Use in conjunction with CCTV	These trained eyes and ears are used to complement CCTV if present. Better observation.	To the extent possible, try to use the same plainclothes officers for each or multiple events as they become familiar with what is out of ordinary for any event (same for officers monitoring CCTV). These officers may be (event or facility) paid off-duty or on-duty or security officers. Some of the best places are roofs or elevated platforms within the superstructure, as well as outside and walking the venue. If available, consider mounted units, bicycle patrols. Additional consideration should be given to stationary, elevated platforms in parking lots. They are great to observe from their elevated position and are also good for crowd control. To supplement lack of officers or even CCTV availability, consider inviting surrounding jurisdictions to provide officers and/or access to network and communication infrastructure to assist, as they may want to use the event to develop officers' skills (use as training). Consider the use of body cams to support and document all incidents.	This is for larger and/or high-profile events and when the threat level is elevated. This is something that is scalable based upon the size of the event intelligence and history. These factors will also determine the numbers to be deployed and associated costs.

COMMAND AND CONTROL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
PLANNING			
1. All parties from Public Safety (law enforcement, fire department, EMS, emergency management) to event and venue security and facilities management should be at the planning table so roles and responsibilities are pre-defined and appropriate command and control is exercised during the event. There should be clear lines distinguishing between the roles of Event Operations and their security vs. Public Safety. • Practice these roles during at least one table-top exercise for each major event With multi-jurisdictions, local resources are normally under the direction of their jurisdiction until an EAP incident occurs, then Incident Command System (ICS) is invoked. • Pre-define the authorities to act	This is important, because you want the most competent and experienced person in charge. Avoid confusion on event days through pre-planning, coordination, clear lines of responsibility and in the event of an incident by following NIMS/ICS protocols. For very large events to ensure that all entities have representation. It is too late to meet at the incident and it will take away critical time from the incident response by discussing how to develop a plan at the scene. Well-coordinated plans save lives and property. By name.	Ensure that all front-line security response and dispatch staffs are trained in ICS and NIMS. Both online and classroom courses are available. Agency/organization representatives in OC and designated incident commanders should have full authority to make timely decisions.	This should occur regardless of the size of the event and should include external resources that might respond to incidents. For smaller venues it means there will be fewer people. For medium sized events some resources maybe on standby, but pre-informed of their role, responsibility and details of the event. The core event team serves as command and control. For smaller events, public safety should be informed, and the core event team will serve command and control.

2. Produce an Organizational Chart and Command Matrix (and staffing plan) listing from top to bottom of who reports to whom consistent with event operations and NIMS/ICS, divided into:

Operations Management
- Administration
- Broadcast Teams
- Event Staff
- Door/Entry Screening
- Communications
- Marketing Promotions
- Traffic/Parking Staff
- Ticket/Registration Staff
- Transportation
- Lodging

Public Safety/Emergency Management
- Law Enforcement (Local, State, Federal)
- Medical/Public Health
- Fire Department
- Emergency Management
- Public Utilities Agency
- National Guard
- Department of Transportation
- Department of Public Works
- Traffic/DOT

Facilities Management
- Adjacent Structures
- Facilities
- Grounds
- Meeting Rooms
- Stage
- HVAC
- Maintenance
- Housekeeping
- IT
- Physical Plant
- Team Logistics
- Food Service
- Concessions/Merchandise

Role awareness and organization.

ICS and its introduction of an Incident Commander applies and is triggered when large/major or far-reaching incidents occur. Minor incidents of a routine EMS response, small fire, fight, etc., would not invoke the transfer to ICS away the Venue Manager/Event Director or on-sight public safety. Establishes role based response in the case of an incident rather than a rank-based organizational structure.

Use components and staffing applicable and appropriate for the event.

All components may not be required for all events.

For small venues/events some resources maybe on standby, but they should be informed of their role, responsibilities and details of the event.

This should be developed regardless of the size of the event. The ICS is designed to be completely scalable for management incidents. It can be applied to events of any size and complexity.

COMMUNICATION

1. Develop an Operations/ Communications Plan that includes options and alternative methods to communicate at all levels from Operations Center to front line staff and appropriate public safety at all levels.	Communications is one of the most important during an event, but it is sometimes not followed.	Interagency communication (law enforcement, fire department, EMS, venue, event, etc.) is essential during a crisis and should be a high priority. Communications can take many forms, from runners, landlines, cell phones, satellite phones, radio, email, texts, apps, video boards and public-address systems.	This is clearly scalable based upon the size of the event and complexity.
2. Test Communication Plan/equipment in a working environment to ensure the equipment and location is functional before each event. • Ensure backup power is available for communications equipment	Reliability of overall communication capability and in a high noise and potentially inclement environment.	Should be multi-agency test, where appropriate.	Applicable to all events regardless of size.
3. Establish redundant and alternative communications systems for operational or emergency communications. • Especially cellphones and pagers as they are the first to go out in a crisis	Technology dependency and reliability under stress.	Use all means and methods to communicate and test these.	A new capability exists, called Long Range Acoustic Hailing Device (LRAD) system for large out-door events.
4. Have megaphones available as a backup for crowd control/attendee notification. • Also use first responder equipment for emergency communications (i.e. law enforcement vehicle loud speakers) • Also use house amplification and video capabilities with pre-recorded emergency messaging.	Be prepared in case normal communications fail.	Test in a crowd environment to see if the messages can be heard/seen, understood, and acted upon. New megaphones offer the capability of pre-recorded messages for various incident types to communicate with patrons. Consider, at a minimum, one for each entry point.	Message boards maybe another option depending on the event/venue.

CONTRACTS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Security requirements (standards, best practices) should be included in the Request for Proposal (RFP) for the meeting/event.	Put potential facility on notice of your security/safety requirements.	RFP should include a process for connecting with local public safety agencies and officials during site visits and planning meetings. Language seeking safety and security information at the RFP stage must be broad and focused on key security and safety elements. Understand that venue cannot share security plan such that this as it makes them less secure; they may not provide specifics at this stage. Include explicit event weapons policy.	This is important regardless of event size. Venues and vendors should be made aware of expectations of the event and should communicate those expectations to their teams.
2. Information sharing regarding risk and capabilities is a two-way responsibility between event planner, venue and public safety	Establishing proper communications and protocol helps to reduce surprises onsite.	Inform venue and safety officials of known issues or possible problems regarding event (i.e. threats, protests, controversial issue or topic, disgruntled individual, special needs, VIP/protection details).	Applicable to all size events.

EVENT STAFFING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Provide appropriate trained staffing levels for all events based upon anticipated attendance numbers, the type of event, history, intelligence and recognized risks/threats. • Using a ratio of 1 trained crowd manager for every 250 attendees/participants is recommended for event staff, as suggested by the National Fire Protection Association (NFPA)	Sufficient trained coverage for a safe and secure functioning of the event.	A major factor in "appropriate" staffing levels will be based upon event type and history, intelligence, weather, alcohol sales/use and risk factors unique to the event. For some venues/events, staffing may be volunteers, so ensure that they understand their roles and responsibilities.	Consider geographical and environmental issues.

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
2. Maintain consistent staffing levels throughout the event. Do not release employees solely for cost savings. Must have sufficient staff to manage shelter/evacuation any time during event.	Sufficient coverage for emergencies to address incidents that may occur.	Crisis and emergencies are unpredictable. Staffing levels should be sufficient to respond to incidents that can be realistically managed without external resources consistent with event risk/threat/vulnerability assessment. Be creative by redeploying event staff to meet operational needs. This includes both event and venue staff as applicable.	Local convention and visitors or tourism bureaus might be able to help event organizers secure additional volunteer or paid staff. Universities and colleges are another source of volunteer labor, if needed.

INTELLIGENCE COLLECTION/ANALYSIS/FUSION/SHARING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Establish a plan for handling the collection, maintenance, sharing, and protection of information. • Establish a program for staff situational awareness and bi-directional information sharing • Implement a system to log and track incident response and resolution	Intelligence is essential for planning, anticipating, implementing venue, lodging and transportation plans, and maintaining situational awareness this includes information that may threaten the event (crime, terrorism, weather, other community activities, etc.).	Information should be handled on a need to know basis. Fusion Centers have a good model for handling, collecting, analyzing, sharing, etc. Conduct pre-event surveys of past events (from all sources possible) for upcoming events. Request information such as attendance, number of security and law enforcement used, total number of incidents including arrests and medical issues, event demographics and crowd dynamics.	Applicable to all size events.
2. The primary law enforcement agency responsible for the event is the best choice for handling and/or protecting intelligence material.	Safeguard information.	The FBI Joint Terrorism Task Force (JTTF) and Field Intelligence Group (FIG) are also good sources of broader intelligence. All sources (local, state law enforcement and Fusion Centers) are important and can provide useful information.	When meeting overseas, familiarize yourself with local law enforcement agencies.

LOCAL CRIMINAL ASSESSMENT/CRIME SURVEY

1. The law enforcement agency that is responsible for the venue should collect, maintain and disseminate this information as required for events.	Intelligence information is critical to assessment, planning and implementation/response.	This intelligence, in conjunction with the results of risk/threat/vulnerability assessments, will allow for effective planning regardless of the venue/event size.	Much of this information is often available online in many cities. The event organizer/venue operator needs this information to make effective decisions for planning.

PUBLIC/PRIVATE COLLABORATION

1. Establish a working relationship with the local FBI JTTF and state or regional Fusion Centers.	Enhances information sharing.	Partnerships are force multipliers.	Applicable for all size venues/events.
2. Join local information sharing groups like InfraGard (public-private collaboration), Neighborhood Watches and community policing units in the event. • Consult with corporate security departments from high profile companies that attend these events or are in the vicinity	All avenues of information. Are they targets of threats or actions?	**www.infragard.org** Local law enforcement neighborhood policing units are great sources, as well as DHS/PSA.	If in doubt, ask local venues, vendors and tourism agencies about the existence of networks relevant to the event's destination.
3. Enhance information sharing on high profile/high- risk constituents.	Attendees at events may include high profile business leaders, politicians, celebrities, professional athletes or other individuals. Potential risks to event range from individual safety threats and crowd management issues to protests.	Proactively seek out information from all sources.	This is important regardless of event size.

TERRORISM ASSESSMENT

1. Assign a liaison with local FBI JTTF and state or regional Fusion Center since it is the best way to be alerted to any intelligence of potential terrorist activity/threat to the venue/event.	Stay aware and be proactive.	For high-profile events, consider having a member of staff get a security clearance through DHS or FBI JTTF, so they may receive classified information for planning and response.	In the United States, contact the FBI and state or regional Fusion Center(s) to inform them of your security sensitive event and see if they are aware of any potential issues. If meeting outside the U.S., the same procedure should be followed with the relevant foreign agency.

SAFETY AND SECURITY

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
PERIMETER CONTROL/PROTECTION			
1. Conduct area Crime Analysis to objectively determine what problems exist on event days and non-event days in the vicinity of your event/venue.	To assess and prepare for any potential criminal activity. To properly establish venue precautions and communicate with attendees regarding personal safety before, during and after the event. Aim to answer questions like: Is the area more/less conducive to crime than average? What types of crimes occur in the area during and independent of venue-related activities?	Law enforcement can provide a crime analysis and gather input from their local counterparts. Local law enforcement agency responsible for the venue would be the appropriate agency for this information. Today this information is available online for most cities/counties at least in the U.S.	Applicable regardless of size.
2. Continually maintain relevant records for reference and analysis over time. • Public facilities may retain this info as they have terms and timeframes that they must follow for records maintenance/retention	For assessment, planning and legal liability.	Implementation of a standardized operations/incident log can create a common accessible framework for staff reporting and record-keeping.	Procedure is independent of size.
3. Encourage or develop close coordination between venue, lodging, transportation and local law enforcement. • Staff the outer perimeter entry/control points with event security	To ensure access control and security of participants and spectators. To establish collaboration and communication framework and protocol for when law enforcement is primary entity and when event/venue security is primary entity.	Coordination is essential to effective security and safety, with clear roles and responsibilities. Do not expect law enforcement to provide event/venue security responsibilities - if threats require their presence it serves as a deterrent and to address order issues, so uniformed law enforcement, would work along with venue security staff.	Coordination with local law enforcement regarding an event can preemptively drive a greater public safety presence and enforcement campaign outside of an event area.

4. Venues should consider fixed or mobile barriers deployed between the venue and all major adjacent roadways immediately surrounding the venue to slow the approach of traffic and provide a managed point of vehicle ingress on event days and/or consider closing them.	Creates a buffer zone between the venue and general traffic. Barriers protect pedestrians and bystanders alongside these roads. By using these barriers, vehicle access points are limited, which makes vehicle verification less stressful. Also serves as an impediment to Vehicle Borne Improvised Explosive Devices (VBIEDs), and vehicles used as an attack weapon.	If roads are just closed with plastic/wood barricades, they should be manned by law enforcement. In areas where traffic cannot be significantly slowed on its approach, and if justified by the risk assessment, the deployment of more substantial barricades to reduce the vulnerability to forced vehicle entry (intentional or accidental). Reinforce areas that are vulnerable to forced vehicle entry with substantial barricades (i.e. bollards, retractable wedges, anti-ram fences, large trucks or buses, Jersey barriers, reinforced concrete decorative planters, etc.).	This will be driven by your Risk Assessment. Participate population will also be a factor. Minus any threats, this is not necessary for smaller events.
5. When possible, arrange to have marked law enforcement vehicles parked randomly outside critical facility assets.	Serves as a deterrent, even if unmanned.	They have to be parked somewhere when not on patrol.	Based on threat level and critical assets. May not be necessary for all events.
6. Ideally each venue should have Concentric Circles of Security (CCS), with generally Inner, Middle and Outer perimeters. • The **INNER** circle would typically encompass everything from the venue exterior wall/fence inward • The Green/Dressing Rooms, Stage, Meeting Rooms, Conference and/ or Exhibit Hall within the INNER is considered a separate High-Security Area • The **MIDDLE** circle would typically encompass everything from the exterior wall/fence outward to at least 100ft (if possible) • The **OUTER** circle would typically encompass everything from 100 foot line to the property line or other arbitrary border a minimum of 500 feet should be established where possible	To protect VIPs, talent and mass gathering areas. Each circle will have different security requirements/ controls and staff trained to avoid confusion. Generally, this information should be made available to attendees to avoid confusion as to access. Each circle/level allows for containment of a situation.	When implementing CCS, the type of venue as well as geography, environment, number of patrons, type of event and surroundings will dictate the number of circles, line drawing and distance for each segment. The inner perimeter may be a room, or a hall or the interior of an entire venue; it depends upon the criteria above. In instances where there is not 100 feet of clearance, vulnerable areas and possible threats must be identified and alternative arrangements made to secure the venue's perimeter through methods such as utilization of barriers, vehicle and pedestrian routes, and placement of law enforcement/ security guards and other event parking/traffic staff.	The Risk Assessment, the size, impact, and history of the event, the number of attendees and history of prior events will drive the size and complexity of the security plan and defined CCSs. Inner Perimeter = Exterior-of-house Middle Perimeter = Front-of-house Outer Perimeter = Back-of-house Access and credentialing will likely vary between each area.

7. Place a renewed emphasis on middle and outer perimeters.	Recent world terrorist events indicate that as the inner perimeter becomes hardened violent extremists target individuals in the outer perimeters.	Implement protective measures for soft target areas surrounding venue.	This is applicable to all size events.
8. Maintain emergency ingress/egress routes for first responders and public safety vehicles.	Ensure rapid, unrestricted response both inside and out.	Pre-designate these routes with public safety so they are aware.	This is applicable to all size events.

PRE-EVENT INSPECTION

1. Conduct a venue inspection each time before the venue doors open for your event to remove all unauthorized materials, vehicles and people to create secure MIDDLE and INNER perimeters. Results of the inspection should be reported to the venue's security department or Operations Center prior to opening. The results of each pre-event inspection should be maintained as documentation that the inspection was conducted, and the area was controlled at a point in time prior to patron entry.	Prevent unauthorized materials, vehicles and people from disrupting the event to the greatest extent possible.	Conducting the inspection will be driven by event type, history, size, intelligence, threat and risk factors unique to the event, especially if there are known threats or knowledge of similar (recent) activities. Should something be subsequently found, a timeframe can be established to predict approximate placement time.	This will require close co-ordination with the venue managers. Event manager and venue manager should conduct this jointly. At a minimum, staff should walk the entire facility for events (for 1,000+ attendees or smaller high-profile events, you should consider using bomb dogs and/or metal detection).
2. Know the neighborhood located within 100 feet of the venue prior to the event and evaluate potential threats, to the greatest extent possible.	This is to prevent potential assailants from using nearby buildings/objects for an attack.	This may not be possible at all venues, but an inspection should certainly be conducted if threat level is elevated for any reason. At minimum, consider whether they present a potential threat. Particularly, buildings that look down upon your outdoor events.	This will be driven by threat intelligence and serves as a deterrent.

ACCESS CONTROL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
CREDENTIALING			
1. Secure the INNER perimeter so that no one without a ticket, pass or credential is permitted entry through venue/event doors, gates or entrances.	To maintain control over the area of your event protect people and property. To ensure only those authorized are granted entry and to protect materials/merchandise in exhibit halls.	Wristbands have been found to work well for temporary staff. Use different colors for different days/events.	Applicable to all size events.
PEDESTRIAN (ATTENDEES, SPONSORS, STAFF/WORKERS, TEAM MEMBERS, MEDIA OFFICIALS)			
1. All open access points should be staffed. Only authorized individuals permitted to enter the venue/event. • Make sure participants are who they say they are by requiring a photo ID during check-in	Without effective access control there is no control.		This should be standard operating procedure regardless of venue/event size, however, access may be reduced for ingress/egress within fire codes based upon event size and attendance.
2. Event day staff (paid, sub-contracted, and volunteers) should use a designated entrance(s) to check-in and receive their credential and post orders after providing a valid photo ID. Then have a checkout process and recap of the day with their supervisor.	Controls entry and authentication of event staff, separating them from attendees. Reduces confusion.	For large venues/events with large staff, use more than one designated entry point organized by role.	Applicable to all size events.
3. Prior to event, have media/press provide a list of all personnel requiring access into the event venue. Upon entering, media personnel should identify themselves with photo ID so that they may be issued a credential. All broadcast bags should be checked, inspected and tagged.	Reduces risk of unauthorized persons gaining entry and prevents unwanted material/items from being brought in the adversary will know if these individuals come and go without any checks.	Tagging of bags/containers allows for staff to verify that it has been properly inspected. Loose or inadequate checks and controls create opportunities to introduce threats and/or hazards.	This should be conducted with no exceptions, despite inevitable complaints, regardless of venue/event size.

4. Secure specific areas to prevent post-event access. Such areas include: • Conference/exhibit halls • Concessions stands, kitchens, and storage rooms • Equipment rooms • Green, dressing, locker rooms • Class/meeting rooms • Staff offices • Suite level(s) • Electrical/mechanical rooms To reduce theft and damage while shutting down the venue, a checklist should be used.	The event is not over until at least 30 minutes after all attendees/ presenters/ entertainers are off the podium/stage. Safety and security requirements for the venue may remain in place for several hours after all spectators have departed which incorporates teardown.	Ensure workers/volunteers understand that the event is not over when the last buzzer sounds, but when event operations say it is. Instill diligence throughout the entire event. Often more issues arise on egress, than on ingress.	Applicable to all size events.
5. Post signs near all entrances clearly identifying prohibited items. Dependent upon state law, ban firearms or weapons from being allowed in the event/venue (include a list of all prohibited items). Include signs at "Park and Ride" to event/venue locations, event shuttle pickup points and other mass transportation locations. • Educate mass transit/ tram/bus drivers (and an assistant) to be on the lookout for prohibited items so patrons have an opportunity to return items to their hotel/vehicle before getting on bus/train • Prohibited items should also be conveyed and enforced with all vendors, staff and contractors	Avoids confusion concerning what is and is not permitted. Avoids attendees from showing up at venue entrances with prohibited items causing them to discard their prohibited items or making them take the items back to their vehicle. Also, avoids issue at entry to venue. Improves the guest experience.	State firearms laws will impact the implementation of venue policies regarding possession, especially on public property. Determine how to deal with off-duty law enforcement officers attending as they may be in possession of a firearm at events. Also use public address systems and video/digital boards should be utilized to communicate to the attendees the protective measures, procedures, restrictions, prohibited items and evacuation routes as they enter the event/venue.	This is applicable to any size venue but would be scaled to the size of the event to prevent backlogs. For smaller venues with no adverse intelligence, random screening may be appropriate.
6. Include signage that advises attendees that, "at the event or venue's discretion, if an individual appears to be intoxicated they will be denied entry."	Provides legal notification/ warning for denied entry.	Staff need to understand how to identify and handle intoxicated parties, and what it means to enforce this notice.	This is applicable to all size events.

VEHICULAR

1. Allow only authorized or credentialed vehicles to be parked within the MIDDLE or INNER perimeters, and then only after they have been screened prior to entry. Check and inspect all broadcast/media vehicles and insure they are properly credentialed.	Vehicular traffic is a pedestrian risk and can also be used as a weapon (i.e., VBIED or ramming). This area is very vulnerable and should be monitored and secured where appropriate.	Authorized vehicles may include law enforcement/emergency vehicles, sponsor vehicles, broadcast equipment trucks and vehicles driven by event/venue employees, staff and officials. ALL vehicles should be checked and credentialed. Particular attention must be paid to the presence of unsolicited emergency vehicles such as ambulances. Make this part of the pre-event planning so marketing can notify sponsors/vendors of changes well in advance of the beginning of the event for load-in/load-out.	This is particularly applicable to large events with an elevated threat profile. This is normally under the control of the venue; therefore, close coordination is required. As an event organizer you want to make clear who is assuming risk for decisions involving vehicular traffic and parking. (May or may not be under the control of the venue, could be the city/county or private entity). Several venues are using License Plate Readers (LPR) that are synced with local law enforcement databases. This helps in identifying banned persons and wanted/stolen vehicles. This is particularly good for large risk averse events.
2. Inspect and credential (label/tag) ALL (including public safety) vehicles allowed inside the MIDDLE or INNER security perimeters. • Broadcast vehicles (at large events) should be located in a designated and secure compound(s) with its own perimeter. A security officer should be deployed at all times at the broadcast/media compound while media is present. Entry to the media area should be controlled and all media should be credentialed. • Roads should be blocked off when necessary and special event-day traffic procedures should be instituted to allow for vehicle ingress/egress	Credentialing/labeling avoids the confusion of whether a vehicle has been inspected upon entry and can also denote which vehicles are permitted where. Assists in preventing VBIEDs. To avoid use of "cloned" or stolen public safety vehicles.	This should be a relatively small number of vehicles. Colored stickers (changed for each event) could be used.	Not necessary for small events or those with no reasonable threat. Not applicable to all events or meetings as many may have no vehicular to the inner and/or middle perimeters. Also, may have not broadcast/production vehicles.

3. For INNER perimeter entry and for venue facilities that offer UNDER VENUE - UNDERGROUND PARKING, vehicle checks should be conducted by trained staff using, at a minimum, visual inspection (inside and out) using undercarriage mirrors for VBIED's prior to each vehicle entering the inner perimeter/underground parking.	Larger vehicles present a greater risk based upon their size, capacity and volume of fuel tanks.	This can be time consuming, so consider using explosive detection canines to expedite the process and use mirrors to augment in case of an alert. Remember working time limitations for bomb dogs.	The RTV assessment, participants, the size, impact, history of the event, number of attendees, etc. will drive the level of vehicle screening. This is applicable to any size venue but would be scaled to the size of the event to prevent backlogs. For smaller venues with no adverse intelligence, random screening may be appropriate.
4. If the venue has parking inside the venue, each vehicle should be searched, and its occupants screened. The use of trained explosive detection canines is suggested under these circumstances, in addition to truck searches and the use of undercarriage mirrors. The sale of non-event daily parking permits should be prohibited in such areas.	Larger vehicles present a greater risk based upon their size, capacity and volume of fuel tanks.	This should be strictly adhered to and enforced due to the magnitude of damage/impact of a VBIED. This can be time consuming, so consider using explosive detection canines to expedite the process and use mirrors to augment in case of an alert. Remember working time limitations for bomb dogs.	Some may want to do this only if specific intelligence indicates a threat. However, there will not always be forewarning, and while it may be low incident it is high impact. So, if you don't screen, you must be willing to accept the risk. Some jurisdictional fire codes prevent vehicles from parking in or close to the venue due to possible fire/explosion of fuel tanks.
5. For venues with parking immediately adjacent to the venue (usually middle perimeter) ensure all vehicles within 100 feet of venue wall are searched both inside and out (use bomb dogs, if possible).	Larger vehicles present a greater risk based upon their size, capacity and volume of fuel tanks.	Consider these high-risk areas. Reserved parking should not be transferable. Remember working time limitations for bomb dogs.	The RTV assessment, clientele, the size, impact, history of the event, number of attendees, etc. will drive the level of vehicle screening.

6. All trucks and delivery vehicles seeking access to the INNER, MIDDLE or underground parking or unloading areas should be inspected visually and with undercarriage mirrors for hazardous materials, weapons and explosives. Depending on the configuration of the venue and the risks, the contents of the vehicle should be inspected by the security staff (visually or bomb sniffing dogs) prior to permitting any truck or delivery vehicle entry to the ramp leading to the service level or any area below the event/venue.	Protection efforts to prevent the introduction of hazardous/prohibited/ explosive items to the venue.	Ideally, all such deliveries except perishables (i.e. ice, fresh baked goods, flowers, etc.) should be delivered at least 24 hours prior to the venue opening, to avoid tying up venue day resources. If possible, consider restricting deliveries to certain times on the day of the event (i.e. two hours prior).	This is particularly important for large events, 5,000+ attendees and/or high-profile VIPs or those events with a high risk profile.
7. All sponsorship displays or concession vehicles within the venue's INNER or MIDDLE perimeters, must comply with local fire codes and, at a minimum, comply with the following: • Inoperable gas cap • Disconnected battery • Minimal fuel in tank • Possession of keys to the vehicle by a designated security or facility team representative • Unattended sponsor vehicles should not impede egress	Protection efforts to prevent the introduction of hazardous/ prohibited/ explosive items into the venue.	All vendors should be made aware of these requirements.	Applicable to all size events.
8. Monitor parking lots to ensure they are accessible for EMS and fire vehicles. Ensure parking aisles are not blocked.	Ensure emergency vehicle access.		This should occur regardless of event size or type.
9. For lots adjacent to the venue event area, remove all unauthorized or unidentified vehicles as part of the inspection process prior to opening of the event. • Conduct at least a cursory screening of all vehicles entering a controlled parking lot • Parking lots should be inspected daily (for multi-day events), and unattended/ unaccounted for vehicles not removed within a reasonable amount of time should be investigated and removed as soon as possible	Unattended vehicles can pose a problem. Individuals who are intent on doing harm will notice if vehicles are left in lots without a response.	Parking lots should be cleared and closed prior to an event for safety and security purposes. This allows you to start with a controlled environment. This is a best practice, but vehicle removal may not be possible at adjacent properties not under facility control. Parking lots that support other activities should be closely monitored.	This may not always be possible depending upon the multi-functions of the venue and the RTV assessment. For larger events or those with security concerns.

10. Prohibit vehicular use inside the INNER Perimeter of the facility during the event.	It is a different dynamic when the venue is loaded.		

DELIVERIES AND WASTE REMOVAL

1. All deliveries (entries and exits) should be prescheduled and documented. Entry should be centralized to a single point, so they can be checked against the list of scheduled deliveries. • Deliveries should be limited at event time, whenever possible • Deliveries should be scheduled through a single entrance, where possible • Delivery of hazardous materials (such as propane) should be scheduled during times of low-occupancy (i.e. overnight or early in the morning) For High-Risk Events: • Advanced scheduling should be completed with company, the driver's license of the driver and helper, and the contents listed on the manifest • All delivery vehicle drivers and helpers must produce government-issued photo identification and must sign in at a control point. The previously submitted driver's license must match that of the person making the delivery, and the previously submitted manifest must be reconciled with the contents of the vehicle at the time of delivery. • Keep a record of each vehicle, driver and helper(s) entering or leaving the venue by use of a log or permit system. Records should be retained through the end of each season/calendar year.	Limit possible accessibility of VBIEDs or chemical agents and the possibility of a vehicle used as a weapon. Propane delivery trucks making refill deliveries pose a significant risk.	Particular attention should be given to armored truck deliveries (i.e. ATM service, food service delivery trucks, etc.). Consider taking a picture with a smartphone camera of the driver and their driver's license.	This is normally under the control of the venue; therefore, close coordination is required. As an event organizer you want to make clear who is assuming risk for decisions involving deliveries. Many venues are multi-purpose/multi-event; therefore, much coordination is required based upon your event RTV Assessment and any other overlapping events.

2. All waste removal should be scheduled, but not during the event.	Coordination.	Consider sealing trash bags with color-coded zip-tie or similar.	For larger events or those with security concerns.
• Do not place dumpsters/ trash receptacles under or adjacent to structural supports	To prevent a dumpster/ trash receptacle from being used as an IED.	During periods of high threat, exterior trash receptacles should not be placed within 100 feet of the venue.	
• Use sufficient dumpsters/ receptacles that will allow for pickup after the event		Consider using blast resistant receptacles. Plexiglas trash cans that are transparent should be considered.	
• Trash receptacles should be emptied regularly with contents placed in dumpsters			

ROBBERY/THEFT PROTECTION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Have a program and procedures to address securing cash collected during the event from robbery or employee theft. • Establish a central bank at the venue that receives monies collected from tickets, parking, and concessions (food and merchandise) and vendors • Should have at least two people • All cash movement from the event bank to a financial institution should be via armored car • Event bank should have CCTV coverage of access points, collection and counting areas and exchange and storage areas • Separate the cash storage area from cash receipt area • Cash should be carried in non-descript packaging concealing the contents from public - keep low key, don't draw attention to the moving of money • Establish a policy that no sales location can amass more than $2,000-$5,000 before transferring it to the bank • Event banks, with large amounts of cash, should have armed guards or law enforcement in the bank • Bank should not be easily accessible from outside venue	Robberies at events/exhibitions and their on- site banks have occurred many times. Pre-planning will help reduce this risk and mitigate issues.	Most of these thefts are based on insider information. Conduct scheduled and unscheduled employee bag checks. Technology such as security cameras and alarms should be used in the central collection or counting room.	Applicable if accepting cash for event entry, merchandise, etc.

Best Practice	Objective	Implementation	Applicability / Scalability
2. Coordinate with law enforcement to address response procedures for robbery or theft.	Reduce danger to patrons, event staff and law enforcement.	**See EAP**	
3. Establish procedures to prevent and address credit card information theft/ skimming.	Prevent loss of information or funds.	Include procedures in Event Operations Plan and coordinate them to participating public safety personnel. **See EAP**	

CYBER SECURITY

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
POLICY AND PLANNING			
1. Develop and implement a cyber-security plan. • Event/Venue Systems • Web/social media presence • Registration • Ticketing/credentialing • Client profiles • Permitting • Life Safety systems • Lodging • Logistics and Contracts • Transportation • Event Management • Venue Management • Electronic signage • Facilities/Equipment Management • Audio/Visual • Rigging and stage	In today's world this has become great risk. To protect people's personal information their life safety.	DHS, FBI and InfraGard can provide input/support and documents for developing the plan.	This is size independent and requires attention from event planning through post event.
HARDWARE/SOFTWARE/NETWORK			
1. Ensure that all operating software and hardware is regularly updated, patched and tested (i.e. registration, credentialing/ticketing, lodging, payments, life safety, medical, incidents, incident management, etc.).	Software currency to protect the integrity of the event. Prevent intentional misinformation. Protect against malware, viruses, ransomware and data loss.	Requires competent technical staff and coordination.	Larger events = bigger consequences. Both mobile and static devices, also during communications connectivity.

2. Install and maintain current cyber-security technologies and techniques (user authentication, firewalls, virus and spyware protection, encryption, etc.).	Must protect Personal Identifying Information (PII), healthcare data (HIPAA) and PCI compliance.		This is relevant for event venues and the presenting organization.
3. Backup all information on a regular basis and store in a secure offsite location.	To prevent data destruction, loss or taken for ransom.	Daily (preferable) or at least weekly backups, will prevent the event/venue from becoming a victim of ransomware attacks.	This is size independent and essential for business continuity.
4. Immediately report all breaches/intrusions/denial of service/Ransomware attacks to the FBI/law enforcement.	The sooner law enforcement can address the attack the better since it can limit system data damage loss.	DHS, FBI and InfraGard can assist with training programs and security tips.	Applicable to all size events.

CYBER SECURITY TRAINING

1. Provide regular user awareness training on security, policy, procedures, responsibilities, threats and incident reporting for staff and volunteers. • Document the training • Ensure records retention	Frequently, a lack of knowledge information results in unintended consequences. Proof for potential litigation.	DHS, FBI and InfraGard can assist with training programs.	All employees with any access to event systems/applications, regardless of device type.

CYBER ACCESS CONTROL

1. **Virtual** - User authentication/password access controls should be created that is "need to know" based.	Prevent unauthorized access.	Insider threats are the most prevalent. Access for all terminated/departing employees should immediately be cancelled.	All access control procedures are independent of size.
2. **Physical** - Access to information technology facilities should be controlled, so only authorized personnel may enter. • Access for all terminated/departing employees should immediately be cancelled	Insider threats and social engineering are the most prevalent.		Applicable to all size events.
3. **Cyber** – Data should be encrypted.		May be the responsibility of contracted vendors, IT teams or credit card processing companies.	Applicable to the transmission of any personally identifiable information (PII).

INVESTIGATION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
REPORTS AND RECORD KEEPING			
1. Have staff prepare a report on each complaint/ dispatch or adversarial interaction with a patron. • Create a documented process for intake of safety and security concerns from all sources speakers, vendors, attendees, staff, etc. • Use database format to easily research parameters	For defense in potential litigation, and maintain under a records retention program. Creates a record of concerns and allows for planned response and resource allocation.	The initial capture of information on an incident could be written on a card, documented or dictated on to a smartphone, then subsequently transcribed on to an incident report.	This is required regardless of size of event.
2. Photograph and/or video ALL individuals that are questioned, detained and/ or ejected.	For identification and event organization protection from incidents, accusations and litigation.	Many state laws may require that this policy be posted.	
3. Cite and record policy offenders, advise them that they may not be permitted to attend events for a year from the date of the incident, based upon offense. • Document all written trespass warnings and share as Be On the Look Out (BOLO) with law enforcement and venue personnel	Need appropriate records for enforcement, statistical analysis and potential litigation.		
4. Ensure accountability of all ejections through identification, documentation and a photograph.	Prevents ejected offender from causing additional problems and liability to the venue/event. It also ensures the safety of others.	Establish a "Phone a Friend" policy that requires any individual ejected for intoxication and who is not arrested, to phone a sober friend or family member to take responsibility for them. Document via government identification to whom the intoxicated person was released and have the person sign a waiver accepting responsibility for the intoxicated individual.	This should occur regardless of event size.

TRANSPORTATION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
TRANSPORTATION MANAGEMENT			
1. Create a written transportation management plan that addresses all manner of transportation modes public and private, use (from booking to delivery), boarding to delivery for your events to include drop-off/parking.	To manage/control patron travel that is under your responsibility.		Regardless of size, all events should have a transportation management plan. Small event, smaller plan; larger event, large plan. Complexity is a direct correlation to the number of attendees, scope of event, modes of travel and RTV Assessment.
PUBLIC TRANSPORTATION			
1. Private vehicles, taxis, rideshare, coaches/buses, subways, trains, airplanes and/or ferry boats may be used to travel to and from the event. Coordinate and anticipate the volume and safety/security of passengers. • Need to heighten security and conduct briefings on • unusual behavior, unattended/abandoned items, terminal/hub/station attendants • During peak periods increase law enforcement presence • Use these modes of transportation as an opportunity to communicate with attendees using signage or announcements concerning prohibited items, weather and other event info	Transportation safety and security awareness through training and monitoring.	This is based on the environment (urban, suburban, or rural), what types of public transportation are available, and by the size of the event. • These become potential targets because of the numbers of passengers, loading and unloading areas that causes patrons to congregate • May require additional units to handle surges For larger events: Metrics related to passenger volume over time for various modes and routes may be available from transportation providers. This information will be very beneficial for planning.	Only law enforcement, public safety, DOT or public works can legally regulate traffic on public roads. Coordination is essential for medium to large events otherwise our public safety partners have no idea of what is about to impact their environment. Often pick-up/drop-off points will be under event and/or venue control.
2. Consider and plan for those you can control, for evacuation/shelter concerns at these transportation hubs/terminals/stations. OR Work with those you use but don't control to ensure they have a plan in place.	Anticipate issues and plan responses. To work with transportation providers to establish contingency routing, pick up and rally points and share in advance.		Regardless of event size.

3. Communicate evacuation/shelter-in-place plans to your patrons.		Include in overall EAP.	Regardless of event size.

RIDESHARE SERVICES

1. Consider these evolving modes of transportation when planning your event and how your patrons may employ them • Pay particular attention to drop-off/pickup areas for these modes at your venues • Work with city/regional transportation department and rideshare service providers to establish designated drop off and pick up locations that mitigate traffic impact and allow for safe onboarding	Patron protection.	These become potential targets when the numbers of passengers, in loading and unloading areas causes patrons to congregate.	This is becoming a dominate mode of transportation and thus may require more preplanning. Consider in context with parking lots, bus/train drop-off/pick-up, pedestrian traffic and the overall perimeter.

BUSES/TRAMS/SUBWAYS

1. If it is necessary to move participants to/from transportation hubs using venue provided buses and/or trams exclusively, then the event/venue must ensure their safety and security.	Secure and safe movement.	This primarily becomes a coordination and scheduling issue.	This is going to depend on the environment and size of event.
2. Conduct background screening on drivers of these vehicles and credential both driver and vehicle. • Include insurance insulation in transportation contracts and	Litigation protection.	Example: Avoid having individuals with extensive problematic driving records or DUI offenses from driving these vehicles or if minors are involved making sure that drivers/attendants don't have sex crime offenses.	This is independent of event size.
3. Conduct searches of these vehicles prior to their use. • Need to heighten security and conduct briefings on strange behavior, unattended/abandoned items • Document training/briefing • Create signage to remind patrons to take items with them	Provide safe transportation.	Consider creating laminated, two-sided cards with vehicle search procedures for drivers.	This is applicable to larger events in which RTV is high.

TRAFFIC MANAGEMENT

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
MOVEMENT			
1. Develop a detailed plan for vehicular flow into and out of the parking lots.	This addresses the most disruptive aspect of the event on the community.	Define and agree upon the event traffic perimeter, area of responsibility or oversight in the planning process.	This is for larger events with heavy personally owned vehicle use. Crowd flow patterns will differ between arrival and departure.
2. In the age of new transportation modes (rideshare services) consider centralizing a separate drop-off/pick-up for these modes that fits into the overall traffic management plan.	Simplifies a location, is more user friendly, provides a safer environment and reduces congestion to traffic patterns.	This brings greater clarity to arrival and departure.	Fits all size events. Crowd density will be higher at these areas on egress than on ingress and could present more of a target.
STREET CLOSURES/BARRICADES			
1. Consider fixed or mobile barriers around the areas immediately adjacent to the venue. Block cross roads along pedestrian flow as necessary. • Reinforce areas that are vulnerable to forced vehicle entry with substantial barricades (i.e. bollards, retractable wedges, anti-ram fences, large trucks or buses, Jersey barriers, reinforced concrete decorative planters, etc.) • Establish proactive measures to thwart the use of vehicles as a weapon, especially in areas of congregating pedestrians	Creates a buffer zone. This has become a weapon of choice.	If roads are just closed with plastic/wood barricades, they should be manned by security/law enforcement.	This is for large events and those that are outdoors and in or adjacent to streets requiring closures.
PARKING			
1. All parking areas under venue oversight should be manned and controlled, or, at a minimum, patrolled.	The venue is responsible for the areas they control, own and lease.	Additional considerations for nighttime events include lighting, vests and flashlights for staff.	This is for large events and especially with elevated risks/threats.

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
2. All parking areas should be illuminated (from dusk to dawn) and, at a minimum, follow standards and requirements in applicable zoning ordinances and codes. • Portable lighting should be utilized in unlit areas or those not sufficiently lit by permanent lighting fixtures	For safety and security purposes.	For those venues with CCTV coverage, consider fixed or mobile platforms to monitor the parking lots.	Especially for events.
3. All lots should be patrolled or manned from the time the parking lots open until they are closed.	For the protection of patrons and the reduction in legal liability for venue/ events parking lots.	Could use roving patrols, elevated observation platforms and/or CCTV. Establish security patrols (security vehicles, bicycles, roving personnel, etc.) in the parking lots and perimeter of the venue.	This is advisable regardless of event size.
4. Consider pre-paid parking since it reduces potential theft of cash and risk to the toll collector/parking attendant.	Reduces risk.		If personally owned vehicle (POV) parking is significant or an issue. Also depends on venue and neighborhood RTV.

PHYSICAL SECURITY AND SAFETY

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Venues should employ protective measures (i.e. fencing, bollards, and enclosures) around exposed utilities such as transformers, natural gas lines, water values, air intakes, generators and telephone switch boxes to protect them against attack and/or damage.	To protect these utilities as they can be intentionally or are sometimes damaged accidently which has cascading effects.	Many ways to accomplish this through various technologies.	A RTV assessment will help identify what needs to be implemented when, where and how. Where and when appropriate, this is something that the venue should do and provide the event promoter/organizer with assurance of implementation/ compliance.

2. Have some full-time facilities personnel on-site during events at venue for maintenance issues and repairs; they should remain onsite until release by a supervisor. • Keep a record of who (repairman) is authorized to access the HVAC, mechanical, electrical, water, and gas/fuel/cooking systems with their contact information • Venue security personnel should accompany all repair persons as practical and necessary	When things happen, it is important to know when systems were last serviced/repaired and by whom. Also, need to maintain an up to date listing of service providers with contact numbers.	Ensure they have photo credential.	Especially important for large events. Where and when appropriate, this is something that the venue should do and provide the event promoter/organizer with assurance of implementation/ compliance.
3. Secure and protect with locks and/or tamper proof seals and/or monitoring via video surveillance.	Prevent tampering.	Let's you know through a quick observation if tampering has occurred. Also, relatively inexpensive.	This is advisable regardless of event size.
4. Test backup systems monthly and/or in compliance with local codes.	Prevents surprises.	Should include load and recommended warranty testing.	This is advisable regardless of event size.
5. Inspect and test all systems before every event and assign security staff or utilize monitoring devices to safeguard vulnerable systems.	Prevents surprises.		The larger the event the more important.
6. Conduct annual structural and physical inspections (to include equipment) and document inspection results/findings along with any remedial action necessary/taken. • Maintain these records for seven years (or as required by state laws)	Preventive measures and liability protection.	This should become part of the risk/threat assessment.	Where and when appropriate, this is something that the venue should do and provide the event promoter/organizer with assurance of implementation/ compliance.

HVAC

1. 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. • Security should be assigned to ensure doors are locked and if elevated threat, to guard vulnerable systems, including air intakes	Ventilation safety to prevent chemical/biological inhalation poisoning.	All HVAC, mechanical, gas/fuel systems and other critical systems should be inspected and protected with locks and/or tamper proof seals.	This is advisable for all venues. Event producers should familiarize themselves with the HVAC zones of the venue and use your contract to restrict unauthorized access to return air systems and return pathways to front-of-house areas of the building.
2. Mailrooms and loading docks should not share a return-air system or return pathway with other areas of the building.	Ventilation security safety to prevent chemical/biological inhalation poisoning.	In older facilities, where existing physical infrastructure makes it cost-prohibitive to retrofit separate air-handling systems; air sampling technology should be available for detecting biological and chemical hazards. Consider offsite mailrooms. State National Guard Civil Support Teams can assist in detection/monitoring.	This is applicable for large events with high risk. This prevents the introduction of biological and chemical agents delivered via mail/package delivery causing death or illness.
3. Inspect and monitor air handling intake vents monthly. • Document inspections	Ventilation security safety to prevent chemical/biological inhalation poisoning.	Rely on facilities personnel for this and require they report pre-event.	Event producers can include these requirements in their contract.
4. Employ physical or electronic monitoring of HVAC (air intakes).	Ventilation security safety to prevent chemical/biological inhalation poisoning.	Both for tampering by an individual or for monitoring of hazardous materials in the air.	This is advisable regardless of venue size and essential for high profile events.

UTILITIES

1. Maintain current contact information for all utility providers (electric/gas/water/fuel) in the venue maintenance office and/or Operations Center.	This will eliminate contact time. Reduce risk.	Both paper and digital.	For venues, regardless of size.
2. If anticipating potential issues at the venue or event, consider having utility company personnel onsite (i.e. adverse weather/threat).	This will eliminate response time. Reduce risk.		

ELEVATORS/ESCALATORS

1. Venues should test the systems and the emergency backup systems (under load) before each event. • Service personnel should be onsite for the duration of major or high-profile events • Work with venue security to ensure that personnel are available on standby to perform elevator lockout procedures should the need arise • Document test	To protect the safety of patrons. This will eliminate response time.	This is a venue responsibility, but event producers/organizers must hold them accountable.	Applicable regardless of venue or event size if elevators and/or escalators are present.

EMERGENCY/GENERATORS/BATTERIES

1. Test emergency backup systems (under load) before each event or request venue provide documentation of the last scheduled backup system test before the event. • Document test	To protect the safety of patrons and employees.	Ensure that venue generators are sufficient to support emergency systems to include Operations Center and cameras as well as emergency lighting.	Should be conducted regardless of venue or event size.

EVENT TALENT SECURITY/SAFETY

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Require identification of all talent, speakers, entourage and officials and appropriately credential them.	Safety of patrons, talent and staff.	Current intelligence and history will provide some predictive ability in scaling necessary protective actions and manpower requirements.	Should be required regardless of venue or event size.
2. Post a knowledgeable security guard on the green room, dressing/locker room door.	Talent security.	How much security will depend on the talent and the RTV?	Some talent may have their own security detail, and you will have to coordinate with them.
3. Prevent high-profile or controversial talent from entering or exiting in close proximity to hostile crowds, as it is not only unsafe for them, but for patrons and security personnel as well.	Potential problems with attendees, grabbing, pulling, throwing, spitting on/at talent as they enter the stage/meeting.	Demonstrations, history, and risk will dictate security requirements. Autograph seekers may also present an issue. Any attempts or actions should be a clear violation of your code of conduct and may be a violation of assault laws.	File complaints for arrest of any violations of law and remove anyone violating the established Code of Conduct.

BEHAVIORAL ISSUES

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
DISTURBANCES - PRE, DURING AND POST EVENT			
1. Develop written policies on how staff will respond to disturbances in conjunction with all participating law enforcement agencies, event managers and venue operators for: • Celebratory disruptions/rioting • Civil disturbances/demonstrations • Drunk and disorderly • Sexual harassment • Stage encroachments • Loitering • Theft • Fighting • Illegal drug use or possession • Thrown items • Use of vulgar language • Inappropriate/prohibited signage	Be proactive, since at some point in time these issues will arise and frequently end up in litigation. Have an established written Code of Conduct as applies to attendees, talent, and staff that is enforceable.	Alcohol tends to be a major contributing factor. If alcohol is permitted, the strong enforcement of over-indulgence will help reduce potential issues.	These policies should be prepared regardless of size.
PREVENTION			
1. Develop a written plan to prevent each of the above, and then practice it with staff.	Prepare staff–prevention is preferable to response and litigation. Also, less costly.	Use the Threat and Hazard Identification and Risk Assessment (THIRA). Anticipate various scenarios and conduct at least a table-top exercise.	Based upon event history, size, threat and current environment.
2. Adopt a Code of Conduct, post signage, advertise it and enforce it to discourage inappropriate behavior for your events. • Ensure staff compliance	Establish and communicate what conduct is unacceptable and what actions are to be taken if that code is broken.	Enforcement should be fair and consistent. Staff training is key!	This is regardless of event size.
3. Implement and advertise the "See Something, Say Something" program.	Be proactive and instill situational awareness.	Include today's technologies, such as texting and social media, as a vehicle for informing participants/patrons and for reporting violations. Resources are available from DHS and FBI.	Ensure staff and patrons know how and to whom to report.

RESPONSE/MONITORING/REPORTING

1. Train your team in Behavioral Intervention to address negative behavior issues.	Proactive anticipation.	Especially for larger events and those with a history of behavioral issues. At many venues with a high-profile event this may be handled by law enforcement or non-law enforcement security staff.	Good skill for an event planner as it helps in dealing with all types of people.
2. For large and high-profile events pre-plan and practice responses to all potential incidents, based upon past events.	Clarify skills, roles and responsibilities.	Where possible collaborate with local public safety.	Especially important for large events and those with high RTV.
3. Use social media monitoring for intelligence and early warning.	Predict and prepare for potential issues.		A very effective tool for situational awareness, especially for larger events and those with sensitive issues.
4. Fully document all actions taken and retain documentation. • Retain for seven (7) years or as required by state law	For litigation purposes and lessons learned.		Regardless of event size.

UNIFORM AND PLAINCLOTHES OFFICERS

1. For large and high-profile events use a mixture of uniform and plainclothes officers whenever possible.	Deterrence, observable help and situational awareness.	Uniforms serve as a deterrent and a visible point of contact for patrons needing help; while plainclothes serve as quasi-invisible eyes and ears that can provide intelligence and early warning and response.	For most meetings, conferences and conventions this will require hiring off-duty officers. What off-duty plainclothes officers can or cannot do at events varies between jurisdictions.

LIFE/FIRE/MEDICAL SAFETY AND PUBLIC HEALTH

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Identify and have accessible to event Operations Center and/or key staff, a list and locations of area hospitals and fire stations. • Have a minimum of one Fire Unit and one EMS Unit with two certified EMT's onsite for events of 15,000+	This will eliminate response time and may save lives.	Close collaboration with public safety can help facilitate this, sometimes at no cost.	Depends upon the size of the event, history, geography, community, weather conditions, attendees, threat information, etc. that could require scaling up.

2. Require pre-approval and provide pre-notification to public safety of specialty attractions (i.e. fireworks, pyro, parachutists, aerial shows/fly-overs, etc.).	These are a higher risk; thus approval, preparation and staging are required by municipal authorities. Reduces legal liability.	This sometimes requires weeks of advance notice.	This should be non-negotiable, regardless of event size and will require special response equipment.

FOOD AND BEVERAGE

1. Affix responsibility for the following food and beverage protective/preventive measures that should be considered: • Ensure all food service distributors/vendors/concessions are reasonably secure, inspected and licensed • Inform food distributors (pre-delivery) that any box, package or container that is open or appears to be tampered with, will be refused • All food and beverage deliveries should be recorded with: date, time, vehicle license number, company and driver name (view and record ID data from driver's license) • Inspect all packages/containers for tampering and if tampering found, refuse. • Notify law enforcement and food distributors (in that order) of actual or suspected tampering incidents • Conduct or require background screening on all food service employees/volunteers • Ensure all food service vendors and employees comply with local health standards, regulations, laws and appropriate inspections are conducted • Ensure food workers are trained in recognizing food contamination and reporting procedures • Ensure all food service vendors and employees are trained on "See Something, Say Something"	Prevent and respond to food borne issues. Protecting food supply from intentional or unintentional contamination.	The local Health Department can assist with food/water borne issues. Include local Health Department food inspectors in the EAP planning and in formal operations plan, provide communications contact in event of a tampering or to report other patron food/drink issues. This is true for event-provided food and drink as well as vendor-provided food and drink for sale. This will require close coordination with food service personnel frequently provided by the venue or caterers/vendors and their compliance with public health authorities.	If it is your event, the responsibility will ultimately fall on you for due diligence reliability. This is especially true for high-profile events with significant attendees.

ALCOHOL MANAGEMENT

1. Create clear alcohol management policies. Specify that intoxication will not be tolerated at the venue/event and enforce it.	Lack of policy increases your liability. Public intoxication/disorder. Lack of enforcement.	Since alcohol is a major contributor of disruptive behavior this is a must, also it is a key contributor to incidents ending up in litigation. Policy needs to be communicated to attendees. Local standards and practices may be different than at other events/venue. **See Crowd Dynamics/ Management (CDM) - Alcohol Management**	This is independent of event size.
2. Ensure employees serving alcohol are of age and have been trained in state laws and in recognizing signs of impairment and how to refuse service. • Document training and testing	Employee knowledge. Reduce liability.	Utilize Techniques for Effective Alcohol Management (TEAM) training for ALL event staff. Event Producers can ensure that liquor liability insurance is issued by serving entity which should put liability squarely on serving entity and insulate the event producer if they are not the directly responsible for serving alcohol.	This is independent of event size.

WEATHER PLANNING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
DEVELOP PLANS			
1. As part of the EAP (for both event and venue), develop, review, train and exercise weather safety plans for all types of adverse weather and response which includes: sheltering-in-place, evacuation and re-entry after an evacuation. • Develop a weather situational awareness plan for each event • Discuss and practice shelter-in-place/evacuation procedures • Decide under what circumstance a game or event will be delayed or cancelled • Include communications technologies during testing • Conduct exercises to identify gaps • Create timeline for monitoring and contingency preparedness • Establish a rally point (if no operations center) in advance for senior staff who can make the appropriate executive decision to delay or cancel an event due to weather	Being prepared and planned for all manners (i.e. heat, snow/ice, hail, wind, rain, flooding) of adverse weather. Use a weather service.	Ensure close coordination between event and venue. FEMA and National Weather Service (NWS) can assist in planning and training for weather conditions. **See EAP** **See National Oceanic and Atmospheric Administration (NOAA) Venue Preparation Checklist** Numerous commercial products exist to monitor weather and alert patrons. Also, local broadcast stations have meteorological equipment and staff. Can be trained and tested through a table-top exercise.	This is applicable for all events, but is particularly important for outdoor events.
2. Simplicity is key-staff will need a simple plan to follow in the event of severe weather conditions.	Timely implementation is critical when employing the weather safety plan.	Good planning, concise directions, familiarization/ training of staff and public safety team are essential.	

MONITORING

1. Weather monitoring is essential to ensure safe events. • Establish trigger points to take action based upon current circumstances • Ensure there is sufficient lead time as adverse weather approaches so appropriate action can be implemented in a timely and safe manner	Being prepared for all types of adverse weather (i.e. heat, snow/ice, hail, wind, rain, flooding and lightning). Planning and practice.	Various methods of monitoring are available through public emergency management, as well as through TV and radio stations and commercial products such as smartphone apps. • If storms are forecast for the day of the event, review safety plans before the event and identify the responsible officials and chain of command to implement the safety plan • You could utilize a subscription weather service to receive alerts as well as tapping into a local National Weather Service. Have contact information for on-duty meteorologist as a backup.	This is applicable for all events. Particularly important for outdoor events.
2. For outdoor events, seek Storm Ready Certification by FEMA/National Weather Service.	Weather mitigation preparation.	Refer to https://www.weather.gov/stormready/	

1. Use weather monitoring and lightning detection tools along with local observations to help determine proximity of lightning and which safety actions to implement (per NOAA). Direction and speed of approaching weather should be accounted for along with locally developing storms that may form nearby. Must establish distances based on the speed of the approaching storm and the time it takes to evacuate the venue or shelter-in-place. FLASH-TO-BANG CONCEPT Begin counting when sighting a flash of lightening. Stop counting when BANG of lightning is heard. Divide the count by five to determine the distance to lightening in miles. EXAMPLE: Flash to Bang = 30 seconds 30 divided by 5 = 6 Lightning is 6 miles away	Lightning monitoring, alert and response.	Severe Thunderstorm or Tornado Watch: A watch indicates conditions are favorable that severe weather may develop. A time period is associated with the watch. Severe Thunderstorm or Tornado Warning: A warning means severe weather has been detected and may be imminent in the area. A time period is associated with the warning. Flash Flood Watch: A watch indicates developing conditions are favorable for flash flooding in the watch area. Flash Flood Warning: A flash flood is in progress, imminent, or likely. Water is expected to rise rapidly. Refer to: www.lightningsafety.noaa.gov When lightning is detected within fifteen (15) miles of the venue: • Notify management and event officials of elevated lightning monitoring • Venue management notifies all staff of potential for a delay designated staff are stationed to direct patrons as necessary • In these cases, the speed and direction of storm movement should be determined and the time that it will enter an eight (8) mile radius of venue. Evacuation from the facility or a shelter-in-place should begin if it appears the thunderstorm is moving toward venue. • Venue management notifies all staff of the potential for a delay designated staff are stationed to direct patrons as necessary When lightning is detected within twelve (12) miles of the venue: • Venue management and officials are notified of impending lightning threat • Venue management notifies all staff of impending delay or suspension designated staff are stationed to direct patrons as necessary • Shelter-in-place begins or continues. If more organized thunderstorms (supercells, squall lines, bow echoes) are headed for venue, evacuation may be required When lightning is detected within eight(8) miles of the venue: • Management and event officials are notified of nearby lightning threat and an event suspension is implemented • Event officials suspend activities • Event management notifies all staff that event has been suspended due to lightning designated staff are positioned to direct crowd as necessary • Evacuation of venue begins all patrons, officials, performers are directed to nearest pre-designated lightning-safe shelter	This is applicable for all sizes of outdoor events.

SHELTER-IN-PLACE

1. Develop, train, and follow the Sheltering Plan in EAP. • Ensure there is sufficient sheltering capacity for the total numbers of patrons, participants and staff • Ensure staff is familiar and trained on the plan	A plan and pre-event familiarity is a must.	Plan, train, exercise. **SEE EAP**	This is applicable for all event sizes.
2. Sheltering by its very nature is temporary but must be accommodating based on the cause for sheltering and the anticipated numbers requiring shelter. Evaluate all potential sheltering areas against all possible incident types to determine their ability to offer sufficient protection from various perils (i.e. thunderstorms, lightning, hail, tornados, ice, flooding, hazardous chemical release) along with the total number of individuals each area can safely accommodate. • If substantial space is not available, enclosed motor vehicles (not optimal) can provide shelter as long as individuals do not touch the metal framework during a thunderstorm • Determine who has the authority to make the decision to shelter-in-place and how it will be communicated • Length of time to shelter-in-place is going to be a factor and must be considered	Plan ahead to prepare for all eventualities. List options by name.	Making the decision to shelter-in-place or evacuate during an incident is a complicated process and requires input from various entities. Things to consider are the facility, the number, distribution and condition of the patrons, participants, staff, the hazard involved and the anticipated response to that hazard. Pre-planning is a must.	

EVACUATION

1. Develop, train/exercise, and follow the Evacuation Plan in the EAP. • Have an accurate estimate of how long it will take for total evacuation of the venue (it should not be more than 20 minutes) • Ensure staff is familiar and trained in the Plan	A plan and pre-event familiarity is a must. Event staff must be familiar with and trained in the evacuation plan.	Plan, train, exercise. **See EAP**	This is applicable for all event sizes.

2. An evacuation requires a plan for moving patrons, participants, staff out of the hazardous area. • Identify the individual who has the authority to make the decision to evacuate	Know the what, where, why, when and how, realizing the impacts of each by name.	Making the decision to evacuate, shelter in place, or relocate during an incident is a complicated process and requires input from various entities knowledgeable in the geography, surroundings and structures, the size, distribution and condition of the patrons, participants, the hazard(s) involved and the anticipated response to that hazard. That is why it must be pre-planned. Sometimes the best course of action is NOT to evacuate, but this must be an informed decision.	

REUNIFICATION

1. Identify a Family Reunification Center(s).	A facility or area where attendees are reunited with their families and friends.	No matter the size of the event this should be planned for and scaled accordingly.	The bigger the event the more significant the planning.
2. Identify and coordinate transportation needs and solutions to move participants to assistance center(s).	Transportation.	Pre-plan needs.	
3. Staff and train sufficient personnel to handle (or contract out) the assistance center(s). • Ensure sufficient communication capability	Manpower and communication.	Red Cross/Salvation Army or other community-based organizations can possibly assist. Check with them in advance for capability.	

DECISION MAKING

1. Planning for evacuating/sheltering/relocation should specifically identify decision-making levels and authority, with one person on-site who will make the decision. • Develop decision trees and trigger points	Avoid confusion and assign responsibility to an individual by name who will be on site.	Make sure when implementing the Plan, that enough time is included for staff to be in place when the evacuation order is given to guests/attendees.	This needs to be closely coordinated between event director and venue director. This should be established pre-event independent of staff rank based on the senior staff member most likely to be in a position to make the decision in a timely manner should the need arise.

2. Provide advance, real-time information on severe weather to patrons (i.e. video board(s), ribbon board(s), social media, local radio announcements); allowing them to make personal decisions before any mandatory sheltering or evacuation order is issued.	Awareness.	Also utilize TV and radio outlets that carry the event to communicate with patrons still in transit to the venue and to provide updates if they are standing by following an evacuation.	
3. Develop a policy and process for re-entry after weather related evacuation. • If sheltering takes place in a secure area without opportunity for the introduction of prohibited items, rescreening is not required • If sheltering takes place in an unsecured area that allows for the potential introduction of prohibited items or unscreened individuals, Re-screen patrons who re-enter venue/event	Reloading venue after evacuation.	Staff should be trained on this procedure. If screening performed, re-screen on re-entry.	Applicable for any size events.

BOMB THREATS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Have a written plan that is part of the EAP that dictates criteria, role/responsibilities and identifies who makes the call, on evacuation or not, for a bomb threat.	Bomb threats are highly disruptive and cause mass confusion over what process to follow, who makes the decision and when to evacuate and how to notify personnel and attendees. Can be very manpower intensive.	**SEE EAP** Follow ICS Unified Command structure. • Have pre-written communication messages for patrons • Define assessment process (FBI and BATF are resources) • Define evacuation process as set forth in the EAP Evacuation Plan for such an incident • Define who is responsible, venue or local government Train receptionist and Operations Center staff on FBI/ Bureau of Alcohol, Tobacco, and Firearms (BATF) Bomb Threat checklist for receiving calls. Coordinate with local law enforcement to trace/ track incoming calls.	This is applicable for all event sizes. Law enforcement can assist in preparing this plan.

2. Make use of the ICS Unified Command for assessment, decision process and response.	Leverage expertise.	Follow NIMS ICS Unified Command structure.	
3. Develop a threat assessment team.	Avoid confusion and lack of expertise.	FBI is a great resource for this.	Provides necessary expertise for decision making.
4. Use Bomb Threat Caller Checklist and train staff who may receive calls. • Install caller identification and/or coordinate phone call trap capability on landline phone	Reduces response time. Identify resources in place based on threat assessment.	FBI, BATF and DHS offer checklists. Consider that the threat may come via Voice over Internet Protocol (VOIP) or social media.	
5. Ensure that all incoming threats, whether telephonic or via other media, are properly recorded and preserved for at least two calendar years following the year in which the threat was received.	For prosecution/litigation purposes.	Seek advice from legal counsel on number of years to retain recorded documentation required (recommended) by local jurisdiction.	
6. Have pre-written announcement messages available to notify patrons as to what actions shall be taken under various circumstances.	So announcements are ready to go during a crisis.	Can be used for social as well as traditional media messaging.	This saves time in the heat of a crisis and avoids confusion or misinformation.
7. For high-profile/high-risk events, if resources are available, conduct bomb sweeps of facility, buses, nearby parking lots, media compound, food/concession deliveries. Once completed, maintain control through: • Access control • Bag checks • Credentialing • Lockdown once cleared • No re-entry policy	Search and secure.	Certainly, for large-scale events resources should be made available. If evacuated for a bomb threat and re-entry is considered, must conduct a full venue search, and re-screen before re-entry.	This is either contracted or provided by local/state law enforcement.
8. Develop procedures and train event staff on suspicious items response and handling. • Establish a code so that staff doesn't use the words bomb or suspicious item when reporting over the radio or phone • All staff should be trained in bomb threat response	Be prepared. This serves to protect both staff and patrons.	Besides law enforcement, the military has EOD resources. For planning purposes bomb dogs on average have roughly a 20 minute active search capability, then must be rested for about 30 minutes to be effective.	Certainly, for events with known threats, resources should be made available.

FIRE ALARMS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Venue or event planner should develop written processes and procedures (part of EAP) with the fire department(s) to deal with fire alarms.	Often fire alarms are ignored or are false alarms. Must be resolved without causing panic or unnecessary delays.	**SEE EAP** A command level fire department representative should be in the Command Center for all events with 10,000+ attendees, at a minimum.	For all size events.
2. Plan should include the decision-making process to resolve alarms. Identify the individual (by name) who will make the decision to evacuate.	Cautionary action.	Local fire department(s) can and should assist in this process. Some hotels do not evacuate meeting rooms if the alarm is on a sleeping room floor. The plan should include this information to clarify the course of action that will occur if an alarm is activated in the building.	
3 The Plan must deal with the ability to monitor and override the system (i.e. post a fire fighter at alarm panel and send an event staff member to the alarm point).	Turned off fire alarm system, in lieu of using an on site fire fighter.	Pre-plan with fire fighter/ Fire Marshall on site. Many large venues have firemen on site. Some state or local laws require evacuation if fire alarm goes off.	For large, high-profile events a fireman on site is recommended.
4. Plan should define the process to make notifications (patrons/talent/staff).		Specify methods of notification.	

PUBLIC INFORMATION PLAN

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Designate and authorize the Public Information Officer (PIO) for events to respond to the media and the general public in case of an incident to establish a single authorized, authoritative voice.	Avoids confusion when an incident occurs, of info from multiple sources.	Use the most experienced individual, regardless of organization/agency, who will be available on site during the event.	For weather, criminal, terrorist incidents public safety PIOs will respond to the media, but if you want your entity (event/ venue) represented with your message it is incumbent upon you to have your designated person.

2. Develop policies and procedures to advise the media and general public of the situation, and to defuse rumors along with panic. • Address how the venue emergency notification system is applied during an event • Address use of social media, who is responsible for disseminating public safety info during events	Effective continual communication minimizes confusion and protects you and your clients' brand.	This may require a collaborative effort since different organizations may have different rules and goals.	For large events establish protocol for PIOs from relevant departments (police, EMS, Fire, City Government, and event PIO) to coordinate messaging and timing to ensure consistent, relevant communication to press, public and patrons.

HAZARDOUS MATERIALS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Venue should have a written plan for dealing with hazardous/toxic material exposure (i.e. fuels, propane, chemicals, fertilizers, garbage, sewage, etc.) as part of the EAP. • Ensure that appropriate individuals are trained on the plan	Ensure safety for workers, participants and patrons. Reduces liability.	**See EAP** The local fire department and FEMA can assist with training and documentation. OHSA can also provide information on this subject.	Event planner should ensure that the venue has such plan.
2. In conjunction with local public safety partners, venue should coordinate a decontamination plan.	Be prepared.	The local fire department and Emergency Management would implement as necessary.	
3. Venue should establish a Hazmat Response Team that is trained to the Hazmat Level 2 defensive level, or a reasonable substitution such as local fire department.	Staff expertise. Reduces legal liability.	Important for larger venues, smaller venues should try to have at least one person HAZMAT trained and works closely with the local fire department.	Venue will be responsible for assisting with spill clean-up/containment efforts.
4. Ensure that hazardous materials are not stored in close proximity to the event. • Prevent fume buildup		Conduct inspection prior to event-consider requesting local Fire Marshall to accompany inspection team.	

PERMITTED AND PROHIBITED ITEMS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
POLICY AND PUBLICATION			
1. Establish a written policy in conjunction with the venue regarding permitted and prohibited items that will or will not be allowed in your event/venue property. • Items to consider prohibiting: coolers, bags, strollers, backpacks, containers, alcohol, explosives, chemicals, flammable liquids, weapons, outside food or beverages (except as required for authorized medical needs) • Post a list of prohibited items in parking lots, transit points and entrances to venues	Must be written and communicated to be legally enforceable. To reduce confusion and prevent patrons from getting to the gates/doors with prohibited items.	Communicate these policies and, that patrons consent to these searches as a requirement for entry to the venue/event. If pre-entry screening is conducted, all primary screening should be conducted by non-law enforcement security staff and backed up by law enforcement where possible. Be prepared for patrons to dispose of prohibited items in bushes, trash receptacles, and under vehicles outside of the door/gate/perimeter.	It is advisable to have this policy for all sizes and types of events. What is prohibited/permitted may vary by type of event/attendees/venues/location.
2. Once established, publicize policy in the broadest manner possible to include the screening/inspection process and penalties for breaches.	Policy awareness.	Should be part of your online and document packets for patrons.	
3. Have a procedure in place and train staff on how to handle patrons that have prohibited items. Enforcement should be consistent and have a zero-tolerance policy		Decide to: • Refuse admittance • Require they take item(s) back to their vehicle (what if they used public transportation) • Have a disposal bin and require they dispose item • Have them check the items at a bag check facility	

FIREARMS: CONCEALTED AND OPEN CARRY

1. A specific policy should be established for lawful open and concealed gun carry on property and venue during an event.

Private Citizens
Review and follow state laws concerning private citizen concealed or open carry on property.

VIP Protective Security Personnel
It is recommended that these individuals not bring their weapons into the venue or check it into an on-site lockbox; if available.

In some states, laws prescribe who can and cannot lawfully carry (particularly on state property). However, most states allow or are quiet on off-duty law enforcement.

Legal requirements related to concealed and open carry vary and are rapidly changing. Not only are there differences as to what is and is not allowed between states, but also for public and private properties. The goal is to offer safety, avoiding an accident or mistaken identity.

Consult legal counsel. Recommend to not allow concealed or open carry of firearms by private citizens or auxiliary/reserve officers (unless working) on the property (parking lots, venue, etc.).

Producers should work with their venue management to ensure that all requisite signage and notifications are made to restrict concealed and open carry on property.

This will require coordination with the venue, as they may have an existing policy. This also will likely vary in some states between private vs public venues.

Also worth noting that producer should inquire with any VIP or executive protection teams whether they will be armed. This information should be relayed to any onsite law enforcement and vice versa. Armed security, protection teams and police should all be aware of each others' presence on site.

SCREENING POLICY, PROCEDURES AND TRAINING

1. For those events where screening is required, establish written policies and conduct staff training for screening individuals and possessions. Procedures should include the use and deployment of staff and equipment.
- Address any exceptions such as: medical devices/equipment, VIPs, officials, etc.
- If patrons refuse to be screened they should be denied entry into the venue
- Document training and testing

To protect event from dangerous and unwanted items.

Legal defensibility.

Test screening equipment and staff performance under actual live conditions and in real condition (i.e. red team tests).

Whatever primary method is used for screening, have secondary or back-up devices/methods.

This will be dependent on RTV assessment, the type event, attendees, client, talent and overall threat.

BAG/CONTAINER CHECKS (IF IMPLEMENTED)

1. Inspect ALL possessions, items and/or containers that are permitted into the venue.
Ensure sufficient lighting at all screening areas for evening events.
All primary screening should be conducted by venue security staff and backed up by law enforcement.

Prevention/protection.

Clearly post signage concerning checks.
Ensure that staff responsible for inspecting bags is properly trained. The DHS's *Sports Venue Bag Search Procedures Guide* and "Check It" bag search video should be considered for staff training.

Be consistent.

PERSONAL SCREENING (IF IMPLEMENTED)

1. Conduct 100% screening of all individuals entering the venue.	Prevention/protection. The only way to prevent prohibited items from entering the venue.		Be consistent.
2. Set up special entry lanes/doors around venue/event for: • Patrons with NO items to screen (express lane/door/gate) • Patrons with medical devices (oxygen tanks, medical syringes, wheelchairs, etc.) • Mothers with diaper bags for young children (must have child with them)	To expedite entry and ensure consistency.	Ensure sufficient signage to make patrons aware.	

SIGNAGE

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. The following signage measures should be used during all events. They should be displayed in highly visible and static locations: • Signage listing contact number(s) for security and/or safety personnel and for reporting suspicious activity • Signage in parking/transportation areas listing prohibited items and identifying acceptable containers • Signage at all pedestrian and vehicular access gates, indicating entrance is conditional upon screening and reiterating prohibited items • Signage throughout the venue that identifies current location relative to exits • Signage indicating what type of access (credentials) is allowed in a particular area • Signage directing deliveries to appropriate checkpoint and destination • Signage for emergency exits that are marked and lighted	Signage is essential to the orderly conduct of an event. Saves patrons from getting all the way to the venue doors with prohibited items and having to go back to their vehicle or abandoning the item(s) at the door or checking the item(s). Many attendees may be unfamiliar with the venue and in an emergency may become confused.	Multiple methods may be employed including paper, wood, metal and video boards. Consider using social media as a method to communicate this information ahead of and during the event.	Signage is especially important if you conduct screening and directing patrons.

TOPICAL AREA: PEOPLE MOVEMENT AND MANAGEMENT

PEOPLE/CROWD MOVEMENT			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY / SCALABILITY**
1. Study flow patterns in and around the venue to identify manageable methods to prevent over-crowding at any location. • Also analyze patron arrival times, how they arrive, what they bring, etc. • Conduct surveys of arriving crowd, ask where they parked, how they arrived (shuttle, mass transit), how long they stood in line, etc. • Use CCTV to follow a guest and monitor how long until the guest arrives at the door	To reduce congestion and enhance patron experience. To better plan for effective people movement through event, evacuation and sheltering-in-place. Liability mitigation.	Video coverage/capture is essential to conducting and validating the analysis both real-time and after event. Several modes of transportation (cars, trains, subways, buses) may offer electronic tracking of passengers.	This is beneficial and necessary for events of 100 or more patrons entering and moving around a venue. The larger the event (many patrons) the more important.
2. Develop a People/Crowd Management Plan, (ingress/egress, density, direction, speed, capacity, etc.) utilizing industry methodologies. • The key to understanding space requirements for a crowd is understanding how much space is required for each person (density = people per square yard or meter)	Predictable is preventable. Anticipate crowd dynamic issues.	Local Fire Marshall can assist as in most cases the Fire Marshal will have to approve occupancy and permitting. Having trained staff and processes in place for rapid dissemination of specific instructions is critical in preventing and mitigating potential problems.	These event plans can help you in preparing for many future events.

3. The development of a Crowd Management Plan must take in to account crowd dynamics and employ some reliable analytical tools.
 	
  • The following tools have been validated to provide effective analytics:
    • **DIM** = Design – Information Management
    • **ICE** = Ingress – Circulation Egress
    • **RAMP** = Routes – Areas – Movement Profile
 	
Three primary influences on crowd behavior (DIM):
DESIGN
• Site areas-different usage of space-static or moving crowds, capacity, ingress/egress flow rates, normal and emergency.
INFORMATION
• Signage, maps, social media, news reports, site communication systems, normal and emergency information.
MANAGEMENT
• Process, procedures, communication systems, chain of command, normal and emergency situations and relaying information to those responsible for public safety.
 	
There are three primary phases of crowd movement/behavior: (ICE)
INGRESS
• Getting in, queuing, screening, barrier design, information, management, flow rates, arrival profiles, early detection of problems.
CIRCULATION
• Moving around–queuing, design, information/signage, management, contingency planning, red flagging
EGRESS
• Getting out, flow rates, egress times, congregating. Normal and emergency, red flagging
 	
You need to understand how these phases and influences affect crowd movement/behavior.
Dynamics = Routes, Areas, Movement, Profile (RAMP)
ROUTES (directions)
• Which directions are the crowds moving (ICE)?
AREAS (spaces)
• What space do we have? How is it used?
MOVEMENT (flow rates)
• Over what periods of time will crowds arrive/depart? How quickly do the key spaces fill (i.e. queuing spaces)? What elements may change the arrival/departure rate?
PROFILE (people)
• What do we know of the crowd demographic/history?
	Reduces legal liability.
	
	Prevention/protection.
		These tools are designed to collect/collate information for events. They are used to:
		  • Compare and contrast events
		  • Identify areas for improvement
		  • Standardize the event planning/licensing/operations
		  • Determine capacities and flow
			Applicable to any size event.

4. Crowd Modeling is an essential element of developing an effective People/Crowd Management Plan. To begin modeling there is a need to understand the venue, its capacity, access and egress routes, the transportation infrastructure, venue constraints under different configurations and weather conditions. Key questions for initial analysis: • What is the type event and why is the crowd coming to this venue?	Reduces legal liability. Prevention/protection. Improves patron experience.	Failure to recognize risk is evidence of either negligence or incompetence in event planning. Three fundamental elements that was common to major incidents are: • DESIGN – related incidents, appear to have been a miscalculation to crowd flow and space capacity • INFORMATION – related incidents, appears to have been an external influence on crowd behavior that induced an accident/incident • MANAGEMENT – related incidents, appears to have been one or more management decisions responsible for accident/incident Most major crowd disasters can be prevented by simple crowd management strategies. Primary crowd management objectives are avoidance of critical crowd densities and effective flow patterns.	For events with 100+ patrons.
5. Have trained crowd managers for events. NFPA recommends a ratio of 1 trained crowd manager for every 250 patrons.	Reduce legal liability.	NFPA Crowd Manager requirements (NFPA 101®: Life Safety Code®, Sections 12.7.6.1/13.7.6.1).	This is important for the wellbeing of patrons.

6. Crowd Management Plan should address the following: • Ensure exits are marked, exit doors are operational, and all egress paths are unobstructed • Ensure fire alarms, sprinkler systems, and emergency lighting is operational. • Ensure fire lanes are unobstructed • Put in place an emergency notification plan, including how people will be notified and who will deliver the message • Ensure aisles and other exit routes remain clear throughout the event • Identify potential spaces and events where crowd • management requirements would apply • Develop a simple training program and a checklist to be used by crowd managers	Prevention/protection.	Fire Marshall can assist. Become versed in the NFPA Crowd Manager requirements (NFPA 101®: Life Safety Code®, Sections 12.7.6.1/13.7.6.1) and the requirement of the local agency having jurisdiction. Some jurisdictions have different thresholds, and they may allow for changes in the requirements based on the nature of the event or whether or not a building is fully equipped with sprinklers.	

BEHAVIORAL PATTERNS/ISSUES

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
BEHAVIOR AND CONTROL			
1. Establish, communicate and enforce a Code of Conduct (rules of acceptable and unacceptable behavior). • Include Code of Conduct to event day program and online • Post signage where possible • Be consistent with enforcement • Encourage and provide a platform/mechanism for patrons to report violations	Prevention over confrontation. Deters continued acts of unacceptable/disruptive behavior. Gives you the legal basis to take action when required. Helps manage expectations.	Involve all stakeholders (venue management, event staff, law enforcement and patrons) in the process of establishing the Code to ensure buy in from all groups that have a role in following and enforcing it. Set standards, stick to them and hold violators accountable. Be fair and consistent across the board when enforcing code/policy violations.	This works for all size of events, but the larger the event and the larger the venue the more important this becomes.
2. Advertise and enforce sanctions for inappropriate behavior.	Create awareness as to what is acceptable and what is not.	Communicate prior to and during the event. Broadcast prior to event and during intermissions/ breaks.	

3. Work within and across venues and the event industry to develop a baseline patron Code of Conduct.	Consistency among events/venues.	Set consistent expectation regardless of location.	Events/venues can expand upon baseline based on the needs and demographics of their event.
4. Designate smoking areas if allowed by local or state law and enforce and a no smoking policy outside of those areas.	Attendee health and comfort.	Most venues already have this in place, many states and cities have laws prohibiting smoking in venues.	

CULTURAL AND DISABILITY AWARENESS

1. Develop legal, fair and consistent policies that are in compliance with ADA and civil rights laws that will serve to avoid claims of bias from profiling, discrimination or mistreatment. • Include a specialist as part of event operations, such as an on-duty ombudsman for referral of complaints, ADA compliance or biased based conduct • Understand the limitations and capabilities of the operating venue • Ensure proper training by venue staff of operation of equipment such as ADA lifts, vehicles or ramps	Provides standards and guidance in the treatment of patrons and staff for fairness and consistency. Reduces legal liability. Ensure readiness of event staff in compliance and communication.	Include cultural and disability awareness, including the use of service animals in staff training. Involve human resources and expertise in planning, policy development and training.	This serves to insulate event liability from lawsuits.

EVACUATION/SHELTERING-IN-PLACE

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Follow the Evacuation/ Sheltering Plan in the EAP for the venue. • Develop with input from public safety partners and venue facilities staff • Take into account attendance, considering both participants and patrons • Review with Incident Command staff at briefings • Designate official who will make the decision • Plan should cover all-hazards • Train staff as added and reinforce before every event • Exercise the plan	Life safety is first and foremost. Provides instructions and guidance to effectively address safety of all individuals in attendance.	**SEE EAP** The Evacuation/Sheltering-in-Place plan is an essential element of the EAP. Test staff on evacuation job duties, evacuation routes, etc. Ask staff the following questions before each event: • Where is the nearest fire extinguisher? • Where is the nearest exit? • If that exit is blocked, where would guests be directed?	Size of event will define complexity, but all size events require an evacuation/sheltering plan. Plan will likely require approval of the Fire Marshal in many jurisdictions. This may be the responsibility of the venue or the event producer.

2. Prior to initiating an evacuation, take into consideration the inherent risks with an evacuation. • Sometimes the best course of action is not to evacuate, or to partially evacuate, and sometimes shelter-in-place or relocation is the best option • Determine the least invasive and most effective method to evacuate attendees from potentially dangerous conditions to include partial evacuations • Evacuation planning should be based on a risk assessment that takes time and distance into account	Think through the process, pre-plan as the decision will likely depend upon the situation at the time. Know your options.	Based upon a people management analysis, identify sheltering-in-place (occupancy) throughout the venue for various incidents, in conjunction with the Fire Marshall. Consider today's social media environment when making decisions and anticipate that it may outpace venue communications if decisions are not made in a timely fashion. Staff training is critical. Brief and exercise procedures.	
3. Making the decision to evacuate, shelter-in-place or relocate during an incident is a complicated process and requires input from various entities knowledgeable in the structure of the facility, the size, distribution and condition of the patrons, participants, the hazard involved and the anticipated response to that hazard. • Identify the individual who has the authority to make the decision to evacuate/shelter-in-place/relocate, along with how it will be communicated	Consider all inputs and hazards. Reduces confusion. Identify ahead of time the parties involved in making this decision and have pre-defined rally point(s) to convene should a decision need to be made.	Plan, train, exercise. **SEE EAP** Must be on site.	
4. The full or partial evacuation, sheltering-in-place, relocation, including designation of routes, should be identified and evaluated for each type incident during planning and updated regularly.		These should be included in the Plan and is applicable to all size venues.	

EVACUATION

1. Follow the Evacuation/ Sheltering-In-Place Plan in EAP. • Ensure staff is familiar and trained in the Plan • Pre-scripted messages should be prepared and used for all contingencies • Understand where people will be evacuated to in the venue	The Evacuation/Sheltering-In-Place Plan should provide instructions and guidance on effectively addressing the safety of all individuals.	The Evacuation/Sheltering-In-Place Plan is an essential element of the EAP.	Essential for all size events.
2. Approach an Evacuation/Shelter-In-Place/ Relocation Plan by first assessing the potential hazards created by an incident. Then recognize and understand the inherent characteristics, strengths and weaknesses of the venue's infrastructure and available resources.		Review all possible causes and plan accordingly. Determine the least invasive and most effective method to evacuate people from potentially dangerous conditions to include partial evacuations/shelter-in-place and relocations.	
3. Have EMT and medical personnel on standby to treat injuries.	Ensures timely response to slip-and-fall incidents and stress/exertion related ailments.		Especially for large events.

SHELTERING-IN-PLACE

1. Follow the Shelter-In-Place Plan in EAP. • Ensure staff is familiar and trained with the Plan • Must identify sheltering areas, their capacity and routes to them	Plan, train and exercise.	**See EAP** Use computer simulations to test plans and train staff as often as possible.	
2. Pre-determine sheltering locations and capacities based upon length of sheltering (event based) for various weather or chemical release incidents.	Foresight allows for better understanding of potential outcomes.		Shorter terms of shelter can accommodate closer positioning, longer sheltering requires greater individual space.
3. Sheltering-in-place should always be considered as an option for protecting spectators and participants from adverse weather conditions.	Based upon circumstances, pre-designate areas for housing/sheltering.	This is going to be dependent upon the environment (rural, suburban or urban) and surrounding facilities.	

VOLUNTARY VS. MANDATORY

1. Time, conditions, circumstances, number of people and the incident type will dictate whether the action is voluntary or mandatory. • Anticipate that an incident could occur that causes a non-ordered impromptu/panic mass flight/evacuation–consider how to respond	Anticipate different potential causes and outcomes. Unanticipated incident.	This is clearly the most dangerous of situations due to panic/stampede flight. Plan response on how to use crowd flow, environment and methods of communication.	This is when a well trained staff pays dividends and saves lives. Even in non-hazardous weather conditions expect crowds to instinctively seek shelter.

COMMUNICATION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Use the venue's PA system, video capabilities, website, and social media to provide information and communicate with guests that are at the event/venue.	Broadest coverage to reach out.	Consider public safety communication capabilities, commercial radios, landlines, cellular, HAM radios, video boards, broadcast media, social media, PA systems and public safety vehicles.	Know what you have to communicate with at all times since it will vary with different events and venues.
2. During an emergency, use all available means of communication to provide timely. Consistent, and accurate information to concerned friends/families of patrons who may be monitoring from home.	Reduce/avoid the spreading of misinformation.	Assign a Public Information Officer (PIO) who will communicate information to the media and public. Having a unified message is important to avoid confusion. Coordinate messages between agencies such as municipal public safety PIOs. Have pre-written scripts for emergency situations that can be posted to official venue and/or team social media accounts, as well as local law enforcement and responding public safety agencies.	Coordinate messages between agencies such as municipal public safety PIOs.

ACCESS CONTROL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. All open access points should be manned and only authorized, ticketed, credentialed and, if required, screened individuals should be permitted to enter the venue/event. • Make sure participants are who they say they are by requiring a photo ID during check-in. • Alert attendees about the need to show ID and visually ware badging/credential.	Establish control and maintain security.	Standard operating procedure. Consider use of red teams to test access control program.	This would include meeting rooms, conference halls, exhibit halls, centers, etc. The smaller and least risk the easier if at all vs. the larger, sensitive and higher risk events that require more controls. Check-in kiosks are convenient, but no one should receive a badge without proving they are who they say they are.
2. Develop written credential processes and policies to assist in controlling access to and within the venue for events requiring greater security.	Litigation protection. Maintain security.	Limit the number of credentials issued. Use different shapes, sizes, colors, and technology. This makes enforcement easier for staff. Consider using matching wrist bands for: • Parent and child • Senior and family member or friend **Reference the** *DHS Best Practice Guide for Credentials*	
3. Use color coded credential boards at all restricted access points to assist staff for clarity and to reduce confusion. • Post credential boards at all access control points.	Eliminate confusion of staff and those with credentials.	Assists staff and streamlines entry. To reduce counterfeiting consider using: • Two-sided printing • Unique shape/color • Use of RFID • Holograms	This is for larger events where security concerns or only paying attendees are permitted. This information can also be made available on staff smartphones.
4. Secure the following areas and post staff or use biometric reader access control devices (fingerprint, IRIS scan, facial recognition) to control access: • Mechanical/utility rooms • Classrooms • Conference halls • Stage • Storage areas • Operations Center	Prevent unauthorized access.	Assign competent and trusted staff.	For most venues, ensuring that spaces of this nature remain locked and that access to keys is controlled and documented.

5. Utilize marquees, public address systems, social media and electronic message boards to communicate to patrons entering the venue/event of the protective measures, locations, procedures, restrictions, prohibited items, evacuation routes and Hot Line number.	Avoid confusion concerning who, what is and is not permitted in to the venue. Speeds entry.	Communicate expectations reduces confusion.	

SCREENING			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY / SCALABILITY**
1. Establish a policy and refuse entry into the venue to anyone who declines to have his/her person or possessions screened/searched. • Must be posted at gates and using all available sources; should be printed on parking permits, tickets, and credentials • Train staff to be respectful of patrons and possessions • Visiting talent, personal items, vehicles and equipment trucks should be screened. This should apply to performers as well.	Safety. 100% enforcement. To be legally defensible.	Consistency in applying the rules will help and having law enforcement officers nearby is strongly recommended. Reference the *DHS Best Practice Guides for Patron Screening and Bag Searches* Reference the Check-It Video, available at www.dhs.gov/video/check-it-bag-check-video Use PA and video board messages at the doors/gates, if available. Consider assigning staff to queue lines to identify prohibited items. Consideration should be given to establishing a secondary perimeter for large events.	This is applicable when screening is required based on talent, attendee demographics, historical observation or event intelligence warrants. Sufficient and effective training is essential.

2. Establish a written policy regarding permitted and prohibited items that will or will not be allowed in venue. • Consider prohibiting: Coolers, bags, backpacks, containers, explosives, chemicals, weapons, alcohol, drugs, tools, poles, canes, selfie sticks, flammable liquids, fireworks, flares, tents, chairs, sleeping bags, blankets, glass containers and suitcases • Post a list of prohibited items at lodging and transit locations (busses and trains, parking lots and entrances to the venue), on venue website, and using all sources available	Must be written and communicated to be legally enforceable. To reduce confusion and prevent patrons from getting to the gates with prohibited items.	Communicate these policies and have participants and spectators consent to these searches as a requirement for entry and printed on tickets. Ensure that gate/screening staff are familiar with the policies and enforce them consistently. Consider clear bag policy.	
3. Develop procedures for staff in conducting proper screening techniques. Procedures should include the use and deployment of staff and equipment. There should not be any exceptions.	Legal defensibility. Must be written and communicated to be legally enforceable.	Enforce compliance with policy and or procedures. Whatever primary method is used for screening, have a secondary method available. Test screening equipment and staff performance under actual live conditions and in real-time with penetration tests.	
4. Base screening process and implementation upon local law, policy, threat/risk assessment (acceptable risk level), current intelligence, past event history, indoor or outdoor event, situational awareness of the specific event and current world climate.	Most appropriate process for the circumstances.	Screenings in some form or fashion should be conducted even if random. Increasing to higher levels of screenings can be done on an event by event basis based on current intelligence, past history, known VIP attendees, etc.	
5. Develop a procedure with law enforcement/ fire department to address handling of dangerous/ prohibited items. • Do not let patrons discard items at entry doors/gates	This will prevent confusion at the gate if an item is discovered.	Have a safe disposition plan.	

6. Post signs near all entrances clearly stating that no firearms or weapons are allowed in the facility.	Prevent firearms consistent with local/state laws.	Signs should cite applicable statutes or ordinances. Since many venues are on public property firearms laws will vary greatly from city to city and state to state. Must comply with laws.	

1. Must include some form of personal screening: visual inspections, pat downs and/or metal detectors (hand-held wands/walk-through). • May be random or mandatory 100% screening Everyone (participants, spectators, event staff, volunteers, and sponsors), needs to be screened, at least visually without exception • The most efficient is walk through metal detectors as primary, handheld wands as secondary and gender specific pat downs as the final option • Provide for multiple trained techniques and technologies as back-up systems in the event of a technical failure	To prevent prohibited/dangerous items from being brought into the venue/event.	• Visual observation is the least intrusive and the least reliable for the untrained eye and even for the trained eye • A pat down is the most intrusive and requires the most training due to sensitivity issues. It also takes the most time. If this method is employed, use all trained adults for this function. • Metal detectors (hand held or walkthrough) are very good for metallic items • The appearance of a professional and efficient screening operation is also an effective deterrent • Screenings should be conducted by venue security staff with law enforcement as a back-up, where available	Consider what is best for your situation.
2. If pat-downs are to be used, ensure extensive training is provided, to include sensitivity training. • All primary screening should be conducted by non-law enforcement security staff, backed up by law enforcement • Use only gender specific (male on male, female on female) pat-downs. • Provide private screening locations; screenings should be conducted by a gender specific security officer with a second gender specific security officer as a witness	This is the least desirable and most problematic.	Ideally, for all screening options there should be a law enforcement officer at each screening point, where available. If pat-downs are used provide monitored semi-private locations for pat-downs, when possible. If pat-downs are used provide monitored semi-private locations for pat-downs, when possible.	

3. If handheld wand metal detectors are employed, ensure staff are trained and enough devices are available to prevent long lines.	This is good but training and manpower intensive.	These are mobile and can be moved between gates. Calibrate devices and be sure to have spares.	
4. If walk-through metal detectors (magnetometers) are employed, ensure sufficient training and calibration of devices; must do further screening for all alerts.	This requires training but is less manpower intensive and less intrusive.	These are mobile and can be moved between gates; ensure calibration and review sensitivity. Ensure a sufficient amount of handheld wand metal-detectors are also available.	
5. If metal detectors are used, visually inspect items that activate the detector.	Ensures that items are not disguised as something they are not and that weapons are not introduced into the venue.	Be consistent.	
6. Develop procedures and training for whatever level(s) of screening are used. • Have male staff search male patrons and female staff search female patrons • Develop procedures and training for screening of small children and disabled patrons • Include sensitivity training • Video all screening operations	Helps avoid complaints. Litigation protection.	Texas Engineering Extension Services (TEEX) offers basic security operations training in access control, personnel, baggage and vehicle screening. Reviewing video coverage is a great tool for after-event analysis/ learning about screening process at all entry points.	
7. Train staff to heighten personal screening/searches in the event security conditions change.	Respond to elevated threat levels.	Ensure that staff responsible for checking bags is properly trained. Using DHS's *Sports Venue Bag Search Procedures Guide* and document their viewing of "Check It" bag search video. Reference the Check-It Video, available at www. dhs.gov/video/check-it-bag-check-video.	

8. If metal detectors are used, calibrate them before each use and document it.	For legal liability.	Have spare metal detectors available (i.e. hand wands or walk-through magnetometers).	
9. Set up special entry lanes at doors/gates around venue for: • Patrons with NO items to screen (express lane/gate) • Patrons with medical devices (oxygen tanks, medical syringes, wheelchairs, etc.) • Mothers with diaper bags for young children (must have child with them)	To expedite entry and reduce aggravation.	Make sure to have appropriate signage to inform patrons of the "with and without" items lanes/gates to help patrons discern the correct lane for them.	

POSSESSIONS

1. Inspect ALL possessions, items, and/or containers that are permitted into the venue. If bags/containers (of any type) are permitted, inspect at entry points (preceding ticket takers) before entry to the venue. • Use tables for bag screening and provide 12-inch-long-20-inch-long dowel rods attached to flashlights for staff to probe inside bags to speed the process • Train staff to conduct these checks and to NEVER put their hands into containers/purses/bags • Provide screeners with latex gloves • Ensure sufficient lighting at all screening areas for evening events • Document training All primary screening should be conducted by venue/event security staff and backed up by law enforcement, where possible.	To prevent prohibited items from being brought into the venue. This protects staff's hands from cuts, scratches and contaminations.	Reducing what patrons can bring into venues significantly decreases risk and expedites the entry process. Bag searches tend to be the most inconsistent. Consider using clear bags for easier examination and to expedite entry. The smaller the better-consider 12' X 6' X 12'.	Depending on your event, the venue and its security requirements will determine what is or isn't permitted and what level of screening is required.

2. Conduct a visual inspection, requiring attendees to open their possessions and, if necessary, empty the contents into a bin. Consider setting up separate lines for people who: • Require a more detailed inspection of possessions • For those entering without any possessions that require inspection • For disabled/mobility impaired or others with special needs	Streamline process to reduce time.	Consider using bins (i.e. airport TSA screening) for personal items instead of emptying contents onto a tabletop. This process is already socially acceptable, and patrons are less likely to lose/drop property. It may also speed up the screening process.	
3. Set up tables for items to be placed on for inspection depending upon what items are permitted to be brought into the venue.	Ease of observation.	Tables speed up the process and provide a stable platform to place items for inspection. Also serves as a barrier between staff and attendees.	
4. Develop procedures and training for whatever level of screening used.	Ensures consistent operation among staff members and reduces delays.	Have staff be discreet and courteous. Ensure that staff responsible for checking bags is properly trained. DHS's *Sports Venue Bag Search Procedures Guide* and "Check It" bag search video are good resources.	
5. If bag check facilities are available, ensure bags are inspected before taking custody of the items. Bag check facilities should be located as far away from the venue as reasonably possible.	Accommodation and keeping potentially dangerous items away from the masses of people.	Ensure proper staff training and inspection of checked bags.	

HANDLING OF DISCARDED POSSESSIONS

1. Develop a procedure to address abandoned items. • Don't place unattended trash receptacles at access points to venue where patrons can discard or abandon prohibited items. Staff and make sure attendees do not dispose of items near entrances	These items are often discarded around entry doors/gates/perimeter of the venue. They can become containers for IEDs.	Unless it is a weapon or illegal drug law enforcement officers do not need to be involved. Venue security staff should be responsible for these items-unless they are evidence, which law enforcement officers will handle. Create a disposal policy.	This is applicable to larger events with security concerns.

TICKETING/CREDENTIALING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
DESIGN AND IMPLEMENTATION			
1. Develop effective ticket and credentialing policies and procedures in collaboration with all stakeholders.	Controls access (i.e. patrons, talent, media, staff, VIPS) to venue and specific areas during specific times.	These will vary by event type, location, security sensitivity, cost, etc.	This is for events where you have controlled access and admission is by invitation, paid or prior registration. This also should be used when multiple events are occurring at the same venue and your event is closed.
2. Consolidate credential management under one central authority with security oversight.	Centralization will eliminate confusion and enhance enforcement.		More applicable to larger events and Event Producers.
3. Issue credentials on an event basis and have an expiration date. Venue management, event staff, etc., should have photo I.D. cards that are used as credentials.	Controls counterfeiting.	To reduce counterfeiting consider using: • Two-sided printing • Unique shape/color • Use of RFID • Holograms • Remove previous date wristbands/credentials from bags or persons who return for new event	This is particularly import for large events where due to size of staff, they don't know each other.
4. Designate credentials for specific areas (where you have different areas with different patron access) that are clear and visible.	Access control with authentic and easily identifiable credentials.	Ensure credentials are designed so that they can be visually identified for specific access/function. Retrieve credentials from individuals that no longer have a need (i.e. contractors).	
5. Do not grant non-credentialed individuals access or give credentials to non-working or unauthorized individuals.	Prevents unauthorized access and allows control.		
6. Recommend a credential system that utilizes holograms, bar codes, RFID and/or photographs to identify the bearer and indicates by shape, size and color the area(s) to which the bearer has access.	Control and visual recognition.	Can employ electronic scanners for ticket/credential validation.	For significant events with security concerns.

7. Credential design should be kept as simple as possible (shapes, sizes, colors). Display credential boards at access points to restricted areas and train staff on the use of credential boards.	Over complicated credentials requiring a complex credential board for interpretation confuses the staff.	Access control with authentic and easily identifiable credentials. Employ anti-counterfeiting techniques.	
8. Design and color of credentials must be substantially different from those used in prior events.	Prevents individuals from using credentials from previous events and prevents confusion for staff.		
9. Issue photo credentials to all persons working the event, employees/staff, talent, and volunteers, public safety, medical, approved media, etc. • All requests for credentials from the media and sponsor/vendors should be in writing • Media, sponsors and vendors should be required to pick up their credentials in person using a photo ID to verify their identification		If possible use an online credential registration capability and require a photo ID when picking up credential.	This is particularly import for large events where due to size of staff, they don't know each other.
10. Credentials should be worn at all times and clearly displayed.	Avoids confusion.	Must be enforced.	Particularly important at venues with simultaneous events.
11. Conduct testing of staff on access credential systems. • Immediately correct any deviations from policies and procedures	Control and consistency.	Measure effectiveness of policies and procedures through training, exercise and refinement.	

BACKGROUND SCREENING

1. Conduct background screening on all staff (i.e. vendors, sponsors, event staff, contractors, volunteers, etc.) prior to issuance of their credentials.	Reduces liability.	NCS4 offers a cost effective program, coupled with training to accomplish screening/training.	When the event security posture requires it, but this is a good practice for your staff regardless.

TRAINING

Best Practice	Objective	Implementation	Applicability / Scalability
1. All ticketing and door/checking personnel should be knowledgeable about tickets and credentials. • Test and monitor for compliance	Patrons become upset when personnel do not know what they are doing.	These personnel should also be familiar with the facility.	

ALCOHOL MANAGEMENT

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
SALES			
1. If the venue allows onsite alcohol sales, follow local and state laws and regulations.	Legality of sales and possession.	Will differ from state to state.	This is applicable only if alcohol is served at the event. This can produce significant legal issues if alcohol is served as part of the event.
2. All sales personnel should meet age requirements and receive training on recognizing signs of impairment (i.e. refuse service, contact supervisor, etc.).	Training and reduction in legal liability. Even if this is contracted out, past experience indicates that the event organizer will also be sued.	State Alcoholic Beverage personnel are a great resource and in most states will offer training. Consider Techniques for Effective Alcohol Management (TEAM) coalition training. Visit www.team coalition.org for additional information.	Ensure venue or catering bar is in compliance with state/local alcohol laws.
USE POLICIES/PROCEDURES			
1. Event and/or venue should create clearly written alcohol possession and use polices. • Specify that intoxication will not be tolerated and will result in ejection. Enforce the policy	Prevent public intoxication and liquor liability issues, maintain guest safety.	Policy needs to be communicated to attendees. Ensure that your policies are in compliance with state and local liquor regulations and comply with your insurance policy and permit.	Intoxication often causes other issues that result in problems.
2. Consider creating family friendly alcohol-free area(s).	Isolate drinkers from non-drinkers and minors.		This is more relevant for family entertainment events.
3. Train staff on recognizing patrons who appear to be impaired and what actions to take.	Lack of trained staff.	Have supervisors deny entry that should be enforced by law enforcement.	

POSSESSION/CONSUMPTION

1. If the venue has a no-alcohol policy and does not sell alcohol, develop a procedure for dealing with individuals that are in possession and/or consuming alcohol.	Policy enforcement.	Communication and enforcement of these policies will enhance the guest experience.	If applicable to your venue/event.
2. Implement a secured perimeter around alcohol service areas, with an exterior and interior ID check, conducted by persons trained in ID verification. Limit quantity of drinks per participant per trip to the bar. Identify underage persons and legal persons visibly.	To address violations of state laws.	Make sure law enforcement working at the venue is aware of and understands current policies and the proper response–by law for a crime committed in their presence requires action. State alcohol enforcement may assist.	Since alcohol is a major contributor of disruptive behavior this is a must when alcohol is served.

TOPICAL AREA: EMERGENCY ACTION PLANNING AND CRISIS MANAGEMENT

PLANNING			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY / SCALABILITY**
1. Develop and continually (for each event annually) revise a written Emergency Action Plan (EAP). Some also refer to this as an Emergency Operations Plan (EOP), Incident Action Plan (IAP). • Collaboration and coordination is key. Develop in conjunction with all involved parties; Public Safety agencies should be responsible for many sections and will frequently take the lead (these will be so noted). • The EAP should include specific measures to cope with and respond to all potential incidents within the event area • The EAP is a separate document from the Event Day(s) Plan but will serve as an appendix	Being able to respond effectively to any incident requires pre-planning, anticipation, coordination, and training. To reduce legal liability.	The size and complexity of the written EAP will be driven by the RTV Assessment, size and type of the event, number of attendees, history of prior events, etc. The EAP may also incorporate several smaller events with a separate section for each specific type of event as applicable. The local and state agencies (who will be responding to incidents) along with the FBI and DHS Protective Security Advisors (PSA) are a tremendous resource. Every FBI Office has a Special Events Coordinator who can be of assistance.	This should occur regardless of the size of event as you have the duty of care for patrons and staff. Larger events will require more extensive planning versus smaller events. This should be developed from your perspective, where possible in collaboration between: Event Organizer, Venue, Lodging, Transportation, Contractors and Public Safety. Many of the items will be handled by public safety, but there needs to be collaboration, coordination, and recognition of their roles and responsibilities.
2. The EAP should address all event day(s) and load in day threats, load out, and potential emergencies. • Minimize injury and loss of life • Establish effective response • Incident stabilization • Protection of property and the environment • Minimize economic impact	Must be all encompassing, as complete planning will afford for better preparation and training. Will also assist in brand protection and reduce legal liability.	GUIDES Compliance regulations, laws and recommendations for review: • Blood Borne Pathogens (OSHA) • EAP 29 CFR1910.38 • *FBI Law Enforcement Crisis Management Handbook* • Fire Prevention Plan 29 CFR 1910.39 e. First Aid 29 CFR 1910.151 • MGT-404 Sport and Special Event Incident Management • AWR-167 Sport Event Risk Management • NFPA 1600 • NIMS 100-800 • State Fire Codes • State health department codes regarding food handling and emergency medical services • Local building codes/structural regulations for temporary structures and stages ICS forms are also useful.	For international events, INTERPOL offers fact sheets and guides that may be relevant, depending on the event destinaiton: https://www.interpol.int/en/News-and-media/Publications2/Guides-manuals2

3. Specify persons to be notified and in the proper order of notification. Ensure the notification list remains current by updating annually and/or when contact changes occur.	Ensure accuracy and that the appropriate individuals get notified.	Keep hard copy and electronic copy. Coordinate with local contacts to ensure that all concerned to the best of your ability (and documented) are involved in the planning process.	It will depend upon the type of event and location and could involve: event, venue, lodging, transportation and public safety.
4. Create a plan for staffing according to the particular event and the assessed risks/threats.	Roles, responsibilities and sufficient resources.	Use this to determine who will take charge of the specific incident.	This may be organization dependent.
5. Ensure plans are protected from unauthorized disclosure.	Not all parts of the plan should be open to everyone, especially tactical plans.	Treat as law enforcement sensitive, need to know.	Not all the parts from public safety will be shared with you or your staff, only those in which you have a need to know, but you do need to know they have a plan for those components.
6. Conduct at least an annual exercise on the Plan and include updated information from previous exercises.	Staff and partner preparation.	Include all parties to test the Plan. Discuss roles and responsibilities.	If you have a reoccurring event. May pick specific components to exercise.

EXECUTIVE TEAM

1. Establish an Executive Safety and Security Committee (ESSC) comprised of leader or their designees from law enforcement (local, state and federal), fire department, medical, health service and emergency management, as well as all appropriate venue staff.	Provides organization, reduces confusion and establishes accountability while getting the most input.	This can be scaled based upon the size of the municipality, geography, history and local environment.	This is for large events with security/safety concerns, but many of these components could be relevant to your event of any size.
2. Have ESSC establish Specialized Management Coordination Components (SMCC) through the committee process.	Assigns responsibility with expertise and accountability.		This is for large events with security/safety concerns. For smaller events a single person may address all these components through coordination and collaboration.

3. Appoint a lead individual (or agency/organization, if applicable) for each SMCC to identify overall responsibility and the setup of each component. Develop a written component for the plan. The following are recommended SMCCs: **EMERGENCY PLANNING STRUCTURE** • Background Screening/Credentialing/Accreditation • Blueprints, Maps, Diagrams, CAD/BIM, GIS • Command and Control • Communications • EOD/WMD/CBRN/Bomb Dogs • Intelligence/Investigations • Jurisdictional Roles and Responsibilities • NIMS/ICS • Public Information/Media Relations • Rapid Investigative Response/Tactical Response • Traffic Control • Transpiration • Lodging • Unified Joint Operations Center • Dignitary Protection • Emergency Management • Parking/Tailgating Areas **INCIDENT RESPONSE PLANS** • Active Shooter • Adverse Weather • Aviation Accident/Incident • Bomb Threat/Suspicious Package/Bombing • Cyber Intrusion/Attack • Demonstrations/Civil Disturbance/Riots • Earthquake (if applicable) • EMS/Medical • Evacuation/Sheltering/Reunification • Fatality(s) • Fire and Rescue • Hazardous Materials Release • Infrastructure Failure • Marine (if applicable) • Mass Casualty • Public Transportation Incidents • Structural Collapse • Terrorism • Weapons of Mass Destruction • Vehicle used as a Weapon	Comprehensive planning. Structure, planning, command and control. All-hazard planning.	The same individual will probably be responsible for any like components between Emergency Planning Structure and Incident Response Plans. These should be lead and developed by Public Safety personnel (law enforcement, fire department, EMS and emergency management) and key individuals from the venue/event.	These are typical areas. While all may not apply to every event, most would to some degree, depending on event size and security/safety concerns.

EMERGENCY RESPONCE OBJECTIVES, MISSIONS AND RESPONSIBILITIES

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. The EAP serves as a guide/plan-providing direction, information, management, coordination, roles and responsibilities.	This provides an organized structure and response procedures should an emergency/critical incident occur.	Should be consistent with NIMS/ICS. Also for use in contractual documents with event service providers.	The EAP should reflect the size and scope of the particular event and scaled accordingly.
2. Provide response procedures to protect people and property during and after an incident.	Reduce event/venue liability.		
3. Provide a structure for coordination between event/venue/transportation personnel and government authorities to promote an effective response and resolution.	Cooperation and collaboration.	This will also serve as a guide for exercises.	

COMMAND AND CONTROL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Designate leaders to exercise authority and provide direction within the chain of command by identifying specific responsibilities.	One of the most important principles of effective inter-organizational success is unity of effort with clear lines of command and control. A pre-defined chain of command is important during crisis situations.	Leadership is a VERY important component as is coordination and team effort. For active venues, conduct monthly review sessions with leadership team to address any questions or concerns.	The appropriate individual should be designated as the Incident Commander (IC) for each type of incident. See NIMS/ICS Identify the Incident Commander for any type of incident. Generally, it is an agency/organization head or designee (i.e. Police Chief, Fire Chief, etc.), or the senior member of the venue/lodging or transportation security team.

JURISDICTIONAL ROLES AND RESPONSIBILITIES

1. Hold pre-event meetings with decision makers to sort out and understand jurisdictional roles and responsibilities of the various public agencies and the venue/lodging management team decision makers. These should be documented.	Clear lines of roles and responsibilities. Eliminates confusion during an incident.	This should occur regardless of venue size. At least annually, have major planning meetings with all parties to address/modify the plans to meet the needs of the venue/event.	Again this is event dependent, size and security/safety concerns will dictate.

COMMUNICATIONS

1. Develop an Operations/Communications Plan that includes options and alternative methods to communicate at all levels from the Operations Center to the venue and public safety operations.	Communication is extremely important. Pre-planning and redundancy are essential. Interagency communications is essential during a crisis and should be a high priority.		This is clearly scalable based on the event, environment and potential incident.
2. Plan for multiple communication platforms with sufficient redundancy to get timely and accurate information to those who need it when they need it.	Redundancy.	Consider public safety communication capabilities, public and commercial radios, landlines, cellular, HAM radios, video boards, broadcast media, social media, text and PA systems.	
3. Test Communications Plan/equipment in a working environment to ensure the equipment is working properly before the event. • Install signal enhancement (repeaters) to ensure venue-wide coverage as necessary for all communications (radio, cellular, data)	Reliability of communication capability overall and in a high-noise environment.	This should be performed prior to EACH event.	

4. Do not rely upon any single method/system of communicating for operational or emergency communications. • With technology advances, don't forget the old reliable capabilities that have proven tried and true, such as Ham radios and their operators • Also, maintain landline phone capability	Technology dependency and reliability.	Always have a back-up even if it is dispatching a person to relay information. For large scale events consider bringing in cellular providers to beef up the existing cellular infrastructure in the area of the venue/lodging to accommodate large crowd use of cellular resources. Request priority routing for public safety. Event organizers should consider the Government Emergency Telecommunications Service (GETS) and/or Wireless Priority Service (WPS) program offered through the federal government to get priority phone service during an emergency.	Radios and smartphones are the most used for redundancy.
5. Have megaphones as a backup for crowd control and emergency communications. • Also use first responder equipment PAs for emergency communications	Be prepared for the unexpected.	Pre-stage megaphones at ingress and egress points around the venue.	This is the most prevalent tool used.
6. Develop audio and video scripts for all types of incidents with specific emergency announcement broadcasts. • New megaphones allow for pre-recording of various incident scripts	Avoids confusion during an incident.	Consider all forms of media. Scripts should be preprogrammed in to the devices to save critical time.	
7. Written instructions should be in place to address incoming threats, whether telephonic or via any other medium. All incoming threats should be properly recorded and preserved.	Essential to initiate an investigation and emergency response. Provides documentation for analysis, investigations, lessons learned and in the event of litigation.		For all events.

8. Establish process to get information on reported threats directed at adjacent facilities (buildings, train or subway stations, businesses, fuel storage, factories, etc.) to the Operations Center. • Specify persons to be notified and the order of notification • Broadest POSSIBLE dissemination should be made to the Unified Command • Review and test before each event to ensure contact numbers are correct	Situational awareness. Eliminate surprises. Avoid confusion.	Primarily handled by Public Safety with venue operations contributions. Environmental surroundings, including adjacent facilities and nearby critical infrastructure, have the potential to impact the venue, participants and spectators so it is imperative to have awareness and monitor these areas. Keep staff informed. Ensure that the notification list remains current by updating for every event.	

PUBLIC INFORMATION/MEDIA RELATIONS

1. Designate and authorize the Public Information Officer (PIO) to respond to the media and general public in the event of an incident so as to establish a single authorized, authoritative voice.
• For large events consider establishing a Joint Information Center (JIC) to:
  • Coordinate messaging among Event Operations and all jurisdictions
  • Share news releases, questions and situational awareness
  • Share information and breaking news with media and the public through news releases, interviews and social media
  • Coordinate social media messaging
  • Speak with a single voice and avoid confusion
	Deciding who will handle media/information reduces what will be a very chaotic environment during an incident/crisis.	Try to use the most experienced individual, regardless of agency/organization who will be available on-site during the event who can speak authoritatively.
		
		This may require a collaborative effort since different organizations may have different rules and goals; consider a two-person team approach (one public and one private).
		
		The incident may dictate who will handle primary media contact or take the lead.
			This is dependent on both event and incident size.

2. Develop policies and procedures to advise the media and general public of the situation to defuse rumors and panic. • Set up a media briefing area away from the Command Center and crisis area to deliver media briefings	Avoid confusion and the appearance of un-informed chaotic reporting.	This should be a team effort. May already be addressed in venue/agency's larger Information Management Plan. Keep media briefing away from the Command Center and crisis area to avoid congestion and prevent media from accidentally getting access to something or someone they should not.	
3. Develop a procedure for reuniting family members in the event of an incident and communicating this information.	Easy family re-unification. Reduce patron and family stress.		

EMERGENCY MANAGEMENT (EM)

1. Emergency Management is the planning to reduce vulnerabilities to develop resiliency to cope with disasters. It does not avert or eliminate threats; instead it focuses on creating plans to decrease the impact of an incident. Failure to create a plan could lead to deaths, damaged assets and lost revenue. • Some large venues today have their own Emergency Management Director	Prevention and preparation.	All states, counties, and major cities have EM units that support events with FEMA resources. In some states the state DHS fills this role.	This can be a great resource for you, if you are planning a large event.

VIP/DIGNITARY PROTECTION

1. VIPs/dignitaries require coordination between law enforcement and event operations due to their celebrity status and possible protective detail (often armed). This includes protection, escort and transportation. • Must ensure that event/venue security personnel and law enforcement know who is armed	Pre-plan as a possible disruption.	If this is a requirement for the event, designate a coordinator. If any pre-broadcast of VIP attendance, this may require extra precautions should be taken, based upon an intelligence assessment. Traffic escorts can also be problematic. Sometimes these VIPs are targets of protestors.	Regardless of event size.

OPERATIONS CENTER

1. Each venue or event should have a designated Operations Center that serves as the control center for the event.
- The Operations Center will coordinate information and resource deployment among event operations, local, regional, state and federal partners.
- Goals:
  - Common operating picture, provide timely and accurate situational awareness for emergency operations
  - Platform for effective multi-jurisdictional decision making
  - Coordination between Public Safety and venue operations
  - Provide timely and effective incident response and necessary resources
  - Coordinate intelligence and investigations
  - Coordinate facility issues
  - Coordinate recovery

Particularly important to centralize communications when lacking interagency communications. Easier to keep everyone informed and on the same page.

Reduces time to react and respond. Allows for easier and better coordinated conferencing.

Allows for centralized resource management and consistent communications.

Make-up of the Operations Center depends on the scope of the events and the number of different jurisdictions.

Depending upon the event/venue this could be a small work room with a phone or a larger room with monitors, radios, computers, etc. that is scalable based upon your event.

It should serve as your hub of control, information fusion and decision making.

Multi-venue events can utilize one central connected operations center with dispatch centers located at larger satellite venues.

BLUEPRINTS, MAPS, DIAGRAMS, CAD, GIS

1. Venue Blueprints/Computer Aided Drawing (CAD) of buildings/facilities, aerial maps, utilities, photographs and diagrams for planning, implementation strategies, and response should be located in or immediately accessible in the Operations Center.
Location directory/maps of:
- All ingress and egress points
- Electrical boxes and transformers
- Emergency shelter areas
- Emergency vehicle staging areas
- Evacuation assembly points
- Hazardous material storage
- Life safety equipment (first aid, AEDs, fire control panel, fire alarm manual pull stations)
- Rail lines
- Transportation hubs
- Utilities locations (and shut-offs)

It is too late to try and collect/find these items during a crisis and it could mean the difference between life and death.

There are various Crisis Management Systems on the market that contain modules to enter/maintain/recall these for use and transmission to public safety units.

If digital they can be projected on screens and sent to smartphones.

Secure a copy of emergency contact information and critical documents (digital or hard copy) at offsite Command Center/EOC.

At least your venue contact should have ready access to this.

2. Everything should be logged and documented.	Litigation protection.	Conduct after-action review for lessons learned and modify plan accordingly.	This is important for legal purposes and future planning.

TRAFFIC CONTROL AND PARKING

1. Develop a detailed plan for vehicular flow into and out of the venue property, and around the event area. The staging and entry/exit of responding emergency vehicles should be included.	Impact on local community.	This requires close collaboration with local, county, and/or state law enforcement and t traffic planners from Department of Transportation (DOT). Coordinate with vendor(s) who manage parking and traffic operations.	This important for larger events. When applicable, make sure that local first responders have logged the entry as a geo-fixed for ingress/egress routes for dispatch. Routing of emergency vehicles should be done in conjunction with local responding agencies working to avoid heavy pedestrian crowd flow and being mindful of the access to area facilities.
2. Manage the patron ingress and egress of vehicles to the venue property, including vendors.	Traffic/parking is one of the top issues with patrons.	Particular attention to this helps with patron satisfaction, as traffic and parking issues are frustrating to patrons. Effective planning and deployment can serve to mitigate this.	

EOD/WMD/CBRN/BOMB DOGS

1. The use and deployment of bomb dogs requires experts. The SMEs must be consulted for the event and develop a plan for dealing with and responding to incidents involving: • Bomb threats • Bomb/explosives search/ screening • Bombing/explosion • Suspicious packages/items –render safe • WMD (chemical, biological, radiological, nuclear)	Anticipate and plan for response.	Major cities/counties in the U.S. have these SMEs on staff; others rely upon the FBI, BATF, and the military for support. Establish a Threat Assessment Team to evaluate and advise on these type incidents; FBI will assist. Form a relationship with local/state canine assets. Allow them to train at the venue so that they can become familiar with the venue layout and the operation.	For large high-profile events or those with high risk.

INCIDENT RESPONSE PLANS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. The EAP needs to include response modules/plans for dealing with each area below, designating the onsite/response Incident Commander for each.	Pre-planned response capability.	Time is critical if an incident occurs; having a plan in place reduces time to respond.	This will be scaled based upon the threat and size of the event. While overall responsibility for coordination will rest with the event producer, incident response will rest with the appropriate public safety agency.
FIRE AND RESCUE			
1. Plans should address the fire response at the venue. Consider staging staff and equipment. Staff should understand the various incident plans and be familiar with the venue.	Pre-planned response capability.	Need to know the location of water supply hook-ups and utility shut-offs.	This will be scaled based upon the threat and size of the event.
EMS/MEDICAL			
1. Due to the nature of the event, and patron demographics, additional medical resources may be required on site. Consider staging staff and equipment. Staff should understand the various incident plans and be familiar with the venue.	Pre-planned response capability.	Prepositioned supplies and equipment can expedite care. Check to see if the venue has AEDs in public areas. Some hotels/venues do not due to corporate policy, so you may need to bring your own.	This will be scaled based upon the threat, demographic and size of the event.
TERRORISM			
1. Be alert for and coordinate for both preventive measures and response capabilities in anticipation of a terrorist attack. Adopt the DHS "See Something, Say Something" program or similar programs that engage event staff, patrons, talent and the public	Pre-planned response capability. Court decisions have held that terrorism is a foreseeable act. Advertise Hot Line number, text or other social media platforms to report information.	The FBI can assist in planning for terrorism and can provide intelligence of potential threats to the venue/event. The threat environment is evolving, and new threats of terrorism are being used by organized groups as well as lone wolves or violent extremists. Mass gathering events have become a recent target.	This will be scaled based upon the threat, nature and size of the event.

ADVERSE WEATHER

1. The Severe Weather Plan should provide guidance, establish procedures and assign responsibilities in severe weather situations which should include evacuation/shelter-in-place/relocation.
 	
• Plan should consider the following:
  • Lightning
  • High wind to include a tornado
  • Heavy rain/hail or flooding
  • Snow or sleet
  • Heat stress
  • Severe cold or hypothermia
• Review during briefings as applicable to the event
• Practice and test staff for evacuation/shelter-in-place/relocation plans at least twice during a season (year)
• Test communications systems
• Develop triggers for postponing, suspending and cancelling events so everyone knows the criteria
	Severe thunderstorms, hail, high wind, tornados, lightning, flooding snow, ice storms, extreme heat or cold and other adverse weather conditions can endanger life, destroy property and hinder operations.
	
	Minimizing injuries and property damage are top priorities.
		Establish liaison with the National Weather Service, as they can assist in plan development.	This is regardless of event size, with a greater concentration for outdoor events.
			
			Assess potential inclement weather threats based on geographic area and timeframe of the event.

2. When a severe weather warning, tornado watch or warning or flood warning is issued, then evacuation/shelter-in-place/relocation plan should be implemented, as appropriate. • Monitor weather closely for the two weeks before the event. If heavy snow and extremely cold or hot weather is predicted, activate the Severe Weather Plan and consider cancellation	Protect life and property.	This will require extensive communications capabilities.	
3. The planning for evacuation/shelter-in-place/relocation should be discussed. Identify the individual who will make the decision with partner(s) input.	Clarity.	Identify by name.	

4. Plan for temperature extremes of hot and cold; include medical response component.		EMS can assist with planning.	
5. Heat Stress • For heat stress, add fluid stations as replenishment needs will increase • Make available an increase of ice to medical stations • As a precaution, have additional ambulances standing by • Identify areas where attendees can find relief from heat (such as air-conditioned buses). Consider using cooling stations such as AC tents/vehicles	Prevention/protection.		
6. Severe Cold, Hypothermia • Start communicating prior to the event the necessity to bring warm clothing • Identify areas where attendees can find relief from cold (such as buses)	Prevention/protection.		

INFRASTRUCTURE FAILURE

1. Assess necessary event infrastructure and ensure proper contacts for each are documented and accessible. Based on the event needs, some examples are: • Regional Airport Management • Transportation Department • Electrical Provider(s) • Natural Gas Provider(s) • Water/wastewater utility provider Venue telecommunications provider	Reduce response/recovery time.	Coordinate planning with community and venue management team.	Review history of these type issues in the area.

WATER/SEWER MAIN BREAK

1. Plan to have personnel from the water company on-call to respond as necessary. • Have a mitigation, response and recovery plan in place	Prevention/protection.	Coordinate planning with community and venue management team.	

GAS LEAK

1. Plan to have personnel from the gas company on-call to respond as necessary. • Have a mitigation, response and recovery plan in place	Prevention/protection.	Coordinate planning with company and venue management team. Also coordinate with fire department.	

ELECTRICAL POWER FAILURE

1. Develop and exercise a plan to deal with the complications from partial or total loss of power. Have a mitigation, response and recovery plan in place.	Prevention/protection.	Electricians should work all events. Coordinate planning with company and venue management team. Outages are often associated with adverse weather.	
2. Venues should have generators/backup power to support life safety, critical communications and emergency lighting. • Develop scripts for power outages that are broadcast via PA, video boards, and social media • Cellular communications should have some backup capability for emergency communication • Establish emergency contacts with local power utility company for coordination and rapid response if necessary	Response/protection.	Secured critical venue IT should be included in emergency standby systems powered by backup electricity.	

ACTIVE SHOOTER

1. Develop and exercise a venue/event plan with local law enforcement to deal with an active shooter during an event. • Observation and surveillance (a combination of human and video) in and around the venue is essential • Have response teams pre-positioned at designated locations	Preparedness.	FBI and DHS offer programs to assist in developing plans. Intelligence is important. Collaborate with all the first responder agencies in the area who would respond to avoid confusion.	

AVIATION INCIDENT

1. Plan should address an aviation accident, attack or nuisance to include UAV/UASs that fly in or near the venue. • Establish policies and develop plans to deal with UAV/UASs both curiosity and adversarial	Crashes or attacks.	The FBI and the NTSB will always be in charge of the impact scene. • FBI: Scene and evidence collection • NTSB: Incident cause Coordinate with local law enforcement. With regard to UAV/UASs, review local statues to deal with banning their use/presence. If statutes are not enforced, work with local governing agency to develop policies.	
2. Plan should include liaison and contact information with the Federal Aviation Administration (FAA).			Particularly for outdoor events.

CYBER INTRUSION/ATTACK

1. Develop and implement a security plan for computer and information systems hardware and software used for the event and coordinate the same with the venue and lodging. Include defined cybersecurity requirements for any hardware or software procured and installed for use at and by the management group/venue/event or other locations with critical links to the venues. • Establish requirements for information access • Reset passwords on a regular basis • Immediately cancel access for terminated, employees, staff, etc. • Implement data loss prevention programs • Backup data daily (weekly at a minimum) to prevent loss or lockout	Protect systems that have operations and control over various aspects of the event/venue. Protect PII, PCI and HIPA information to reduce liability and fines. Ensure timely access to IT personnel in the Emergency Operations Center, including on-call schedule for response staff.	Many components of today's venues are operated via cyber programs that control the components (i.e. HVAC, lighting, PA, video boards, etc.). This should also include public safety systems.	This is for all size events.

2. Develop an Incident Response Plan to deal with an intrusion/attack/loss of data/ransomware. • Implement a forensic analysis following a cyber-attack that results in the theft of information, unauthorized access to systems or disruption/destruction of systems	Reduces impact. Comply with reporting requirements.	Immediately notify the FBI. Have an IT specialist on site.	For non-U.S. events, contact the relevant legal enforcement agency.
3. Safeguard personal devices that connect to event/venue systems. Do so only under clearly defined and secured processes.	Prevention/protection.	This includes staff that connect via personal devices to the systems.	
4. Keep an accurate and current inventory of all venue-owned IT devices and users.	Prevention/protection.		
5. Define security requirements for third-party vendors or other non-event/venue personnel who will be granted access to IT systems.	Prevention/protection.		
6. Provide training on information security policies, procedures, responsibilities and incident reporting to all employees that use or have access to the event/venue's information technology systems. • Document training, content and attendees			

MARITIME (IF APPLICABLE)

1. If venue is accessible by navigable waters, then marine patrol and life safety response capabilities should be considered to address criminal/terrorist incidents, accidents or "boat-gating."	Boats of various sizes can be used to deliver attacks. Drinking and boating can/will present issues.	Coast Guard, marine law enforcement and state wildlife agency can provide assistance.	Applicable only in marine environments.

DEMONSTRATIONS/CIVIL DISTURBANCE/RIOTING

1. The Crowd Management Plan should include the response by venue security and local law enforcement to address demonstrations, civil disturbances and rioting. • Ensure sufficient resources are available	Considering radical protests/demonstrations, competitor rivalries, alcohol consumption and celebratory rioting at or near venues. The potential exists for an isolated incident(s) to evolve into a major civil disturbance with personal and property damage.	Pre-planning is important to prevent an incident from getting out of control. Intelligence and advance information are essential to include social media monitoring. Know your clientele.	This is a growing issue that can be size irrelevant.

STRUCTURAL COLLAPSE

1. Venue should identify and determine availability as well as the response time of internal or external resources (staff and equipment) when addressing a structural collapse.	To address structural collapse (includes temporary seating/bleachers).	The public safety response will usually be handled by the Fire Department. The cause of the collapse could be accidental or intentional. Also, consider that it may be a crime scene and a mass causality incident.	

MASS CASUALTY

1. Event producer should coordinate with venue/local authorities to develop a plan that addresses specific needs for mass casualties/fatalities. • Onsite staff need to be very knowledgeable of the mass casualty plan since many medical resources will be off-site and will need time to respond	To address mass casualty incidents.	All cities/counties in the U.S. are required to have Mass Casualty/ Disaster Plans therefore, the EAP should contain these Plans as an Annex. The city/county EMS Mass Casualty/Disaster Plan should be used as a template to facilitate preparedness and response planning for the venue. Plan should include onsite morgue capability.	
2. The plan should consider the consequences of damage to public utilities at the venue as well as disruption of public transportation.			

EARTHQUAKE (IF APPLICABLE)

1. Develop with venue an Evacuation/Shelter-in-Place/Relocation Plan for the venue that sets forth the who, what, when, where and how. • Develop with input from public safety partners and event staff • Review with Incident Command staff at public safety briefings • Prepare for all-hazards • Include a Traffic Management Plan for evacuation should it be required • Should identify shelter-in-place in and around the venue	Life safety is first and foremost during evacuation/shelter-in-place/relocation Plan provides instructions and guidance on effectively addressing the safety of all individuals in attendance.	The Evacuation/Shelter-in-Place/Relocation Plan is an essential element of the EAP. **Training Resources:** NCS4 offers grant funded training through DHS/FEMA for plan development and execution: • MGT-412: Sport and Special Event Evacuation Training and Exercise	Applicable if in earthquake prone area. Event/venues in these areas should have a plan in place, then you only need to familiarize you staff with the plan.
2. Define all the potential hazards and scenarios that an earthquake could cause a partial or full evacuation or sheltering. • Identify the individual who will make the decision to relocate along with how it will be communicated		Evacuation planning should be based on a risk assessment that takes time, distance, density within given spaces and size of group(s) into account. During events ensure egress points are unlocked and have personnel posted to direct people in an evacuation or sheltering movement.	
3. Evaluate every potential location for shelter-in-place against all possible types of incidents to determine their ability to offer sufficient protection, along with the total number of individuals each area can safely accommodate. This can be further complicated by an earthquake damaging potential shelters.		Making the decision to evacuate, shelter-in-place or relocate during an incident is a complicated process and requires input from various entities knowledgeable in the surroundings and structures, the size, distribution and condition of the patrons, staff, the hazard involved and the anticipated response to that hazard. The length of time for sheltering-in-place will be a factor and must be considered – the longer the time the more individual space required.	Movement to open outdoor areas may be the best course of action.

4. The routes of travel need to be determined for full or partial evacuation, sheltering-in-place and relocation event. This will be complicated by an earthquake.		These all should be included in Plan(s). Consider "what if" scenarios as they relate to closing various exits and rerouting. This is where simulation can be useful.	
5. Event staff must be posted to control and expedite the movement of people during an evacuation, shelter-in-place and relocation. • Also, to reroute individuals if something changes		Staff have to be ready to direct patrons from their location to the next staff member or to the exit.	
6. Voluntary vs. Mandatory • Time, conditions, circumstances, number of people and the incident will dictate whether the action is voluntary or mandatory. • Anticipate that an incident could occur that would cause panic resulting in a stampede mass evacuation; consider how to respond.	Anticipate different potential precipitators and outcomes. Unanticipated incident.	This is clearly the most dangerous of situations. Plan response of how to use the crowd flow, based on the environment (lighting) and methods of communication.	This will potentially be a panic situation.

HAZARDOUS MATERIALS

1. Venue/lodging should have a plan for dealing with hazardous materials (i.e. fuels, propane, chemicals, fertilizers, garbage and sewage).	The expose to hazardous materials could cause a mass casualty event.	The local fire department and emergency management services are great resources.	
2. Material Safety Data Sheet (MSDS) must be available for all hazardous materials in the venue. Include contact information for assistance and maintain copies in the Operation Center.	Knowing where to get the information is important. Avoid delays during a crisis.	If highly hazardous materials are present, have a hazardous materials specialist (usually a fire fighter) on site for large events. MSDS are available in digital or hard copy format.	
3. Include procedures and security for fireworks and other pyrotechnics, if used during the event.	Potential for fire or explosion.	Must have a fire unit on site. Provide security for the pyro upon delivery until deployed.	

BOMB THREAT/SUSPICIOUS PACKAGE/DETONATION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
PLAN/POLICY/PROCEDURES			
1. In conjunction with the venue/lodging, have a written plan that is part of the EAP that dictates the criteria, roles/responsibilities and identifies the individual who decides on an evacuation.	Prevention/protection.	FBI, DHS and BATF can assist in developing plans.	Regardless of event size.
2. Make use of the Unified Command for assessment, decision process and response.		Establish a Threat Evaluation Team. The FBI can assist.	
RECORDS AND RETENTION			
1. Ensure that all incoming threats, whether telephonic or via other media, are properly recorded and preserved for at least two calendar years following the year in which the threat was received.		Local/state laws determine control retention times. Check with legal counsel to determine length of time for retention of recorded documentation for the venue.	
THREAT CHECKLIST			
1. Use Bomb Threat Caller Checklist and train staff who may receive calls/texts. • Install caller identification and/or coordinate phone call trap capability • Call may be via Voice Over Internet Protocol (VOIP) • Threat may come from social media		FBI, BATF and DHS can provide this.	Once a threat is made you should always contact law enforcement and report the threat.
THREAT ASSESSMENT			
1. Create a Threat Evaluation Team that can be called upon when threat(s) received.			

PRE-EVENT SWEEPS

1. Create a program that requires employees to check their own work areas (white-level search) daily for anything out of the ordinary.		White-level search is an inspection by all staff of their respective workplaces for any articles that are unusual, suspicious or unable to be accounted for.	For events with security concerns based upon Risk Assessment.
2. Establish pre-event sweeps ideally a few hours before the event and keep controlled (lockdown) until door opening.		Set a timeframe ahead of event for pre-scans/sweeps-this will be dependent upon the size of the venue, the threat intelligence and manpower/dogs/equipment. Once sweep is complete, areas must be locked down. Venue should be sterile and can only remain that way if access is controlled.	For events with security concerns based upon Risk Assessment.

HANDLING OF SUSPICIOUS AND/OR UNATTENDED-ABANDONED ITEMS

1. Prepare a document on "How to Recognize and Handle a Suspicious Package or Envelope" and train staff.
• All letters, envelopes and packages should be handled in accordance with instructions set forth in the above document
• The plan should include the following:
  • Attempt to identify the owner by asking individuals located in proximity to the item
  • If the owner of the item is identified, return to assigned duties
  • If the owner cannot be located, remember the acronym **HOT** to evaluate need for further action:
    • **H** – Does the item appear to have been hidden?
    • **O** – Is the item overtly suspicious (wires, phones, etc.)?
    • **T** – Is the item typical for the area /type of event?
    • Inform Command Center/law enforcement officer or call 911 if it is threat
		Follow USPS, DHS, FBI or BATF suspicious mail and package best practices when preparing "How To" document.
		
		Venues will rely on public safety personnel to respond and handle this. Review OSHA requirements.	

Best Practice	Objective	Implementation	Applicability / Scalability
2. Consider processing mail off site, if possible. • Any facility used for mail processing should have independent HVAC systems and alarms or monitoring systems that preferably have current or pending SAFETY Act approval			
3. Ensure that all staff are trained on recognizing suspicious items and proper handling (protect the area and notify Operation Center).	Training and testing.		

PUBLIC TRANSPORTATION INCIDENTS

Best Practice	Objective	Implementation	Applicability / Scalability
1. Develop a plan to address incidents that could occur with the various modes of transportation (bus, train, subway, ferry, rideshare, etc.) that are used in close proximity to the venue. Develop contingency plans for each transportation mode	Planned response.	For larger events consider having a representative(s) in the command center. For smaller events ensure contact numbers are available in case of an emergency.	

WEAPONS OF MASS DESTRUCTION (WMD)

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR

Best Practice	Objective	Implementation	Applicability / Scalability
1. Develop a plan to address the response by the venue management team and external resources in the event of a WMD incident.	Preparation for a worst-case scenario.	WMD incidents by their very nature are mass casualty and criminal or terrorist acts and therefore are crime scenes. FBI will take control. Also, because of the magnitude of these types of incidents, a major public safety/emergency management response will be necessary. FBI and state emergency management should assist in planning.	For large events with security concerns based upon RTV Assessment. WMD weapons are classified as Chemical, Biological, Radiological and Nuclear (CBRNE).

2. Integrate Plan with the larger public safety/ emergency management response plan.	Determine plan from time of incident until help arrives.	For rural or smaller communities, it may take longer for specialty units to arrive.	

FATALITY/DEATH

1. Develop a plan to deal with onsite fatalities: • Natural Causes • Accidental • Criminal It is important to identify who will take the lead in the event of a fatality at the event. Determine when cancellation should be a consideration. Location will be a factor. Determine who will deliver the message.	Manage brand reputation and ensure information is communicated sensitively and appropriately.	If the fatality is the result of criminal activity, event cancelation may be required as it could be considered a crime scene and thus impact the event.	You may not be able to move the body until a medical examiner releases it, thus possible event cancellation.

AFTER-ACTION REVIEWS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. An After-Action Review (AAR) is an important component of the continued security and safety process.	"Lessons learned" are important to continuous improvement.	Essential to the process for improvement.	Applicable to all size events. Large events, large AAR; smaller events, smaller AAR.

2. Conduct review after every event. • WHEN-conduct the review as soon as possible after the event, optimally within 48 hours • WHERE-any comfortable, quiet location that can accommodate all key personnel around a table • HOW-using the Specialized Management Coordination Components (SMCCs) as a format for the review - obviously the primary input is verbal, but the total review should include written reports, arrest reports, complaints, etc. • WHO-key personnel who were in event management roles and those who headed up the SMCCs (If you used SMCCs) • WHAT-a written AAR draft report should be prepared with an analysis of the information obtained. The AAR should be provided to all meeting participants to review for completeness, accuracy, and to provide additional feedback.	It is advantageous to capture the info while it is still fresh in everyone's mind. This creates a relaxed environment. These are natural segments. Collect input from key personnel and those under them to gather input from all staff levels.	Appoint a scribe to capture and document the information.	
3. After the review is completed, the final AAR should be provided to the participating components with a list of recommendations.	Document process and lessons learned.	Review what was done right and what needs improvement.	
4. Incorporate results of the AAR back into the planning cycle (i.e. what to keep, what to change, how and why changes should be made).	True value of the process.		

TOPICAL AREA: BUSINESS CONTINUITY, RESILIENCE AND RECOVERY

BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR)

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Venue/event should prepare a BC/DR Plan for each venue/event. • Anticipate events that could cause the potential for evacuation/shelter-in-place/relocation at the venue	These should be addressed in Risk/Threat Assessment Plan.	Consider using local DHS Protective Security Advisor and Infrastructure Protection Program to assist. FEMA can also provide resources.	This is more venue-oriented because of the actual facility, but the impact of a disaster will also impact the event and future events.
2. Identify security and safety needs for continuation, cancellation, resiliency and recovery.		Would also be part of a mitigation strategy.	Business sustainability is the key.
3. Mobilize event/venue staff, as a "care team" for emergency response, with method to notify and activate them.	Best utilization of resources for immediate response and recovery.	Company sponsored insurance carrier may be a resource for emergency planning and notifications.	

RECRUITMENT AND RETENTION OF PERSONNEL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
STAFF POSITIONS			

1. Personnel (full-time employees, event staff, volunteers, etc.) that are properly screened (background checks), trained, equipped and motivated are the keys to a successful event safety and security program. What needs to be done before recruiting/selecting/hiring employees and event staff?
• Determine staffing requirements (supervisory vs. workers)
• Develop organizational/personnel structure
  • Define roles and responsibilities
  • Determine span of control (i.e. 1 supervisor for every 8 staff)
• Identify special skills (certifications)
  • EMT
  • Communication
  • Fluent in other languages
  • First Responders
  • Computer skills
  • Riggers
  • Equipment operators
	The proper, hiring, training and staffing of the venue and event is extremely important.
	
	Because all employees will have some effect on safety or security, whether that is their main function/role or not.
		Most of these practices are applicable to both employees and volunteers. Individuals with customer service skills are a plus. Consider recruiting law enforcement, military, fire and Department of Corrections applicants for security/safety positions.	This must be done but is scalable based upon venue/event size. The threat, intelligence and history can be determined by a risk/theft/vulnerability assessment.
			
			This is requires collaboration, as many of the workers/personnel are employed by the venue, hotel or transportation company.
			
			So each component should follow this from their perspective.

2. Maintain an adequately sized, equipped and trained safety/security force based upon venue/event and risk assessment.	Sufficient personnel to adequately address safety and security.		This will depend upon RTV Assessment.

3. Create staff Performance Management Plans, as they are a valuable tool for staff development that would: • Clearly communicate goals, objectives and expectations • Allow staff to perform self-evaluations • Utilize a spreadsheet for event comments on staff and incorporate into annual/season plans • Identify individual short and long-term goals • Utilize strong skills and develop weaker skills	Continual evaluation and improvement.	Each component should have this.	Many venues and lodging have these plans for employees.
4. Document exercises, indicating the scope and duration, names of personnel who participated, actions for improvement and recommendations for plan modifications.	Liability protection.		This helps multiple components work together to address any potential incident. Many venues hold these exercises.
5. Find creative ways to establish a cadre of safety and security personnel. • Develop a cadre of staff that can handle all events • Reward positive behavior	Addresses high turnover. Easier to train and maintain. Much more cost effective from a training/consistency standpoint.	Contracting is one possibility. Select, train, test, deploy. Since money/pay is not always a big factor for recruiting and retention keep it interesting and exciting by finding ways to offer staff opportunities/ rewards.	This is generally for larger events, but is also applicable to smaller events with security concerns.

6. If using volunteers, establish a Volunteer Director to actively manage volunteers.
• Make sure there are clear roles and responsibilities as well as:
  • Number of volunteers in any area will determine amount of supervision/ span of control (1 to 8 is optimal)
  • Plan for attrition/no shows (example, 15%), continue to monitor performance and adjust
  • Establish volunteer communications–both directions
  • Create a volunteer application process–selection is important
  • Survey volunteers for special skills
  • Languages, EMT/CPR certifications, volunteer event experience
  • Seek law enforcement/ military/first responder experience
• The language that is used in volunteer job descriptions or application process must be appropriate
  • Try to not have volunteers do the same job as paid employees
• Create a Safety and Security Volunteer Handbook - keep it as brief as possible and include pictures (short and simple)
  • People can lose interest and feel overwhelmed if there is too much information
  • Update this after each season if necessary
	Volunteers are not an option for all venues.
	
	Coordination and management of volunteer staff.
	
	This can create labor problems.
		Volunteers can be a huge force multiplier if effectively trained, managed, nurtured and inspired. They can also be the source of major headaches if not.
		
		If using volunteers, the Volunteer Director is an important position, so hire carefully.
		
		Do not look for people just to fill openings, look for a cadre upon which to build a team.
		
		This could be a collaborative effort with the industry between: event, venue, lodging and transportation.
			Applicable to events using volunteers.

TRAINING OF PERSONNEL

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Create relevant training programs that are required for all personnel. • Establish a Mentoring Program for on-the-job training of new or replacement personnel	Training of staff is extremely important. Testing is as well. Reduce legal liability.	Training should be conducted prior to every event (i.e. on event day before gates open). Conduct annual training of all staff. Test or quiz staff to determine the effectiveness of training. Challenge staff during the year with questions. Encourage staff to review policy and procedures on a regular basis.	This is regardless of event size. It is your team and they reflect your business, quality of capability is important.
2. Specify basic training requirements. • Create a catalog of needed skills and required training to include guest relations, problem-solving and basic security procedures (i.e. access control, situational awareness, screening, etc.) • Offer CPR/AED training for everyone	Specialized training.	Consider handouts, online modules or classroom presentation.	
3. Establish an events handbook that clearly explains expectations, rules and guidelines.	Documentation and protection for legal liability.	Hard copy or online.	
4. Set-up periodic refresher training for full-time and event staff, at least annually.	Things change; programs and personnel need to stay current.	Document this training.	
5. Hold annual training for security personnel on proper screening and inspection techniques for patrons and their belongings. Maintain training records. • Annual security awareness training of non-security staff such as registration/check-in, food service personnel, room monitors and others must also be conducted, with a record of training maintained • Conduct assessments to evaluate awareness and compliance	Regular documented training.	Consider hosting lunch and learn programs throughout the year and invite different speakers/trainers.	

LEADERSHIP AND DEVELOPMENT TRAINING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Develop, implement and maintain an effective staff training/learning program that covers training ALL full-time staff and event supervisors.	Security and safety knowledge and awareness.		Regardless of event size.
2. Document ALL training and retain these records in paper and/or digital format for at least 5 years or as required by state law. • Training records should include: a. Date and location of training b. Time of day and duration of each session c. A description of the training d. Name and qualifications of the instructor e. List of attendees and their signatures f. Results of any evaluation or testing	Good records retention policy.	If contracting services, the third-party vendor or service provider contract should require documentation of training records for those individuals working the venue(s) including elements a – f. Conduct random checks for verification.	
3. Document ALL drills/ exercises and retain these records in paper and/or digital format for at least 5 years or as required by state law. • Exercise records should include: a. Description of drill/ exercise b. Date held c. List of participants d. List of equipment tested or employed in the exercise e. Name(s) and qualifications of the exercise director(s) f. Any lessons learned to improve planning and response	Good records retention policy and reduce legal liability.	If contracting services, the third-party vendor or service provider should provide documentation of training records for those individuals working the venue(s), including elements a – f. Conduct random checks for verification.	

CONTINUOUS IMPROVEMENT CYCLE

1. Establish a Continuous Improvement Cycle program.	Keeps staff motivated, increased their desire to learn and help improve job performance.	Consider doing this multi-venue or on a regional basis.	Recommended for all events.
2. Establish a Continuous Improvement Inventory of metrics for event/venue safety/security and incident management systems.	Consistency.		
3. Establish a program to reward positive behavior/execution/practice of what they have learned.	This keeps staff motivated.		

SUCCESSION PLANNING

1. Establish a succession plan and train people so that they can step in and assume a key role if/when needed.	Proper planning. Event folders must be meticulously prepared for every event. It allows successor to fully understand event preparation and execution.		The larger the event, the more critical this process becomes.
2. Have staff record what they know and how they accomplish their goals (basically an Operational Manual that is done over time).	Give successor the ability to get up to speed quickly.		Self acknowledgement and awareness also produces effective change where appropriate and pride in their role.

STANDARDS AND CERTIFICATIONS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Adopt standards and seek certifications for event/venue security staff involved in safety and security roles, management of same, as well as other event day positions.	Improves performance.		
2. Make sure to check staff certifications and document them.		May be verified by entity or department.	

HIRING AND BACKGROUND SCREENING

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Conduct a background check on all personnel working in ANY capacity in the venue. • Understand privacy issues regarding employment, interviews and records • Ensure that background checks follows state and federal laws • Ensure hiring standards and process are legally defensible	Staff represent the event/venue. They must not be any issues with staff that negatively impact the venue.	Programs are available and can be developed to allow potential employees or volunteers to obtain and pay for background checks. Include background check requirements in any agreements for contracted staff (i.e. security, parking attendants, concessions, etc.).	This is essential for all size events.
2. Ensure personnel meet certain basic skills based upon the roles and responsibilities of their job. • Use an online application process • A job-related test can assist in evaluating candidates	The right people for the right position.		This is essential for all size events.
3. Ensure personnel meet basic social communication skills/image (dress), including foreign language skills, as they will be interacting with patrons/customers.	Image and branding. Quality guest services.		This is essential for all size events.

THIRD PARTY CONTRACTS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Specify all details of required expectations of performance, roles, skills, qualifications, certifications and measurements/metrics in contracts. • Set high standards and hold contractor to those standards–ensure they know the standards when they apply/compete for the contract • Do not let them sub out to another company • Conduct due diligence on potential contractors • Require references and check them out • Work with venue administration to ensure purchasing rules and procedures are in compliance	Set expectations, standards or knowledge and performance. To avoid poor contractor performance and legal issues later.	Make sure to specify exactly the who, what, when, where and how; if there is a dispute the venue will have the legal basis to hold them accountable. Be specific regarding contract items. List training requirements, uniform, code of conduct, etc., as part of the contract.	Hold contractors to the standards you set forth in your contracts.
2. Obtain documentation for third-party vendors on an annual basis: • Proof of background checks • Proof of liability insurance/bonding • Proof of workers' compensation insurance	To protect the organization.	Maintain copies of this documentation.	
3. Integrate third-party contractors into planning, training and unified command structure.	Avoid "us and them" as it will be defeating.	Best if they participate in exercises.	
4. Ensure that security staff employed at the venue, who are not active law enforcement personnel are licensed and/or certified by a state regulatory body where licensing and certification is required or available.	Be in compliance with laws.	Keep track of licensing and certification renewals to ensure they remain valid/current for contract services. If not up-to-date, it may invalidate insurance coverage. Check these annually.	

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
5. Ensure contracted staff is given venue familiarization/orientation and understands policies and procedures.	They cannot help patrons if they do not know the layout of the venue.	This is important for effective incident response, as well as customer support.	
6. Assign a supervisor to observe and evaluate overall staff performance during the event.	Verification.	Provide feedback to contractor.	This person should have been involved or knowledgeable with the RFP and contract.

RELATIONSHIP BETWEEN THIRD PARTY/LAW ENFORCEMENT/EVENT ADMINISTRATION

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Schedule meetings between all parties to facilitate coordination and an understanding of each other's roles and responsibilities. • This should occur on a regular basis	Eliminate potential friction.	Include in post orders.	For larger events or security sensitive events. Building relationships in the various cities of your events establishes a familiarity between event planner and public safety. This is also important if you are using private security so there is a relationship to de-conflict potential issues.

POST ORDERS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Prepare and employ post orders for all staff (full-time, part-time, contract, volunteer).	Assists event day staff (i.e. part-time, seasonal, volunteer and third-party contractors) with their role, responsibilities, methods of communication and EAP.	Post orders help ensure consistency in job responsibilities and security.	Certainly for larger events requiring a safety and security staff/team.
2. Post orders should include post description, role, responsibility, communication, emergency procedures and equipment for that post and map/diagram of the venue.	Awareness.	Post orders have been produced in various formats: • Booklets • Cards • Digital (smartphone) • Apps	

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
3. Post orders should be simple, such as in a bulleted format, on laminated cards for each staff member (full-time, part-time, contract).	Clarity and brevity.		

TOOLS FOR EMPLOYEES

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Ensure staff has the necessary tools to perform their tasks and are trained in using them.	Properly equipped and trained.	Tools should include: • Radio • Cell phone/smartphone • Pen and paper (small notebook) • Flashlight • Guide • Staff credential • Post orders • Emergency procedures	Regardless of event size, but essential for larger events with larger staff.
2. Consider using an event software program that assists in managing all event staff. These systems enable direct contact with individual staff, participants, vendors and sponsors with one simple email or a touch of a button.	Get information out and save time.	Various venue/event information management systems exist.	For large events and certain smaller events, depending on status.

PRIVATE SECURITY AND LAW ENFORCEMENT

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. If contracting private security, establish boundaries, accountability and partnering with law enforcement and on-board venue staff.	Eliminate an us vs. them environment and finger-pointing if something goes wrong.	Exercises can foster this process.	For larger, security sensitive events–pre-event meeting are essential.
2. Plan and train together to help build a team approach.		Lead by example and teach supervisors to do the same.	Where appropriate.

REWARDS

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Reward positive behavior and exemplary performance as it encourages more of the same and establishes loyalty.	Helps with retention and positive attitudes.	Various types of recognition have been found to work: • Acknowledgement (oral and written) • Merchandise • Service pins • Gift cards/prizes • Event tickets for relatives • Prime parking	

EXERCISES			
BEST PRACTICE	**OBJECTIVE**	**IMPLEMENTATION**	**APPLICABILITY / SCALABILITY**

1. Plan and conduct exercises of all plans on an annual basis.
 	
• The plans should be exercised on a regular basis to ensure the plans meet current conditions and that all will respond accordingly
• Remember that the event can serve as an exercise
• Designate a knowledgeable person/compliance officer to document observations (i.e. what worked, etc.)
	Exercises are extensive operations or maneuvers, intended to train personnel, assess capabilities. Evaluates knowledge and skill.
	
	Exercises have many benefits:
	• Reduce problems, mistakes or omissions that can occur during an actual crisis
	• Time spent producing and participating will pay off when a crisis occurs
	• Helps eliminate "it can't happen here" attitude
	• Teach venue executives the complexity of preparedness and decision making during crisis situations
		Exercises are scalable. There are four main types:
		• ORIENTATION
		  • Provides overview of plan
		  • Familiarizes participants
		  • Use with new plan or team members
		  • Informal, easy and low stress
		  • Planning cycle 30 days, duration 1 hour
		• TABLETOP
		  • Scenario in narrative format
		  • Practices team building and problem-solving
		  • Addresses one issue at a time
		  • Somewhat detailed with a medium stress level
		  • Planning cycle 2-3 months, duration 2-4 hours
		• FUNCTIONAL
		  • Simulates scenario as realistically as possible
		  • Short of mobilizing personnel, equipment and resources to an actual site
		  • Evaluates specific functions
		  • Typically detailed with high stress level
		  • Planning cycle 6-8 months, duration 4-6 hours
		• FULL SCALE
		  • Deploys personnel, equipment and resources to a specific venue
		  • Evaluates operational capabilities in an interactive manner
		  • Facilitates communications and coordination across organization and public and private sector
		  • Very detailed with high stress level
		  • Planning cycle 8-12 months, duration 6-8 hours. The FBI, and DHS offer exercise services.
			This applies to event organizers, venues, lodging and transportation modes.
			
			This is important large, reoccurring events.
			
			These need to be coordinated between event and venue; it is an added benefit to include lodging, transportation and public safety personnel.
			
			Online training modules can be used to augment training between exercises.

2. Employ exercises to test plans, implementation and execution. • Conduct annual table-top exercises and full-scale exercises. Ensure that a gap analysis is done following each exercise and that recommended changes are implemented.	Testing, reinforcing and correcting.	Personnel must be aware of plans prior to exercise.	
3. Document exercises, indicating the scope and duration, names of personnel and organizations who participated, actions for improvement and recommendations for plan modifications.	For litigation purposes, lessons learned and improving future exercises.		

TOPICAL AREA: TECHNOLOGY, INFORMATION MANAGEMENT AND SECURITY

TECHNOLOGY USE

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Identify who manages and has budget responsibility for the following: • Purchase and installation • Maintenance and service • Internally sourced or outsourced agreement for equipment and services • Upgrades and enhancements	Users frequently are not the owners responsible for technology systems (i.e. CCTV, card access, UPS). Without control, it is essential to communicate and collaborate to ensure needs are met.	Technology can be a force multiplier or a burden depending upon how it is managed. Establish a collaborative team to iron out any issues and establish who has control over what, so that things will run smoothly during the event. In today's technology driven world, it is important to leverage advances in technology and innovation to achieve the best cost.	Securing the exchange of personal data, payment information and technology access points is more important today than ever, regardless of event size.

INFORMATION MANAGEMENT

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. In all likelihood, information management systems will fall under one or more of the following: • Venue Administration • Event Administration • IT Department or CIO • Marketing Department • Facilities Department • Legal • Risk and Compliance Team • App/Tech/Preferred Providers • Insurance • Security Teams	Meeting and event organizers frequently are not the business owners responsible for technology systems; however, they may be the owners of the information exchanged during event registration and execution. That is why it is essential to communicate and collaborate with the people managing information systems/applications to ensure security needs are met.	Having a designated person responsible/in-charge for this is the best approach Each country has different rules for how data may be collected, what must be disclosed about its use, what it can be used for and when records need to be purged. Work with information management owners to ensure each event is in compliance with data use regulations governing event attendees.	Depending on the size of the event, data may determine whether or not professional support may be required. No matter the size of the organization, collaborating and partnering almost always results in a better outcome.

2. Types of information management systems used vary by event. Some examples include: • Event registration for live or virtual events • Association management systems • Security cameras • Metal detectors and magnetometers • Augmented Reality and Virtual Reality platforms • Voice-activated AI-technology • Dropbox and other cloud-based platforms • USB keys • Texting platforms • Marketing databases and email lists • Surveys/polls and audience response systems • Website cookies • Social media channels and paid social • Website retargeting campaigns • Hotel reservation systems and loyalty programs • Hotel rooming lists • Strategic meetings management software • Speaker management databases • Event apps • Text • Location-based technology and trackers (GPS, Beacons, NFID/RFD) • Badge scanners • Lead retrieval devices • Digital networking tools • Appointment-setting software • WiFi and other internet connections onsite • Office or event-specific intranets • Email servers • Travel and expense management systems • Master account billing • Content capture and live-streaming technology • Audiovisual and event production systems • Access control/badging systems • Customer Relationship Management software • Airline or transportation manifest • Vendor/exhibition management tools	Identify all the ways in which data is collected, stored or exchanged before, during or after the event.	Creating a list of all the ways information is collected, managed, communicated or analyzed helps identify potential vulnerabilities as well as cross-departmental dependencies.	Some data collection and management systems may be managed by internal teams other than the meetings department. Others may be contracted to a third party. The larger the event organizing/production organization, the more likely it is that the meetings/event team will be supported by internal business units. In smaller companies or for smaller meetings/events, the meeting/event organizer may have more direct control over information management systems.

3. Identify who owns the information policies and content related to and generated by the employed technology system(s): • Control and use of the system • Controls and views content and reports • Grants permissions and releases information • Guarantees compliance with industry standards • Ensures compliance with privacy and data use policies in relevant jurisdictions	Accountability and accessibility Users (event organizers/venue operations) frequently are not the owners responsible for technology systems; however, they may be the owners of the information. Without control, it is essential to communicate and collaborate to ensure needs are met.	Event and/or venue may have a Chief Information Officer who is in charge. Determine venue/event needs and whether or not the existing systems meet these needs. If not, define requirements and identify who can fulfill these needs.	Event organizers should be able to tell participants what data is being collected, why it is needed, what it will be used for and how it will be protected. Transparency is key to building trust, whether it is between buyers and suppliers or event organizers and participants.
4. Confirm the reliability of the systems and the integrity of the data collected on an annual basis, along with the availability of the information through either automated diagnostics or manual testing.	Unreliable and unavailable data is worthless. Regulations change. Equipment and systems degrade over time and should be tested regularly.	Take ownership with what is under event/venue control and partner with others over what fall outside event/venue control. Test IT prior to each event to include video cameras and recording capabilities.	
5. Consider using Command Center/event/incident/operations information management software. • Web-based, accessible anywhere • Central digital repository • Mobile device accessibility • Analytical tools	Keeps all entities current with the same information and serves as an official record for litigation and after-action.	There are various Information Management Systems on the market that contain modules to enter/maintain/recall reports for use and transmission to public safety units.	When possible co-locate event operation centers and staff with local first responders, event security teams and law enforcement. If an incident occurs, relay information to the proper party so it may be resolved.
6. Make sure all automated systems have redundancy and off-site backup capabilities.	Redundancy is often the only recovery capability.	Off-site backup is a must in case something happens to the primary system or location or its power source.	Where is data stored? What happens if the power goes off or a cell tower goes down? If there are physical backups, what steps will be taken to prevent theft? If cloud-based, what kinds of firewalls are in place to deflect bad actors, like hackers? If the system is disrupted in any way, how long will it take to get it back online? What kind of gap will that create? What information do you need to have in physical form at the event if that happens or switch to the back-up system?

7. Consider using a Geographic Information System (GIS). • Mapping capabilities using geospatial information and live feeds for situation maps, briefing maps and interactive mapping that can track participants in real-time	For visual situational awareness and managing people movement.	This can accommodate NFC/RFID feeds tied to badges, mobile devices and event apps.	Tied to an event app, GIS information can be used to send push notifications to move attendees away from crowded areas to less-trafficked exhibitors or sessions. It also may be used as an emergency communication system to alert affected attendees away from incidents or towards exits, or to convey other emergency-related information.
8. Access control, patron monitoring systems/software used for data collection and analysis, such as electronic ticketing, RFID, apps, etc., should be protected from unlawful access and use.	To ensure the security of the data collected from event participants or others.	Where is the data being stored and who has access should be addressed. Understand how data should be encrypted and what security is in place to prevent access points from being compromised.	Before signing contracts with vendors, become familiar with data collection and use policies and how data will be disposed of post-event. Understand how data is encrypted and protected.
9. Travel Meeting Management software must have clear security controls as most contain Personally Identifiable Information (PII) and credit card info.	Prevent theft of patrons, personal and financial data.	Where is the data being stored and who has access should be addressed?	Make sure vendors are in compliance with PII regulations. If there is a breech, how soon will you know? How would communicate and handle that? What are your notification responsibilities?

DATA SECURITY

BEST PRACTICE	OBJECTIVE	IMPLEMENTATION	APPLICABILITY / SCALABILITY
1. Assemble an internal IT/ Risk Assessment team to conduct security assessment on technology and data-handling procedures before contracting vendors.	Determine what is an acceptable risk, internal ownership for each data collection or technology touchpoint and people internally or externally who will be cleared to access the data collected.	Sample discussion-starting questions: • Where does the data go? • Who owns the data? • What criteria is there for gaining access to the data? • Where is the historical event data and can we access it? • What can we agree to on ownership and responsibility? • How do we protect our patrons and their data? • What's an acceptable risk? • All data should be private? • When do we want customization? • What are protocols for remote users? • Who will be looking at the data we're collecting?	This is relevant to all events using digital data.
2. Set data-handling and privacy policies for the event and be transparent. • Allow patrons to opt-in verses opting-out	Transparency about what is being gathered, why it is being gathered and how it will be used is important.	List the policy or links to policy on all forms and websites where data is being collected or behavior is monitored. If people are being recorded or if their movements are being tracked, signage or releases may be required. Include data ownership, treatment and use details in vendor contracts.	Most IT departments are aware of European GDPR regulations and have standard privacy and data use policies. Work with vendors and other third-party suppliers to ensure compliance.

3. Set up internet access, devices and apps in ways that increase event security. • Include security and access information in "know-before-you-go" communications as well as any applicable warnings about connecting to rogue hotspots. • If possible, set up private networks for event Wi-Fi	Avoid public access (free) Wi-Fi connections to protect data being transmitted via email or through websites.	Don't use open or public Wi-Fi channels for events. Instead, require networks that are password-protected. Stipulate in the contract the number of SSIDs and bandwidth required for the event. Know that bandwidth needs to support 3-5 devices per person. Include recourse, reparation and rebate language in the contract that protects the organization and spells out what will happen if something goes wrong with the internet. Partner with the venue and/or its audiovisual team to ensure greater security: Know where their access points (AP) are, what they are and how they can be secured.	Whether for personal or professional use, any device that is set to its preset factory password is vulnerable to cyberattack. Include security and access information in know-before-you-go communications as well as any applicable warnings about connecting to rogue hotspots.
4. Regularly screen USB charge ports or don't use them.	Prevent infection of laptops, mobile phones and other devices by avoiding USB ports.	USB ports are easily infected by malware. In public spaces, such as airport lounges and hotel rooms, use the device's charger plug rather than the USB port. Disable USB ports on kiosks and laptops if they are not regularly screened. Require speakers submit presentations weeks in advance to avoid USB key usage onsite. Or use AV-supplied laptops, and don't reuse USB keys after files are downloaded.	Providers of charging stations and rental laptops should be able to inform how they prevent malware from infecting USB ports and how often they screen devices. If a presentation management system is out of budget range, files can be shared by cloud-based technologies, or organizers can require speakers to bring their own laptops.

5. Evaluate what should and should not be posted on event websites, signage and hotel readerboards.	Protecting the identity of the group, if organizational policies, leaders, participants or speakers may be targeted. Protecting the identity of the individual attendees also may prevent cybercrimes such as room block poaching and identity theft.	Consider listing the name of the event rather than the company's name on transportation signage and hotel readerboards. If your event website has a "look who's coming" area, list by companies only. Do not list by individual's names. Room block poachers use that information to phish attendees. It also allows bad actors to gain access to your event by impersonating someone who's on your list, or opens attendees up to potential harm if they're being stalked.	Important for all events using electronic information delivery. Some events, for privacy or security reasons, may opt not to have information listed on the hotel readerboards at all.
6. Collect emergency contact information when people register, use technology to communicate before and after incidents occur. • Make cell phone and emergency contact fields mandatory on registration forms • Explain the data will only be used in case of emergency	Finding information about what to do in case of an emergency should be fast and easy.	Emergency maps, plans and contact numbers should be in a prominent place in the event app. While people are waiting for the event to begin, AV teams can show videos or slides instructing attendees about emergency procedures. Push-to-text notifications for different kinds of incidents can be pre-loaded for quick deployment in case of emergency.	Applicable to all size events. Push-to-text notifications are fairly inexpensive, but become useless if the mobile network goes down. So finding ways of communicating what people should do before anything happens is the best way to cultivate a safe and aware mindset.
7. Train employees, attendees and exhibitors to recognize emails phishing for information.	Avoid fraud and theft by educating event stakeholders and participants.	Some phishing emails look like conference communications. Train staff, attendees and exhibitors to avoid emails that deviate from the event's format, include execution (.exe) files or ask for a password in exchange for downloading a file.	In first communication (such as registration confirmation) think about including information about types of communication that will follow. For example, it will always come from a certain person or outline what instances (if ever) you might require them to enter a password or download a file. Include contact information for whom to alert if they receive a suspicious communication.

8. Correctly dispose of information and data.	Protect intellectual property and sensitive conference materials.	Bring a shredder onsite. Sweep the conference rooms and dispose of anything left behind. Know what AV teams will do with rental laptops or presentation management systems after the event ends. Include in contract language expectations for data disposal, treatment and use.	Important regardless of event size. If clean-up falls to venue staff, know what they do with the materials, are they are shredded or how data is disposed.
9. Use collected data to improve the quality of the event experience.	Enhance safety and security without compromising the event experience. Data collection with a purpose.	Include questions about food allergies and physical impairments on the registration form so those needs may be anticipated and met. Use data collected via surveys and polls, speaker evaluations and attendee movement information from badge-scanning or other tracking technology to determine where attendees went, what attendees liked and disliked. Use information to determine how to improve subsequent events. Monitor social media for anecdotal evidence as well as complaints for event issues that need to be addressed. During the post-con meeting, ask venues about event bandwidth usage. It helps organizers estimate need for budgets and determine usage for future events.	In today's use of technology this is applicable to all events. Few event organizers share how survey data is used. Telling the story of how an event was improved by listening to feedback can be a powerful way to engage audiences and encourage two-way feedback. Relying on data also will strengthen the meeting or event professional's strategic role within the organization.
10. Isolate medical records and other sensitive personal or financial information to a separate encrypted environment. • Employ two-factor authentication or other extensive password protocols	Block bad actors from accessing sensitive data.	Set different access levels to data based on need-to-know basis. Anything that needs to be protected should be encrypted.	This is applicable regardless of event size. Consider, block chain, if a practical solution.

APPENDIX I: TABLE OF ABBREVIATIONS

AAR	After Action Review
AED	Automated External Defibrillator
BATF	Bureau of Alcohol, Tobacco and Firearms
CAD	Computer Aided Drawing
CCTV	Closed Circuit Television (i.e. video surveillance)
CCS	Concentric Circles of Security
DHS	Department of Homeland Security
EAP	Emergency Action Plan (synonym: Incident Action Plan)
EOP	Emergency Operations Plan
EM	Emergency Management
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
EOC	Emergency Operations Center
EOD	Explosive Ordinance Disposal
ESSC	Executive Safety & Security Committee
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
HVAC	Heating, Ventilation, Air Conditioning
IAP	Incident Action Plan (synonym: Emergency Action Plan)
IC	Incident Commander
ICS	Incident Command System
ID	Identification
IED	Improvised Explosive Device
IT	Information Technology
JIC	Joint Information Center
JTTF	Joint Terrorism Task Force
MAA	Mutual Aid Agreement
MSDS	Material Safety Data Sheet
NIMS	National Incident Management System
NTSB	National Transportation Safety Board
NWS	National Weather Service
PA	Public Address System
PSA	Public Service Announcement
RTVA	Risk, Threat and Vulnerability Assessment
SMCC	Specialized Management Coordination Committee
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UPS	Uninterrupted Power System
USPS	United States Postal Service
VBIED	Vehicle Borne Improvised Explosive Device
VOIP	Voice Over Internet Protocol
WMD	Weapons of Mass Destruction
WPS	Wireless Priority Service

APPENDIX II:

AUTHORITATIVE REFERENCE LIST AND RELEVANT COURSES

- ASIS Business Continuity Guidelines
- ASIS SPC.1-2009
- AWR: Sport Event Risk Management
- Best Practices Guides for Professional Sports Leagues
- Business: A Practical Introduction by Brian Williams, Stacey Sawyer, and Susan Berston
- Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 1.3.6 Reporting Use of Force
- Core Crisis Preparedness Measures Implemented by Meeting Planners, Hilliard, Scott-Halsell, Palakurthi
- Customer Service Skills for Success by Robert Lucas
- Cybersecurity and Event Planning, Timothy M. Banks
- Deficits in Crisis Preparedness by Meeting Planners, Hillard, Scott-Halsell, Palakurthi
- Department of Homeland Security Legal Division Handbook
- DHS National Incident Management System: Guideline for the Credentialing of Personnel
- DHS Protective Measures Guide for U.S. Sports Leagues
- Difference Between Duty of Care and Travel Risk Management
- DOJ Crime Scene Investigation: A Guide for Law Enforcement
- DOJ Planning and Managing for Major Special Events
- Enhanced Sports and Special Events Incident Management
- Essentials of Contemporary Management by Gareth Jones and Jennifer Jones
- Facility Management by Edmond Rondeau, Robert Brown, and Paul Lapides
- FBI Law Enforcement Crisis Management Handbook
- FEMA ICS 100
- FEMA IS 230c
- FEMA IS 235b
- FEMA IS 242a
- FEMA National Incident Management System
- Graham v. Connor, 490 U.S. 386 (1989). HR by Angelo DeNisi and Ricky Griffin
- Hotel Security and Safety Assessment, OSAC
- How Prepared are Event Planners in Responding to an Act of Terror?
- ICS 200
- Information and Technical Assistance on the Americans with Disabilities Act
- Intercollegiate Sports Events Safety & Security Best Practices Guide (1st & 2nd Editions)
- IS-700.A: National Incident Management System (NIMS) An Introduction
- IS-906

- MGT 310: Threat and Risk Assessment
- MGT 314: Senior Officials Workshop for All Hazard Preparedness
- MGT 404 Sports and Special Events Incident Management
- MGT 412: Sport and Special Event Evacuation Training and Exercise
- National Institute of Justice Officer Performance and Safety
- National Special Security Events: Transportation Planning for Planned Special Events
- NFPA Fire Code 1600
- NFPA Fire Code 14.4.1
- NFPA Fire Code 1-67
- OSHA Compliance Assistance Quick Start
- Presidential Policy Directive — Critical Infrastructure Security and Resilience - PRESIDENTIAL POLICY DIRECTIVE/PPD-21
- Protective Measures Guide for U.S. Sports Leagues
- Safety, Security & Risk Management Guidebook, Events Industry Council
- Security Management of Sports and Special Events by Stacey Hall, Walter Cooper, Lou Marciani, and James McGee
- Techniques for Effective Alcohol Management: A Comprehensive Alcohol Management Program for Sports and Entertainment Professionals
- Three Dimensional Model of Stadium Owner Liability in Spectator Injury Cases by Joshua Kastenburg
- U.S. Constitution 4th Amendment
- U.S. Department of Transportation and National Highway Traffic Safety Administration's Alcohol and Highway Safety 2001: A Review of the State of Knowledge
- Vicarious Liability: Two Supreme Court Decisions

APPENDIX III:

2017 MPI THOUGHT LEADERS' SUMMIT ATTENDEES AND BEST PRACTICES CONTRIBUTORS
Thanks to everyone who made *MPI's Essential Guide to Safety and Security* possible.

LEAD SPONSOR
MPI Foundation

INDUSTRY PARTNERS
APEX Risk Management Task Force
Events Industry Council (EIC)
Hospitality Sales & Marketing
  Association International (HSMAI)
IACC
International Association of Exhibitions
  and Events (IAEE)
National Center for Spectator Sports Safety
  and Security (NCS4) at the University of
  Southern Mississippi

SPONSORS
Allied PRA
American Airlines
Delta Air Lines
Disney Destinations
Disney Meetings
Freeman Audio Visual Inc.
Greater Palm Springs Convention & Visitors Bureau
IHG - InterContinental Hotels Group
Discover Los Angeles
Marriott International
PSAV
Rosen Shingle Creek Resort &
  Golf Club/Rosen Hotels & Resorts
San Francisco Travel Association
Venetian/Palazzo Resort Hotel & Casino
Visit Dallas

FACILITATORS
Kristi Casey Sanders, CMP, CMM, DES, HMCC, MPI
Paul Denton, NCS4
Gary Gardner, NCS4
Misty Helm, MPI
Lou Marciani, NCS4
Don Paisant, NCS4
Jeff Steele, NCS4
Daniel Ward, NCS4
Elli Voorhees, NCS4

SCRIBES
Stacey Engelmann, DMCP, Imprint Group
Nancy Henkel, CMP, Medical Association
  Management & Meetings for BroadWater
Stephanie LaRussa,
  University of Central Florida student
Marie Peterson, CMP, Detent Events
Alex Plaxen, Little Bird Told Media
Jessie States, CMM, MPI
Elli Voorhees, NCS4

CONTRIBUTING AUTHORS/ATTENDEES

Kristi Allan, CMP
Michelle Allgauer
Dawn Amick, CMP
Brian Avery
Dahlton Bennington
Dee Blakeney
MaryAnne Bobrow
Betsy Bondurant
Lynne Bowis, CMP
Juel Brathwaite-Alleyne
Doreen Burse
Frank Bustamante
Gregory Butler
Sherry DeLaGarza,
  CMP, CMM
Brook Dilworth
Cathy DosSantos,
  CMP, SMMM, HMCC
Louise Elleo
Meaghan Ferrazza
Ginny Fountain
Ernie Garcia
Chris Gatch
Darren Green
Annette Gregg,
  CMM, MBA
Cheryl Hatcher,
  CDME, HMCC
Todd Helton
Tyra Hilliard
TJ Johnson
Kyle Jordan
Laurie Kazimer
Allison Kinsley
Steve Kinsley
Alan Kleinfeld
Lisa Kopp
Karen Kotowski
Edie Leibman
Julie Lynch
Matthew Marcial, CAE, CMP
Judy McClain
Tim McGuinness
Leslie Menichini
Kimberly Montoya
Mary Mycka
Stacie Nerf
Michael Owen
Michael Pinchera

Sandy Pizzarusso
Tim Quigley
John Rissi
Christine Roberts
Carmela Robertson
Jimmy Romo
Jim Russell
Jim Rye
Danny Salas-Porras
Bernie Schraer
Tom Schwinden
Libby Severance, CTIE
Stefanie Simmons,
  DES, CTA
Lynette Smith
Tyler Stewart
Jesse Suglia
Darren Temple
Erin Tench
Eileen Valois
Paul Van Deventer
Elizabeth Weisbrod
Catlin Whitington
Betty Wilson