U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Best Practices in Anti-Terrorism Security (BPATS) for Sporting and Entertainment Venues

The Department of Homeland Security (DHS) is continuing its efforts to develop knowledge products that will help security professionals implement security programs designed to prevent and defend against acts of terrorism at mass gathering venues.

In the aftermath of the terrorist attacks of September 11, 2001, the private sector expressed considerable reluctance to deploy security technologies and services in civilian settings due to the enormous potential liability risks in the event those deployments were impacted by an act of terrorism. As the private sector owns and operates most of the Nation's critical infrastructure, this reluctance created the potential for under-investment in and under-deployment of necessary security technologies and capabilities. Congress thus enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 6 U.S.C. §§441-444, to assist in mitigating these risks, and to encourage the widespread deployment of effective anti-terrorism technologies and services that could save lives. The SAFETY Act Program is administered by the Office of SAFETY Act Implementation (OSAI) in the Science and Technology Directorate, U.S. Department of Homeland Security.

In 2012, OSAI engaged the Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA), a DHS Center of Excellence at Rutgers University, to undertake a research project, "Best Practices in Anti-Terrorism Security" (BPATS I) for sporting and entertainment venues. BPATS I resulted in a "Best Practices in Anti-Terrorism Security for Sporting and Entertainment Venues Resource Guide," which is posted on the SAFETY Act Program website, www.safetyact.gov. The BPATS I Guide presents important components of a stadium anti-terrorism security plan. This knowledge product has been well received and used by security professionals across the United States.

A well-developed layered security program should have a means to perform regular assessments of capability and effectiveness. The availability of relevant measures and metrics will assist in this regard. Hence, OSAI decided to continue its research engagement with CCICADA – a follow-on project was developed to examine Metrics and Measures of Effectiveness for anti-terrorism security at sports and entertainment venues (BPATS II). The intent of the project was to generate more quantitative measures that will go beyond the Yes/No metrics that were discussed in the BPATS I Guide.

The research project reviewed relevant literature on the evaluation of venue inspection and credentialing processes, of practices used by government agencies and the private sector, and consulted with venue and sports league security directors to assess the utility and feasibility of proposed measures. The results and recommendations of the study have been encapsulated in a Metrics & Measures of Effectiveness Resource Guide.

As you review this Resource Guide, keep in mind the following:

1. The SAFETY Act Program is a voluntary program designed to incentivize the development and widespread deployment of effective anti-terrorism technologies, services and capabilities. It is not a regulatory program. Applications are evaluated based on criteria published in the Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) at 6 Code of Federal Regulations, Part 25.
2. Hence, the Resource Guide is not a list of specific requirements, but a guide for venue owners, operators and security professionals to use as appropriate to strengthen anti-terrorism security for their venues. Besides strengthening venue security, implementing all or part of the Resource Guide should assist an entity in preparing a successful application for SAFETY Act coverage.
3. The Resource Guide is not a comprehensive guide for the sum total of metrics and measures of effectiveness for sporting and entertainment venues. The Guide focuses on the aspects of access control and screening patrons, credentialing venue staff, and assessing training. While these aspects are critical, there are other areas for which metrics and measures of effectiveness should also be developed. We note that both the methodology and the detailed metrics given in the Resource Guide have been assessed in a structured manner by leading experts in the industry, and should be replicable for other aspects of security for sporting and entertainment venues.

Before consulting the Guide, let's review some key concepts used in the Guide:

Some basic terms: Different operational facets of maintaining security (e.g., patron screening) are referred to as **aspects**. Actions that may be taken to address a specific aspect of venue security (e.g., using walkthrough metal detectors -- WTMDs) are referred to as **activities**. We can further classify activities into different **categories**. For example, categories of activities for the aspect of credentialing and access control include Technology Implementation, Employee Hiring and Credential Design and Issuance. **Metrics** are ways to measure an activity or a component. In the Resource Guide, metrics are listed for each category.

Essential v. Conditional activities: Some activities are **Essential** in the sense that they should be done for every kind of event at the venue; in most cases, their function cannot be achieved by doing something else. Others are **Conditional** in that they are desirable and add value, but could be made up for by doing other things instead, or whose need might depend on the kind of event for which you are providing security. Experts consulted during this study agreed that the risk associated with events varies by type of event. The study's researchers thus recommend that **event classes** relevant to the facility be defined by a venue, and that the

venue's security plan indicate how activities relevant to their facility are chosen to be appropriate risk-reducers for each event class as the venue has defined it.

Stage 1 and Stage 2 Metrics:

- **Stage 1 Metrics** indicate whether or not particular activities are being done in support of the corresponding aspect of security.
- **Stage 2 Metrics** are more detailed, apply to components of an activity, and measure things like the frequency of carrying out an activity or the percentage of times it is successful. A wide variety of Stage 2 Metrics was considered; only those that were determined to be important and operationally feasible by the panel of experts consulted have been included.

We hope the attached Resource Guide will be valuable in your work. Your comments and feedback are welcome. Please send them to OSAI@hq.dhs.gov.

Sincerely,

Bruce Davidson
Director
Office of SAFETY Act Implementation
Science and Technology Directorate
Department of Homeland Security

Best Practices in Anti-terrorism Security (BPATS)

Tier II

Metrics & Measures of Effectiveness

Resource Guide

November 2016

Based on a research study undertaken for the Office of SAFETY Act Implementation, Science and Technology Directorate, Department of Homeland Security by:

Command, Control and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security University Center of Excellence

Table 1.1: Final Essential Metrics for Screening

Category	Stage 1 Metric	Stage 2 Metric
Training	Are screeners trained before working?	How many hours are screeners trained before working?
		How many hours are screeners trained on Walkthrough Metal Detectors (WTMDs)?
		How many hours are screeners trained on Handheld Metal Detection Wands?
		How many hours are screeners trained on patdowns?
		How many hours are screeners trained on bag checks?
		How many hours are screeners trained on visual inspections?
		Are screeners' skills tested before working?
		How many patrons are screeners' skills tested on before working on WTMDs?
		How many patrons are screeners' skills tested on before working on Handheld Metal Detection Wands?
		How many patrons are screeners' skills tested on before working on patdowns?
		How many patrons are

Category	Stage 1 Metric	Stage 2 Metric
- continued - **Training** - continued -	- continued - Are screeners trained before working? - continued -	screeners' skills tested on before working on bag checks?
		How many patrons are screeners' skills tested on before working on visual inspection?
		What is the "pass" percentage screeners need to achieve before approval to work as a screener for WTMDs?
		What is the "pass" percentage screeners need to achieve before approval to work as a screener for Handheld Metal Detection Wands?
		What is the "pass" percentage screeners need to achieve before approval to work as a screener for bag checks?
		What is the "pass" percentage screeners need to achieve before approval to work as a screener for visual inspection?
Patron Inspection – General	Are patrons rescreened when a suspicious item found?	-
	Is there a form of inspection at perimeter entrance points?	What is the ratio of perimeter entrance screeners to screening lanes?

Category	Stage 1 Metric	Stage 2 Metric
Bag Check	Are contents of all bags inspected?	-
Using Walkthrough Metal Detector Technology and Inspection	Is there a protocol in place for what to do with a patron who alarms the WTMD?	Is there a designated screener watching for WTMD alarms?
	Does the venue have a marked location of where the WTMD queue starts prior to screening?	How many feet away does the WTMD queue start prior to the current patron being screened?
	Does venue have a procedure for testing WTMDs to ensure they maintain their intended level of security?	How often are WTMDs tested by supervisors with test items?
		How many times per year are all WTMDs tested?
		How often are WTMDs recalibrated?
Red Teaming	Does the venue conduct red teaming?	How often does the venue conduct red teaming with a variety of mock items?
		Are qualified red teamers from outside the venue brought in?
		What is the detection rate required of screeners when red teaming?
		Do failures by security staff during red teaming result in the re-training of staff?
Monitoring	Do supervisors monitor screening performance?	Do supervisors intervene with screeners they observe conducting poor screening procedures?

Category	Stage 1 Metric	Stage 2 Metric
	Does management monitor supervisors?	-
Inspecting Employees, Vendors, Etc.	Are all media inspected?	Are all cameras and technology taken out of bags and checked (e.g. turned on and off)

Table 1.2: Final Conditional Metrics for Screening

Category	Stage 1 Metric	Stage 2 Metric
Patron Inspection – General	Do screeners conduct visual inspections?	-
	Are patrons asked to remove hats and open jackets?	Are supplemental patdown policies in place to secondary screen clothing which a patron does/will not remove?
	Are all patrons screened with the same precision and thoroughness? (There is no familiarity in screening.)	Are screening and inspection policies that are applied to regular patrons also applied to VIPs?
Bag Check	Are maximum bag size policies enforced?	What are the dimensions of the maximum allowable bag size into the venue?
Using Walkthrough Metal Detector Technology and Inspection	Do WTMDs have a reliable power source?	If WTMDs are battery operated, how often are they re-charged?
		If WTMDs are battery operated, how often are batteries replaced?
		If WTMDs are battery operated, how many hours is the battery rated to operate?
		Are screeners trained to know if the power to the WTMD is on or

Category	Stage 1 Metric	Stage 2 Metric
- continued – **Using Walkthrough Metal Detector Technology and Inspection** - continued -		not?
	Are WTMDs set at a security level which meets the NILECJ 0601.00 security level 2 or higher standard?	-
	Do WTMDs have visual and audio alarms?	What percent of alarms are missed by security staff?
	Is there a standard way of staffing WTMDs?	How many screeners are used to operate a single WTMD?
		Is there a "traffic cop" controlling the flow of patrons through the WTMD so that multiple patrons are not being screened at once?
Using Wanding and/or Patdown Inspection	Do screeners check a patron's upper body, both front and back of patron, down to and including the patron's ankles?	-
Incident Database	Are red teaming results recorded?	-
	Is contraband found within the stadium recorded?	Are contraband trends analyzed?
Inspecting Employees, Vendors, Etc.	Are all employees, vendors, contractors, etc. inspected?	-

Table 2.1: Final Essential Metrics for Credentialing

Category	Stage 1 Metric	Stage 2 Metric
Access Control Technologies	Does the venue deploy an access control system?	Is the credentialing and access control system design based on a risk assessment?
		Does the venue utilize technology (e.g. CCTV, guards) to monitor points of access?
		How many hours of CCTV video is archived?
		Is there a protocol for managing the CCTV storage which includes controlling personnel access?
		How many personnel have access to the CCTV storage?
		Does the venue utilize any "anti-piggybacking" / "anti-tailgating" technologies or resources to support the access control system at access control points in and around the venue?
		What percent of entry points to secure areas have access control technologies?
	Does the access control system include verification/inspection of credentials at access control points in and around the venue?	Does the access control system track/log who/which credential is attempting to access each point?
		Does the venue utilize a key card system which tracks credential usage?
- continued -	Does the venue have a cyber-security plan in place to support the protection of technology based system?	-

Category	Stage 1 Metric	Stage 2 Metric
Access Control Technologies - continued -	Does the venue have a procedure for accessing, using and tracking keys?	How many persons have access to a master key set?
	Does the venue require employees to check-in/out for work?	-
Technology Implementation	Does the venue track alarms/failures of the access control system?	Does the access control system provide immediate alarm to a centralized location when access is rejected or "attacked"?
		What is the average time for alarm to reach centralized location?
		Does centralized location have access and control over the CCTV System?
		Do alarms require the generation of a report as to why the alarm went off?
	Does the venue have response protocols in place to address technology failures and alarms during operations?	How long does it take for staff or staff operated CCTVs take to visually see the alarm/failure location?
Employee Hiring	Is risk associated with or considered for each hire/promotion at the venue based on job type/function and/or access requirements?	Are complete job descriptions created for each position at the venue?
	Are background checks completed for employees at the venue?	What percent of employees undergo a background check?
Credential Design & Issuance - continued -	Does the credential design have multiple identification features? - continued –	Does the credential have a photo displayed?
		Does the credential have a unique identification number, such as a barcode or employee ID number to distinguish individuals?

Category	Stage 1 Metric	Stage 2 Metric
Credential Design & Issuance - continued -	Does the credential design have multiple identification features? - continued –	Does the credential identify the individuals position/function at the venue?
	Does the credential design have non-transferable features?	How often are credentials re-designed?
		Does the access control system/credential program allow for remote deactivation of card swipe access? Are credentials issued for specific dates, times, events?
	Does the venue have policies and procedures in-place for issuing credentials and venue access to media, guests, contractors and vendors?	What percentage of guests are credentialed?
		What percentage of vendors are credentialed?
		What percentage of contractors are credentialed?
		Do those persons not credentialed but require access to the venue require preapproval and a temporary credential?
Employee Training & Monitoring - continued –	Does the venue implement a training program training their workforce (both venue employees and/or contractors) on the access control technology for which they will be required to use?	What percentage of staff are trained on use of the access control technology?
		What number of staff are trained to operate the CCTV?
		What percentage of staff are trained on communication procedures for communicating unauthorized access attempts?

Category	Stage 1 Metric	Stage 2 Metric
Employee Training & Monitoring - continued –	Does the venue train its workforce on its credentialing program?	Does the venue provide staff a way to communicate co-worker credential misuse?
	Does the venue have procedures for addressing employee misconduct?	Does the venue track employee misconduct?
	Are procedures/protocols in place with contractors should any contracted employee breach conduct and access control policies?	-
Employment Termination	Does the venue have procedures in place to collect materials such as expired/terminated credentials, uniforms, sensitive information?	Does the venue track and record lost, stolen, or deactivated and unreturned credentials?
	Is there an employee procedure for reporting lost or stolen credentials?	How many lost or stolen credentials does the venue have on record in the last calendar year?
	Does the venue have procedures to deactivate credentials which have barcode, card swipe or biometrics technologies?	How long does it take to deactivate a credential?

Table 2.2: Final Conditional Metrics for Credentialing

Category	Stage 1 Metric	Stage 2 Metric
Technology Implementation - continued-	Is the deployment of current and future access control technologies based upon a risk assessment?	Does the venue map the locations of its deployed access control system assets?
		How many points of access does your facility currently have within its system?

Category	Stage 1 Metric	Stage 2 Metric
Technology Implementation - continued-	Does the venue have a technology maintenance plan which follows vendor/manufacturer guidance and requirements?	-
Employee Hiring	Is there a decision process for determining the level or depth that a background check should be completed at?	What percentage of background checks includes criminal background checks?
		What percentage of background checks includes education and license verification?
		What percentage of background checks includes employment eligibility checks?
		What percentage of background checks includes drug screening?
		What percentage of background checks includes homeland security or terrorism checks?
	Is there a process for conducting re-checks of current employees?	-
	Are vendors/contractors required to undergo background checks?	-
Credential Design & Issuance	Does the credential design have anti-counterfeiting features?	Does the credential display a custom logo?
	Does the credential design have easily identifiable access level indicators?	How many access level indicator features are used?
		Are any access level indicator features easily discernable?
		Does the credential implement a system of letters, number and/or colors which indicate access rights?
		Has the venue established an access level hierarchy?

Category	Stage 1 Metric	Stage 2 Metric
Employee Training & Monitoring	Does the venue implement a human resource monitoring program?	Does the venue monitor and collect reports of negative or suspicious behavior?
		Does the venue have a way to anonymously report co-workers of misconduct or behavioral issues?
	Does the venue have policies and procedures in-place for responding to insider threats or reports of employee misconduct including attempted unauthorized access?	How often are the access control system and employee monitoring databases analyzed for threats?
		Is misuse of credentials terms for immediate termination?
Employment Termination	Does the venue have procedures for destroying credentials?	How many people are involved in the credential destruction process?
	Does the venue have a policy to notify staff at access control points in and around the venue and those responsible for record keeping of a terminated employee?	How long does it take for Human Resources to be notified of a contractor's termination?
		How long does it take for security to be notified of a contractor's termination?
		How long does it take for security to be notified of an employee's termination?

Table 3.1: Final Essential Metrics for Training

Category	Stage 1 Metric	Stage 2 Metric
Course Development	Are courses designed to reduce risk?	-
	Are courses developed based on job/task analysis of the position?	What percentage of employees who are involved in the WTMD inspection process take courses on WTMD screening?
		What percentage of employees who are involved in the Handheld Metal Detection Wands inspection process take courses on Handheld Metal Detection Wands?
		What percentage of employees who are involved in the bag inspection process take courses on bag inspection?
		What percentage of employees who are involved in the visual inspection process take courses on visual inspections?
	Do courses support best practices?	How many best practices do the courses support?
Instructional Process	Do training courses have defined course objectives?	Do courses outline performance standards?
		Does training require students to apply learned behavior?
Course Implementation	Are trainings provided in	Are trainings/courses updated

Category	Stage 1 Metric	Stage 2 Metric
	uniformity? (e.g. all materials are covered equally for each training course.)	annually?
		How often are courses and course materials updated?
		Are courses provided by qualified trainers?
		What qualifications are required of trainers for each course?
		Does the venue require attendance to trainings?
		How frequently are staff trained for each particular job/task/position?
		What is the number of training courses available onsite?
Testing of Training: Monitoring of Instruction	Do venues have a method for evaluating student performance?	Are trainees given a graded exercise/test on their knowledge?
		Are trainees given a graded exercise/test on their practice?
		Are procedures/criteria outlined for retesting individuals?
		Is documentation of grades/training maintained and available for inspection/review?
		How long are records about training course performance kept?
System of Administration/Records Management	Does the venue have an Administration/Records Management system for training record keeping?	-
Complaints Against Staff	Does the venue track	-

Category	Stage 1 Metric	Stage 2 Metric
	complaints against staff?	

Table 3.2: Final Conditional Metrics for Training

Category	Stage 1 Metric	Stage 2 Metric
Course Development	Are training courses based on institutional knowledge?	-
	Are courses inclusive of best practices from federal, state and local guidance resources?	-
Instructional Process	Does the course outline the level of instruction necessary for a successful class?	Is there an outline of the required contact hours?
		How many hours of training are required for each job/task/position?
		Are trainee to instructor ratios identified for each course?
		Are the classroom requirements outlined for each course?
	Do courses provide references to source materials (e.g. venue policies and procedures)	-
Testing of Training: Monitoring of Instruction	Does management provide oversight to supervisors?	-
- continued –	Do supervisors provide oversight to the implementation of instructions/trainings? - continued –	Are staffed removed (suspended/terminated) if they do not meet the standards outlined in training?
Testing of Training: Monitoring of Instruction - continued -	Do supervisors provide oversight to the implementation of instructions/trainings? - continued –	Does the venue track the error rate/proportionate reliability among staff?
		Are reports developed/reviewed from third party agencies

Category	Stage 1 Metric	Stage 2 Metric
		conducting "red teaming"/"secret shopper" programs?
		How frequently are staff tested using "red teaming"/"secret shopper" programs?