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

Homeland Security

Best Practices in Anti-Terrorism Security (BPATS) for Sports 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, posted on www.safetyact.gov.

.

OSAI subsequently asked CCICADA to undertake a research project on Economics of Security and Randomization. It was felt that some additional resource material was needed to assist private sector security managers with concepts and considerations as they develop proposals for funding for their venue security programs. We also wanted to increase their awareness of the potential benefits of incorporating aspects of a well-designed and well-executed randomization protocols as part of their overall security program.

As you review this Research Report, 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 Report is not a list of specific requirements, but a resource for venue owners, operators and security professionals to use as appropriate as they strengthen anti-terrorism security for their venues.
3. It is our impression that randomization protocols are not extensively used, and, as the Report indicates, there are some nuances to its effective incorporation into an overall layered security program. The recommendations contained in this Report were developed by the CCICADA research team following significant study of the available relevant literature and discussions with a number of security practitioners.
4. This Report was prepared with the professional sports and entertainment venues in mind. That does not mean, however, that ideas in this Report can be adapted to improve security at other venues.
5. A few final cautionary notes:
    a. Some recommendations contained in the Report may be good candidates for implementation at your venue. And some may not. We believe that your thoughtfulness and exercise of sound discretion will enable you to determine whether some of the material presented in this Report may be a good fit for your venue.
    b. By funding this project and by including this Report on our program website, neither DHS, the S&T Directorate, nor the Office of SAFETY Act Implementation is requiring implementation of any of the recommended actions as a requirement to obtain SAFETY Act coverage. Also, it is not our intent to suggest or imply that a sports league or corporate Best Practices program should be changed should aspects of this Report are at variance with a Best Practices program.

c. This Report is intended to be more of a “think piece” that will encourage security professionals to consider potential courses of action that could strengthen their anti-terrorism security program.

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

The Office of SAFETY Act Implementation

Science and Technology Directorate, DHS

Best Practices in Anti-terrorism Security (BPATS)
Tier III

Economics of Security and Randomization

September 2018

Command, Control and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security University Center of Excellence

Summary of Recommendations

Section 1 Recommendations: Economic Benefits and Costs of Security at Sports and Entertainment Venues

1.1. Costs and Benefits of Security Initiatives

Recommendation 1.1.1: Select specific security practices based on estimated risk reduction in overall risk, compared to costs.

Recommendation 1.1.2: While doing a full-fledged cost-benefit analysis of a security initiative is difficult due to many benefits and some costs being hard to quantify, it may in many cases as an initial step be more important to be able to identify subtle costs and, especially, benefits to security initiatives, such as unexpected enhancements of patron satisfaction, surprising workforce cost reduction, etc.

Recommendation 1.1.3: When considering a new security initiative, identify the threats being targeted and define the criteria for good performance prior to evaluation of the technology or process implementing the initiative.

Recommendation 1.1.4: Consideration of opportunity costs should be included in the full identification of costs of security.

Recommendation 1.1.5: When considering a new security initiative, consider its deterrent value when evaluating benefits, but be aware of evolving interpretation of metrics to measure deterrence.

Recommendation 1.1.6: When considering a new security initiative, weigh the costs and benefits of shifting the attention of an attacker from a strengthened area to another area.

Recommendation 1.1.7: Consider a Return on Security Investment (ROSI) approach. In attempting to do a ROSI calculation for planning purposes, engage experts from other domains to brainstorm threats and countermeasures, and attempt to rank them.

Recommendation 1.1.8: Consider lowering costs by renting new security technology, sharing equipment, or buying on a contingency basis, as opposed to purchasing outright.

Recommendation 1.1.9: When calculating return on investment of a security initiative, consider the costs avoided by implementing that initiative.

Recommendation 1.1.10: Be aware that security initiatives can enhance patron satisfaction and so can serve as a benefit.

Recommendation 1.1.11: Consider ways in which a new security initiative may reduce personnel costs

Recommendation 1.1.12: Making people aware of security in place can multiply the benefits of security initiatives.

Recommendation 1.1.13: Venue managers should explore quantifying the risk of terror attacks as well as the risk mitigation and consequence reduction strategies in their security plans as they negotiate terrorism insurance.

Recommendation 1.1.14: Scheduled and unscheduled site visits to venues by contractors or leagues to assess their security posture could help influence insurance access, premiums and other market components. (However, while beneficial, these visits can distract security and should be focused to have minimum interference.)

Recommendation 1.1.15: Venues should consider their nearby neighborhoods as an aid in enhancing patron satisfaction, a way to enhance security by extending the perimeter, as a potential place for shelter and reunification, and in awareness of threats from nearby facilities.

1.2. Patron Satisfaction

Recommendation 1.2.1: Patron satisfaction should be continually measured, but especially so when new or additional security measures are put in place to ensure that patron perceptions do not lean toward dissatisfaction. (Patron satisfaction is important, but should not deter effective security procedures. Patrons will learn to adapt, especially with effective communication provided to them.)

Recommendation 1.2.2: Providing information about waiting times and explanations for delays using signage and screens at the waiting areas, and offering entertainment to the customer during the waiting time, are examples of methods to enhance customer satisfaction while they wait on security lines.

Recommendation 1.2.3: Providing incentives for arriving at a venue early can minimize vulnerability of patrons lining up for inspection and improve screening effectiveness by reducing screener fatigue during a late surge. These incentives, if they increase attendance, or encourage patrons to consume more products because they are there longer, may pay for themselves.

Recommendation 1.2.4: Continued development of, education in the use of, and deployment of social media monitoring software at venues is important to enhance the overall security plan and assist with enhancing the overall patron experience.

Recommendation 1.2.5: Train security to show empathy and explain/demonstrate the randomized nature of a process.

Recommendation 1.2.6: An observable (transparent) process reduces the chance of perceived bias or profiling.

Recommendation 1.2.7: Reframe the way patrons perceive random selection from bad to good luck.

Recommendation 1.2.8: Use psychological cues and interventions to decrease patrons' perception of waiting time.

Recommendation 1.2.9: Segmenting patrons can enable better utilization of resources and decrease average waiting time.

Recommendation 1.2.10: Develop and validate satisfaction scales that explicitly capture security.

Section 2 Recomendations: Randomization Designs

2.1. General Observations about Randomization

Recommendation 2.1.1: Randomization is just one part of an overall security plan. New investments, including randomization, should be evaluated as part of a holistic security view.

Recommendation 2.1.2: Consider various goals of randomization including deterrence, monitoring operational effectiveness, keeping employees alert, and doing a job partially when doing it fully is not feasible or recommended.

Recommendation 2.1.3: How randomization is applied will depend upon the goal. The first step in implementing a random security protocol should be to assess what you are trying to protect against or otherwise accomplish. What is the goal: to deter an adversary or detect an item?

Recommendation 2.1.4: Apply randomization in many ways.

Recommendation 2.1.5: Randomization should not replace “check all” (in screening and other processes) unless the venue cannot afford to check all. Randomization can enhance 100% checking as an added process. There are certain exceptional cases where the value of obfuscation and its deterrent effect might make randomization the preferred choice over 100% implementation, but such cases must be thoroughly analyzed.

Recommendation 2.1.6: Adding a randomized secondary check improves security in two ways: It raises the detection rate through catching more on a second try, and the visible additional security has some level of deterrent effect.

Recommendation 2.1.7 Adding a randomized secondary check improves security by giving an indication of the ”miss rate.”

Recommendation 2.1.8: Randomization should be geared to the type of event, threat level, and number of events that are conducted at a venue.

Recommendation 2.1.9: Randomization requires documented procedures and easy execution to ensure consistency.

Recommendation 2.1.10: All kinds of randomization require training.

2.2. Recommendations Arising from Randomization in Other Sectors and Settings

Recommendation 2.2.1: Having a collection of possible security plans (a Playbook) from which to choose from for each threat level, and choosing one of them randomly for each event or randomly choosing a day for each to be run, is a promising idea for sports and entertainment venues.

Recommendation 2.2.2: A venue should consider sharing expensive technologies and specially trained personnel (e.g., trace explosive detection swabs, X-ray machines, highly trained K-9s) with other venues or organizations on a random basis.

Recommendation 2.2.3: Determine the legal authority required to effectively implement a security randomization initiative.

Recommendation 2.2.4: For "sophisticated randomization" tools to be successfully implemented at sports and entertainment venues, the implementation must be simple with the complex math in the background, and there needs to be close collaboration between technical developers and users in order to inform the complex math required.

Recommendation 2.2.5: If the goal is to develop tools for randomization that are adopted widely and are easily applied/modified for use at all kinds of sports and entertainment venues, simple tools of randomization are likely a best way to start implementing randomization for venue security

2.3. Summary of Ideas for Randomization in Sports Stadiums

This section has a detailed summary of ideas for randomization. Recommendations are reserved for Sections 2.7 and 3.1.

2.4. Assessing the Effectiveness of Randomization

Recommendation 2.4.1: In assessing the effect of randomization as a deterrent, take into account that, at least after an initial increase, concrete measures such as contraband caught might decrease

Recommendation 2.4.2: In using metrics to assess the effect of randomization, take into account relevant factors such as size of crowd, level of effort devoted to screening, and the weather.

Recommendation 2.4.3: Utilize simulation and other tools to understand the potential practical effect of a security initiative before implementing it, as well as to understand the potential practical impacts of implementation.

2.5. Recommendations on Randomization in Patron Screening Resulting from Simulation Experiments

There are no recommendations in this section; but see Recommendation 2.4.3.

2.6. Employee Background Checks

Recommendation 2.6.1: Ensure that the organization has necessary legal authority to conduct repeat (random) background checks.

Recommendation 2.6.2: Conduct randomized rechecks over a defined time period, ensuring that each employee is selected at least once by the end of the period.

Recommendation 2.6.3: Each employee should have equal chance of selection during a testing period. (Do not remove an employee from the testing pool because they were selected in a previous pool.)

Recommendation 2.6.4: Randomly select employees for more in-depth background screening.

Recommendation 2.6.5: Randomly verify that third party vendors/contractors are conducting required background checks.

Recommendation 2.6.6: Have a developed and clearly defined process and written policy concerning conducting background checks.

Recommendation 2.6.7: Random selection methods should be scientifically valid and the randomness of the selection method must be verifiable.

Recommendation 2.6.8: Ensure employee privacy.

Recommendation 2.6.9: Do not discard a selection without adequate explanation.

Recommendation 2.6.10: Distribute the tests reasonably throughout the year.

Recommendation 2.6.11: Refresh the pool of employees before each random selection.

Recommendation 2.6.12: Retain and maintain records and maintain testing pool.

2.7. Best Practices for Randomization

Recommendation 2.7.1: There is a continued need to identify practical and logistical issues to aid venues in finding ways to initiate randomization.

Recommendation 2.7.2: There is a need to develop procedures for security director and event staff training in randomization practices.

Recommendation 2.7.3: A list of potential randomization practices with which to initiate randomization at sports and entertainment venues consists of the following practices (codes refer to full list of randomization practices in the Appendix):

- Randomly check personnel IDs during the working day (E2).
- Randomly check person matches face on badge (E4).
- Have security management randomly visit various posts and functions (P2).
- Randomize perimeter patrols with qualified personnel (P3).
- Schedule red teaming probes of quality randomly by location (S2).

- If there are explosive-detecting canines, have them walked randomly through parking areas (S5).
- At a checkpoint randomly select some cars for explosives check (by under-carriage mirror or canine) (S8)
- Schedule visible police presence near venue, and request random pattern, timing or location to increase deterrence and avoid countermeasures. (S10)

Section 3 Recommendations: Practical Implementation of Simple Randomization for Patron Screening

3.1. Best Practices for Implementation

Recommendation 3.1.1: There is a continued need to identify practical and logistical issues to aid venues in finding ways to implement randomization in practice.

Recommendation 3.1.2: There is a need to develop procedures for security director and event staff training in randomization implementation methods.

Recommendation 3.1.3: Venues should use an implementation procedure for randomized screening (secondary screening) that is easiest to implement in their context and achieves the goals of minimizing patron perception of bias.

Recommendation 3.1.4: Venues should experiment with the idea of developing a set of security practices/protocols (a Playbook) that are available for random implementation on a given day/event.

3.2. Patron Perception

Recommendation 3.2.1: Brand and insert into the organizational culture (and continually reinforce) that the organization and its security procedures are “just, fair, protective, etc.”

Recommendation 3.2.2: Keep patrons informed about and engaged in security protocols and procedures.

Recommendation 3.2.3: Minimize risk of perceived bias through employment of a perceptibly diverse security staff and ensuring that the selection process (for additional screening) is easy to understand and “predictably unpredictable” (i.e. random).

Recommendation 3.2.4: Ensure that the staff consistently receives diversity and de-escalation training and encourage personnel to be personable and friendly as they explain imminent security procedures.

3.3. Behavioral Issues

Recommendation 3.3.1: Use of behavioral triggers for enhanced patron screening can begin well away from the venue itself.

Recommendation 3.3.2: Implementation of behavioral triggers for enhanced patron screening can involve processes other than specific screening protocols such as use of WTMDs, wands, or explosive swabs.

Recommendation 3.3.3: Because the “science” and the “practice” of using behavioral indicators is changing, venue security directors should seek to get the latest information before utilizing them.

Recommendation 3.3.4: Venues need to be aware of vulnerabilities potentially caused by protocols for family group screening.

Recommendation 3.3.5: If groups arrive together and one member of the group is chosen for secondary screening, the venue needs a carefully-thought-out policy for where other members of the group stand during the secondary screening so as not to interfere with other screening activities.

Overview and Key Concepts

Background

Our nation's sports and entertainment venues (stadiums, arenas, etc.) host millions of patrons annually, form the basis for a multi-billion dollar industry, and present an inviting target for terrorists, as illustrated by the November 2015 attack on the Stade de France in Paris and the May 2017 attack at an Ariana Grande concert at the Manchester Arena. In 2012, the DHS Office of SAFETY Act Implementation (OSAI) commissioned the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) to do a research project, "Best Practices in Anti-terrorism Security" (*BPATS I*) for sporting and entertainment venues, which presented the important components of a sports and entertainment venue anti-terrorism security plan. BPATS I resulted in a guide "BEST PRACTICES in Anti-Terrorism Security for Sporting and Entertainment Venues RESOURCE GUIDE." This *BPATS Guide*, completed in 2013, is available from OSAI at: https://www.safetyact.gov/pages/homepages/SamsStaticPages.do?path=sams\pages\BPATS.

A follow-up project by CCICADA, BPATS II, completed in 2015, focused on metrics for anti-terrorism security at sports and entertainment venues and generated more quantitative measures to extend and improve the simple Yes/No metrics that are predominant in the BPATS Guide. The suggested protective measures/metrics arising from it have been incorporated into an OSAI Best Practices Matrix with the relative assignments such as suggested, recommended, or strongly recommended which can be employed in response to various current and potential threats. (See https://www.safetyact.gov/externalRes/refdoc/Matrix.pdf.)

Following the 2015 Paris attacks, CCICADA convened a conference at MetLife Stadium to discuss stadium security post-Paris. A major theme arising from that conference was the economic value of randomization in all aspects of security. (Randomization is not as simple as "every 4th patron." It can be innovative and as complex as a venue security director can make it, as this report aims to show.) The theme of randomization led to BPATS III, a research project focusing on the economic benefits and costs of security at sports and entertainment venues, on randomization designs, and on practical implementation of simple randomization for patron screening. This report on BPATS III will succeed if they help the overall sports and entertainment venue security community to understand the potential for increased security from randomization of all aspects of venue security, and to find ways to assess the economic costs and benefits of security initiatives of all kinds, with an emphasis on randomization.

This report focuses on professional sports and entertainment venues. Other venues or organizations hosting running races or automobile races or outdoor concerts have special issues to which not all of the ideas in this report apply, e.g., having no or limited access control. Nevertheless, many of the ideas in this report can be adapted to improve security at events like these.

Context

During the course of this research project, the threat environment for large venue security changed in significant ways, as there is increased awareness to areas "beyond the perimeter."

Some general principles of security at large venues remain basic. For example:

- No security plan is cast in stone. It should be reviewed regularly as resources, capabilities, threats, technology, and intelligence change.
- Do not put all your eggs in one basket – security plans must be diverse and flexible; randomization is just one piece.
- Extend the perimeter: security plans should have concentric layers; layers may be handled by different agencies or authorities, but should be coordinated.

Description of CCICADA

The Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) is a Department of Homeland Security University Center of Excellence (COE) based at Rutgers, the State University of New Jersey and has 17 academic and industrial partners as well as numerous collaborators in the homeland security enterprise. CCICADA has been involved with sports and entertainment venue security almost since its inception in 2009.

Section 1: Economic Benefits and Costs of Security at Sports and Entertainment Venues

Sports and entertainment venue ownership and management have a need for tools and methods to help them understand the economic benefits of security enhancements that may impact insurance costs, business risk and/or patron satisfaction or loyalty. Also needed is a way to demonstrate that increased security may lead to increased patron satisfaction in spite of the need for changes in how security engages the customer. Similarly they have a need for the improvement of security, e.g., through inspection processes and credential checking.

1.1. Costs and Benefits of Security Initiatives

An extensive review of literature as well as discussions with subject matter experts (SMEs) have been conducted, focused on methods to understand the economic impacts and return on investment (costs and benefits) of security initiatives. Here we describe ways to determine recommended practices for analyzing costs and benefits of security initiatives, with inspection and credentialing as specific cases in point, and describe selected good practices.

In contrast to risk assessment and mitigation, which are well-developed, quantifiable disciplines, the costs and benefits of security initiatives have not been well researched. (There are some exceptions, e.g., in some parts of the transit industry.) A key difficulty is that economics requires specific calculations such as the "Risk Equation": Risk = Threat x Vulnerability x Consequences. This requires all three factors to be accurately estimated. But there is no data on the incidence of terrorist attempts on US sporting venues (making Threat hard to estimate); estimates that an attack will succeed (vulnerability) are essentially speculation; and estimates of consequences arise largely from abroad and are large, which makes it important to be able to estimate probabilities accurately. Still, thinking in terms of risk reduction is recommended when analyzing the potential costs and benefits of a security initiative.

Recommendation 1.1.1: *Select specific security practices based on estimated risk reduction in overall risk, compared to costs.*

This is not easy to accomplish. The development of visual aids that will take a lot of information and distill it into a quick reference chart can help venue security directors to do risk reduction and other cost-benefit calculations. There is so much information being directed towards security directors that any time-saver will help.

In general, the topic of cost-benefit analysis of security initiatives is not very well developed, and even less so in the sports and entertainment venue area. What we offer here are some specific ideas that we recommend as good practices in seeking to lay out and analyze the costs and benefits of sports and entertainment venue security. However, we have been led to the conclusion that no specific practices are well enough developed to be recommended as "best practices" for cost-benefit analysis of security at venues. One security director at a transit agency that attempts to do detailed cost-benefit analysis told us that such cost-benefit analysis is especially important in long-term strategic planning, as opposed to development of tactics/operations. One basic conclusion is that a detailed quantitative analysis of costs and benefits may not be as valuable as the ability to identify costs and, especially, security benefits that are not easily identified, let alone measured. This may not be true for those industries in which numerical cost-benefit analysis is already well established (as in some parts of the transit industry), but it is likely the case in the sports and entertainment venue realm where even an identification of costs and benefits is a needed first step. Some examples of these are described in this section.

Recommendation 1.1.2: *While doing a full-fledged cost-benefit analysis of a security initiative is difficult due to many benefits and some costs being hard to quantify, it may in many cases as an initial step be more important to be able to identify subtle costs and, especially, benefits to security initiatives, such as unexpected enhancements of patron satisfaction, surprising workforce cost reduction, etc.*

Our work with one venue on assessment of benefits of a drone detection system has been instructive. The cost of a proposed system is known. The measurement of benefits depends upon goals set by the venue. Do we want 95% probability of identifying that there is a drone or drone controller being used within a certain amount of time? Of identifying the drone operator location within a certain amount of time? Within a certain distance? Of identifying where the drone is traveling? And so on. Clearly the issue is complex, but it starts by defining the criteria for good performance (avoidance of consequences) and the perceived threat precisely.

Recommendation 1.1.3: *When considering a new security initiative, identify the threats being targeted and define the criteria for good performance prior to evaluation of the technology or process implementing the initiative.*

Costs. Costs of security initiatives include lifecycle costs of hardware or software, costs of increased personnel and training, and costs of informing the public about those initiatives. These are relatively easy to measure. Indeed, security is often carefully budgeted and costs tracked. Not so easy to quantify are "opportunity costs." What other item(s) or investments am I not making now because of my use of resources on a particular new security approach?

Recommendation 1.1.4: *Consideration of opportunity costs should be included in the full identification of costs of security.*

Benefits: Deterrence. Benefits are much harder to quantify than costs. While security initiatives are often initiated to "catch bad things," the primary benefit of increased security at sports and entertainment venues might be its contribution to deterrence. Many venue security managers told us that "show of force" likely had a deterrent effect, even if that is hard to measure. It is argued that terrorists are rational in their decision making because they are focused on success and are otherwise risk averse, so if a security initiative leads to confusion and uncertainty, terrorists will be deterred. One potential concrete metric for benefits is the amount of contraband collected before security screening. Looking in the bushes at a prison on visitation day, we are told, one finds many items people were afraid to try to bring in. However, since deterrence seeks to tip the "pain-pleasure" balance toward the "pain" side, if deterrence is working, there may actually be less contraband over time once security protocols have been deployed. The goal of deterrence is to reduce the benefits or increase the costs to an adversary. Another complication in measuring the benefits of deterrence is that if increased security is working and deterring an attack, it may just shift the attention of the attackers elsewhere (e.g., the outside of the venue as in the Manchester attack), thus requiring additional security initiatives. Thus, the overall costs and benefits may have to be viewed more broadly than to concentrate on a particular initiative. Finally, while most people we interviewed felt that deterrence was difficult to measure, one person from another industry said that they do detailed numerical estimates of deterrence as a function of attractiveness of a target.

Recommendation 1.1.5: *When considering a new security initiative, consider its deterrent value when evaluating benefits, but be aware of evolving interpretation of metrics to measure deterrence.*

Recommendation 1.1.6: *When considering a new security initiative, weigh the costs and benefits of shifting the attention of an attacker from a strengthened area to another area.*

Why Benefits are Hard to Determine. Some reasons our interviewees gave for why benefits are difficult to describe let alone quantify are of interest.

- If a camera helps you win a lawsuit from an unruly fan, how much of the benefit can you attribute to the camera?
- Usage year to year of text messaging for fan complaints has gone down; does this mean people have gotten used to security initiatives?
- Social media tools can track incidents by type, but do they show which component of security leads to reduction in incidents?
- You can keep track of items confiscated, but it is hard to interpret the meaning of an increase or decrease. More threats? Better detection? Deterrence?

Some venue managers take the position that investing in security is a strong goal and practice, they feel it is important for protecting "the brand," and feel that it is cheaper to deal with security in advance than after an incident. More typical is for costs to run the funding of security initiatives, capped by budget constraints, with benefits only described in general, not quantitative terms. There is little evidence of cost-benefit analysis being done by venues – at least not in a formal sense.

The concept of "Return on Security Investment" or ROSI goes back to Sonnenreich, et al. in 2006 (SageSecure LLC) and is meant to be analogous to return on investment, or ROI. (The following website provides an online ROSI calculator: https://advisera.com/27001academy/free-tools/free-return-security-investment-calculator/.) ROSI depends critically on the assumptions made as to what benefits and costs appear, and difficulties of using it include omissions, optimistic assumptions about costs or benefits, etc. The effect of these complications can be minimized by engaging experts from other domains in a ROSI calculation. [Note: this description is meant to provide information resulting from research but does not represent an endorsement of this tool by CCICADA.]

Recommendation 1.1.7: *Consider a Return on Security Investment (ROSI) approach. In attempting to do a ROSI calculation for planning purposes, engage experts from other domains to brainstorm threats and countermeasures, and attempt to rank them.*

Examples of Cost-Benefit Analysis. We did learn from practitioners of some interesting examples of cost-benefit analyses and specific ways to measure benefits of security initiatives.

- Rent vs. Buy: Venues with infrequent events often conclude that rental of equipment is more cost beneficial than purchase, making their implementation possible. Leasing or renting is becoming a more appealing option because technology is moving faster than the life cycles of the current technology.
- Equipment Sharing: Share with another nearby or partner venue to increase the availability and use of security equipment.
- Contingency Purchase: When benefits of a new security technology are unclear, the venue can purchase a system on a contingency basis with the vendor organization installing the system at their cost and the venue purchasing it if the performance meets agreed-upon standards of performance.

- ROSI (Background Checks): Multiple studies assert that there is a positive return on investment of some three times an employee's salary for pre-hire background checks. Calculation of return on investment includes money saved by avoiding problems.
- The implementation of randomized patrolling on the roadways at a major airport is reported to have led to capturing more contraband (but see Recommendation 1.1.5) and to fewer hours of overtime by security personnel. So a security initiative does not have to increase personnel costs.
- The implementation of randomized ticket checking on a rail system is reported to have led to catching more fare beaters and also savings in terms of time spent choosing a location for ticket validation checking.
- Those running races on city streets understand that extra security and road closures have an impact on the community, but the costs to the community and the costs of security are widely overcome by the substantial economic benefit of the event to the community. This cost-benefit analysis is labeled a key reason why the city wants to run the event.
- Benefits can be multiplied (a force multiplier) by making people aware of the security in place. Some stores place monitors near main cameras and in some big box hardware stores they have a motion sensor sing to make patrons aware of the camera. One venue security manager told us about instructions to security staff to make themselves visible at each stoppage of play by walking up and down the aisles – it made patrons think that security had increased.
- In many venues, the patrons expect security and the benefit is an unmeasured contribution to patron sense of well-being.

Recommendation 1.1.8*: Consider lowering costs by renting new security technology, sharing equipment, or buying on a contingency basis, as opposed to purchasing outright.*

Recommendation 1.1.9*: When calculating return on investment of a security initiative, consider the costs avoided by implementing that initiative.*

Recommendation 1.1.10: *Be aware that security initiatives can enhance patron satisfaction and so can serve as a benefit.*

Recommendation 1.1.11: *Consider ways in which a new security initiative may reduce personnel costs.*

Recommendation 1.1.12: *Making people aware of security in place can multiply the benefits of security initiatives.*

Insurance Costs. Our study considered the possible benefits of security enhancements on insurance costs: reduced premiums, decreased deductibles, increased coverage. In spite of industry guidance to ask for premium reductions in balance with increased SAFETY Act certified products and services (Business Insurance, 2005), we found no examples of such reductions or other adjustments. However, we learned that some believe that the cumulative impact of more and more sports and entertainment venues getting SAFETY ACT–certification/ designation or even just improving security processes will eventually have an impact on insurance. It should be emphasized, in addition, that even if insurance costs do not improve, the effort to attain SAFETY Act coverage should lead to improved security.

Interviews with security officials responsible for settings other than stadiums and entertainment centers and with their risk consultants suggest a possible approach for stadium management to take when negotiating with insurance carriers. In such negotiations, the quantification of risk and the steps taken to reduce the risk appear to carry much weight. One approach that has worked in other settings is to provide risk quantification using "exceedance curves," i.e. curves plotting the probability that a loss will exceed a certain amount. While an in-depth treatment of methods of risk quantification is beyond the scope of this project, we note that without such attempts at quantifying risk, insurance carriers are likely to be very conservative in their pricing.

Recommendation 1.1.13: *Venue managers should explore quantifying the risk of terror attacks as well as the risk mitigation and consequence reduction strategies in their security plans as they negotiate terrorism insurance.*

Recommendation 1.1.14: *Scheduled and unscheduled site visits to venues by contractors or leagues to assess their security posture could help influence insurance access, premiums and other market components. (However, while beneficial, these visits can distract security and should be focused to have minimum interference.)*

<u>Considering the Costs and Benefits to Surrounding Areas</u>. The project team sought to understand the extent that venue security managers consider costs and benefits to surrounding areas when determining their security initiatives. One venue offers free beer coupons at establishments near the venue – using partnership with the community to aid in enhancing patron satisfaction. (A venue security manager pointed out that partnerships with the community have the benefit of enhanced information sharing opportunities.) Another designed its new facilities with enhancement of surrounding areas in mind – both to improve the neighborhood and to act as a security buffer. As noted above, an organization that runs marathon races seeks to minimize the impact of security and street closures with publicity and signage.

Every sports and entertainment venue should have a gathering place for evacuees. In addition to considering costs and benefit to the nearby neighborhood, a venue security manager could look at ways to utilize that neighborhood as a place for shelter or reunification in case of an emergency.

Recommendation 1.1.15: *Venues should consider their nearby neighborhoods as an aid in enhancing patron satisfaction, a way to enhance security by extending the perimeter, as a potential place for shelter and reunification, and in awareness of threats from nearby facilities.*

1.2. Patron Satisfaction

As this project started, it seemed that many sports and entertainment venue business managers might view security procedures as having a potentially negative impact on patrons' experiences. However, we found through interviews about surveys venues had used that for the most part, patrons were not unhappy with increased security, and actually were happier with it. One venue security manager told us they got complaints for the first 15 or 20 events after increasing security, but now only get one or two a year. Another told us that patrons occasionally complain about lines if they arrive too close to the beginning of a game, but generally understand that late arrival means they might miss the start of the event. Venues occasionally get complaints about profiling, and some that have not tried randomization worry that random selection might be (mis)perceived as profiling. However, there are practices to minimize these kinds of perceptions (see Sec. 3.2).

Patron satisfaction is dynamic and although to date, increased security measures have on balance been viewed favorably, venue managers do not know when additional processes will tilt patron satisfaction to the unfavorable side. Still, several venue security directors emphasized that while patron satisfaction is important, security is still the bottom line and security concerns need to underlie security plans.

Recommendation 1.2.1: *Patron satisfaction should be continually measured, but especially so when new or additional security measures are put in place to ensure that patron perceptions do not lean toward dissatisfaction. (Patron satisfaction is important, but should not deter effective security procedures. Patrons will learn to adapt, especially with effective communication provided to them.)*

Literature on Patron Satisfaction. There is a lot of literature on patron satisfaction in a variety of industries. Among the key components of overall satisfaction are perceived waiting time, perceived fairness, and atmosphere, parking, staff attitudes, and food. Security, however, is not recognized by existing scales that measure satisfaction. The study of the psychology of waiting time tells us things like: Uncertain waits are perceived as longer than known, finite waits; unexplained waits are perceived as longer than explained waits; unfair waits are perceived as longer than equitable waits; and occupied waiting time is perceived as shorter than unoccupied waiting time. Among other things, this suggests providing information about waiting times and explanations for delays, using signage and screens at the waiting areas, and offering entertainment to waiting customers. One venue security manager told us about providing jugglers and other entertainers, another told us about venues that provide video monitors and, among other things, put up trivia questions, and a third told us about having a guest services "street team" for waiting patrons to answer queries about delays and procedures. (Not everyone we interviewed felt that entertaining customers waiting in line was that important since people seem to accept the need for security.) In another part of relevant literature, the theory of service fairness tells us that organizations failing to project an image of service fairness cannot develop the level of customer confidence needed to establish loyalty. This implies that it is critical to introduce randomization in such a way that perceived service fairness is kept in mind and to train security personnel to apply a randomization process properly.

Recommendation 1.2.2: *Providing information about waiting times and explanations for delays using signage and screens at the waiting areas, and offering entertainment to the customer during the waiting time, are examples of methods to enhance customer satisfaction while they wait on security lines.*

Surveys. Some sports and entertainment venues use "secret shoppers" to assess patron experience getting into the venue and ask other security-related questions. Others do customer satisfaction surveys. One venue security manager reported that 100% of survey respondents said that WTMDs made them feel safer or at least as safe as before; 11% felt that WTMDs made entry slower than expected and some complained about that; and one person complained about the need for children to go through WTMDs. We reviewed earlier surveys of security at sporting events. At the 2002 FIFA World Cup, security was not significant in respondents' decisions to travel to the World Cup, but, once there, a significant proportion was conscious of the safety measures. The general perception was that World Cup organizers' tight security did not detract from tourists enjoying the soccer competition. At the 2003 Rugby World Cup**, s**ecurity measures were judged sufficient and attendees were not deterred by the threat of terrorism.

Incentives. We also investigated whether there were relatively inexpensive incentives that patrons would accept in exchange for the general inconvenience caused by increased security. Of specific benefit are incentives that encourage patrons to arrive early. Most of those interviewed hadn't thought of providing incentives/rewards for extra screening or arriving early. We explored a variety of such incentives (low-priced beer, give-aways for early arrivals, reduced parking fees, entry in lotteries for prizes, ability to go on the field before the game, etc.) and developed some tools for analyzing the costs and benefits of such incentives, noting that sometimes the cost of such incentives can be offset by extra income for the venue. Thus the security benefits, reducing vulnerability in the unsecured area arising from patrons lining up for inspection, and reducing screener fatigue during the late surge, are obtained at zero or low cost. Some venue security managers reported that traffic and mass transit schedules and time of getting out of work limit the number of people who can arrive early, and some felt that it would be too difficult to get their patrons to change their ways. From those that have tried such incentives, we note one caution: A dual peak arrival may bring the need to allocate staffing resources in a different way, with more staff needed earlier.

Recommendation 1.2.3: *Providing incentives for arriving at a venue early can minimize vulnerability of patrons lining up for inspection and improve screening effectiveness by reducing screener fatigue during a late surge. These incentives, if they increase attendance, or encourage patrons to consume more products because they are there longer, may pay for themselves.*

Social Media. We looked into the use of social media as a tool to measure patron satisfaction and extended our inquiries to examine its role to aid security practitioners. Responses from venue managers include utilization to enhance a security plan, enhance patron satisfaction and develop/test marketing metrics to enhance the patron experience. Several venues primarily use social media tools to provide early warning of a potential security threat based on tailored "key word" search parameters. Hits are relayed to law enforcement personnel for further investigation and mitigation, as deemed appropriate. Other venues utilized social media tools exclusively for marketing or to identify patron satisfaction relative to vendor services, security entry procedures, parking availability, ticket prices and overall patron experience, to name a few. Social media applications and use continue to evolve as a mainstream method of communications and interaction and have broad implications to potentially provide real time actionable response to emerging security threats as well as identifying patron satisfaction. Already social media and related technology are used by patrons to order food or souvenirs at a seat or even in the parking lot, to look at replays, to communicate with security, etc., and who can predict what future uses will be? There is good reason to integrate social media apps and security.

Recommendation 1.2.4: *Continued development of, education in the use of, and deployment of social media monitoring software at venues is important to enhance the overall security plan and assist with enhancing the overall patron experience.*

Based on a review of marketing and behavioral science literature and interviews with practitioners, we make the following recommendations for improving patron satisfaction with security processes, and in particular with randomization. It should be noted, however, as one venue security manager told us, that some things are beyond the control of the venue. In particular, in sports stadiums, you are likely to get more complaints if the home team is losing.

<u>Recommendations for Improving Patron Satisfaction with Security Processes</u>

Recommendation 1.2.5: *Train security to show empathy and explain/demonstrate the randomized nature of a process.*

We heard the story of a person who was chosen three days in a row for extra screening at the entrance to an amusement park, and whose children thought their father had done something wrong and were very upset about it when security could not explain why he had been chosen.

Recommendation 1.2.6: *An observable (transparent) process reduces the chance of perceived bias or profiling.*

Moreover, showing that you are doing things randomly decreases likelihood of attack due to the deterrent effect.

Recommendation 1.2.7: *Reframe the way patrons perceive random selection from bad to good luck.*

Can we compensate those chosen with a "reward" such as entry into a lottery?

As noted above, some venues offer entertainment while people are on line. This is one example of an intervention that decreases patrons' perception of waiting time. More generally, we have the following recommendation.

Recommendation 1.2.8: *Use psychological cues and interventions to decrease patrons' perception of waiting time.*

It may make for better utilization of resources to have people with no bags go through a separate lane with faster flow and lower staffing needs. A number of venues do this. With adequate preparation, one could also include true season ticket holders in special lanes. These observations lead to the next recommendation.

Recommendation 1.2.9: *Segmenting patrons can enable better utilization of resources and decrease average waiting time.*

After reviewing the scarcity of validated instruments that measure the impacts of security procedures on patron satisfaction, we recommend that fundamental and applied research in this area be encouraged.

Recommendation 1.2.10: *Develop and validate satisfaction scales that explicitly capture security.*

Section 2: Randomization Designs

In the BPATS I Best Practices Resource Guide, CCICADA suggested randomization as a best practice in a variety of areas. For example, the patron screening process can include a procedure in which patrons can be randomly chosen for more (or less) rigorous inspection. Similarly, security officers can be deployed according to randomized schedules, and employees can be randomly chosen for background re-checks. Simple and complex randomization designs have been used in other settings to make better use of security resources and to increase levels of deterrence by making it more expensive for an adversary to guess a defensive strategy. This project was partly motivated by the need to understand how well this has worked, and the need for ways to judge the effectiveness of such randomization designs. It was also partly motivated by crucial implementation issues (see Section 3): security personnel may not utilize or even understand all of the ways simple randomization can help; they may fear leaving decision to "a coin toss," while patrons might fear or perceive that bias or improper profiling is driving some randomized screening techniques.

2.1. General Observations and Recommendations about Randomization

It is important to emphasize that randomization is just one part of an overall security plan. The threat environment is constantly changing and evolving and the venue security community is evolving with it. New initiatives require a combination of planning, threat awareness, training, and implementation of new methods and technologies. New investments, including randomization, should be evaluated as part of a holistic security view.

Recommendation 2.1.1: *Randomization is just one part of an overall security plan. New investments, including randomization, should be evaluated as part of a holistic security view.*

Goals of Randomization: Randomization aims at making it more complicated/confusing/ expensive for adversaries, which acts as a deterrent. Virtually all the experts we consulted mentioned this as a key goal of randomization. However, there are other goals: monitoring operational integrity (e.g., by randomly rechecking credentials of employees); stimulating the capability or alertness of security personnel (e.g., through use of red-teams); achieving intermediate levels of security when threat intelligence and/or budget considerations do not recommend 100% application (e.g., when inspecting some fraction of persons or covering part of a venue with cameras is better than not doing anything). Randomization can keep your employees alert, but sometimes the emphasis on randomness can be distracting; therefore it is important to mix in enhanced search (e.g., a focus on specific threats).

Recommendation 2.1.2: *Consider various goals of randomization including deterrence, monitoring operational effectiveness, keeping employees alert, and doing a job partially when doing it fully is not feasible or recommended.*

Recommendation 2.1.3: *How randomization is applied will depend upon the goal. The first step in implementing a random security protocol should be to assess what you are trying to protect against or otherwise accomplish. What is the goal: to deter an adversary or detect an item?*

Sometimes randomization can be based on quite sophisticated methods having their basis in complex game theory models that assume that adversarial strategies make use of knowledge about venue strategies. In Section 2.2, we discuss examples from security at airports, harbors, light rail, etc. that make use of such sophisticated game-theoretical methods. As a general rule, however, simple randomization may be easier to implement and accomplishes the "unpredictability" purpose.

Randomization can be applied to the patrons, to the security camera monitoring, to the pre-game venue inspections, access control, badge verification, etc. It should *not* be focused on only one part of the security profile.

Recommendation 2.1.4: *Apply randomization in many ways.*

It is well recognized that no security initiative is perfect. Randomization may allow you to do more at less cost, but of course may also "catch" less. Since the goal is to maximize the probability of "catching" bad things (or preventing them), the feedback we have gotten is that randomization should not replace doing something 100% of the time if the venue can afford it. As an example, the professional leagues all want 100% inspections. When some venues "ramped up" with only randomized inspections, their patrons asked for more (and security directors were more comfortable doing more). However, it should be noted that any added screening, particularly when applied randomly, raises the adversary's costs. Conceivably, the deterrent effect (if it could be measured) might make randomization preferred to 100% checking.

Recommendation 2.1.5: *Randomization should not replace "check all" (in screening and other processes) unless the venue cannot afford to check all. Randomization can enhance 100% checking as an added process. There are certain exceptional cases where the value of obfuscation and its deterrent effect might make randomization the preferred choice over 100% implementation, but such cases must be thoroughly analyzed.*

While "check all" is the standard in professional sports, at least in terms of screening, this recommendation may even apply to certain aspects of screening, and may also apply to other processes besides screening, e.g., check of employee ID badges. (One venue security director told us that, with the turnover in event staff, ID badges often go missing or get "handed around.")

Recommendation 2.1.6: *Adding a randomized secondary check improves security in two ways: It raises the detection rate through catching more on a second try, and the visible additional security has some level of deterrent effect.*

This recommendation comes directly from one interviewee, who suggests one consider relevant threats (traditional edged weapons, small arms, IEDs, VBIEDs), vulnerabilities, and consequences.

Adding a randomized secondary check can improve security in other ways. For instance, when wanding is done for randomly selected patrons who have "passed" a WTMD test, this provides valuable information on the "detection rate" of the WTMD plus its operation.

Recommendation 2.1.7 *Adding a randomized secondary check improves security by giving an indication of the "miss rate."*

A variety of observations about randomization came from interviews with practitioners. Here is a selection of important observations about randomization.

Important Observations about Randomization

- When a process is too expensive to do 100% of the time, randomization can still reduce threats and increase security. It is a low-cost way to introduce a higher level of security.
- There are advantages to being unpredictable.
- Randomization "makes the bad guys work harder;" "it gives them pause for thought."
- Randomization diminishes the effectiveness of surveillance by the adversary. "The goal is to defeat a sophisticated surveillance team."
- Randomization keeps those with intent to do harm off balance. (It could also keep patrons engaged in security efforts– something like See Something Say Something.)

- Randomization serves as a deterrent: If procedures are seen to be uncertain, unpredictable, adversaries might alter their calculation of the likelihood of success or failure.
- Deterrence is especially effective when it is known that a random security process is being implemented, but the exact protocol or randomization scheme is not visible.
- Randomization may keep your staff sharp and engaged if it has them not doing the same thing over and over again.
- Randomization should be geared to the type of event, threat level, and number of events at a venue.
- Randomization has the positive unintended consequence of requiring a venue security manager to take a fresh look at their security.
- Randomization requires documented procedures and easy execution to ensure consistency.
- In some cases, randomization allows for additional security within a limited budget, as when one wants secondary inspection but cannot afford 100% secondary.
- Randomized secondary screening recognizes that primary screening is not 100% effective; it "fills the gap," increases the probability of detection (as any added security initiative does), leads to increased deterrence, and makes patrons feel more secure.
- All kinds of randomization require training.
- A venue security manager must work within constraints of: employee skills and understanding, patron perception and satisfaction, legal guidelines, labor contracts, equipment and technology limitations, etc.

We formalize several of these ideas as recommendations.

Recommendation 2.1.8: *Randomization should be geared to the type of event, threat level, and number of events that are conducted at a venue.*

Recommendation 2.1.9: *Randomization requires documented procedures and easy execution to ensure consistency.*

Recommendation 2.1.10: *All kinds of randomization require training.*

2.2 Randomization in Other Sectors and Settings

Our team assessed how randomization has worked in other security settings, with careful consideration as to the portability to the sports and entertainment industry. Some federal programs, a major airport, a rail system, and other organizations have all deployed randomized designs to improve physical security.

Recommendation 2.2.1: *Having a collection of possible security plans (a Playbook) from which to choose from for each threat level, and choosing one of them randomly for each event or randomly choosing a day for each to be run, is a promising idea for sports and entertainment venues.*

One venue security manager provided a cautionary note about using a Playbook. It might raise questions of consistency, and require an explanation for why a particular security protocol is used sometimes and not others.

Recommendation 2.2.2: *A venue should consider sharing expensive technologies and specially trained personnel (e.g., trace explosive detection swabs, X-ray machines, highly trained K-9s) with other venues or organizations on a random basis.*

Recommendation 2.2.3: *Determine the legal authority required to effectively implement a security randomization initiative.*

Recommendation 2.2.4: *For "sophisticated randomization" tools to be successfully implemented at sports and entertainment venues, the implementation must be simple with the complex math in the background, and there needs to be close collaboration between technical developers and users in order to inform the complex math required.*

Recommendation 2.2.5: *If the goal is to develop tools for randomization that are adopted widely and are easily applied/modified for use at all kinds of sports and entertainment venues, simple tools of randomization are likely a best way to start implementing randomization for venue security.*

2.3. Summary of Ideas for Randomization in Sports and Entertainment Venues

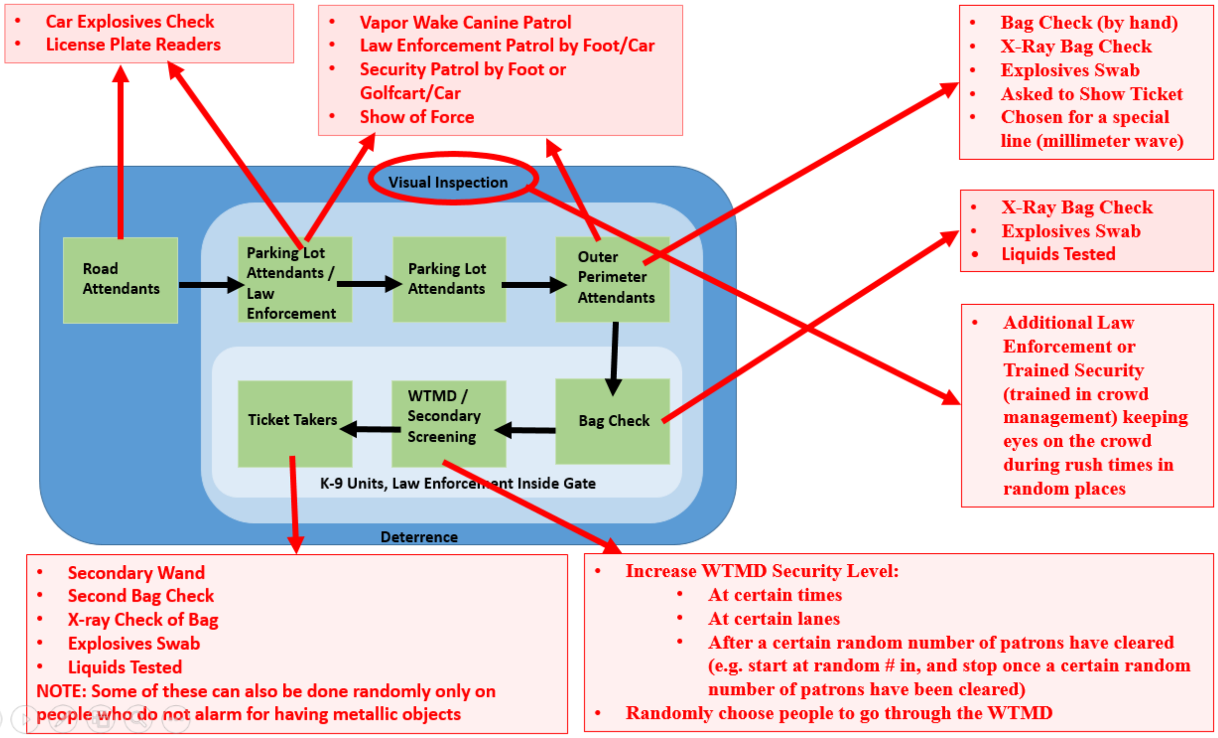
Car Explosives Check
License Plate Readers
Vapor Wake Canine Patrol
Law Enforcement Patrol by Foot/Car
Security Patrol by Foot or Golfcart/Car
Show of Force
Bag Check (by hand)
X-Ray Bag Check
Explosives Swab
Asked to Show Ticket
Chosen for a special line (millimeter wave)
X-Ray Bag Check
Explosives Swab
Liquids Tested
Additional Law Enforcement or Trained Security (trained in crowd management) keeping eyes on the crowd during rush times in random places
Visual Inspection
Road Attendants
Parking Lot Attendants / Law Enforcement
Parking Lot Attendants
Outer Perimeter Attendants
Ticket Takers
WTMD / Secondary Screening
Bag Check
K-9 Units, Law Enforcement Inside Gate
Deterrence
Secondary Wand
Second Bag Check
X-ray Check of Bag
Explosives Swab
Liquids Tested
NOTE: Some of these can also be done randomly only on people who do not alarm for having metallic objects
Increase WTMD Security Level:
At certain times
At certain lanes
After a certain random number of patrons have cleared (e.g. start at random # in, and stop once a certain random number of patrons have been cleared)
Randomly choose people to go through the WTMD

Figure 1: Flow chart illustrating various ways to add randomization to patron screening.

<u>Screening:</u> There are many ways that venue security managers and collaborators can add randomization to patron screening processes, as well as in areas outside of the venue prior to patron screening. We have created a flow chart illustrating some such ways (see Fig. 1). For instance, prior to patron screening, attendants at nearby roads and security in the parking lots can patrol random areas or be placed randomly to do visual inspections. Venue managers can randomly select cars for an explosives check, or can position license plate readers in random spots. In the parking lots, law enforcement and/or security can randomly do a show of force for deterrence, as well as randomly patrol areas/parking lots by foot, vehicle, or golf cart. Venues can also randomly patrol with vapor wake K-9s. Venues can add random processes to select patrons for some kind of security check such as: a bag check, x-ray bag check, explosives swab, ticket check, or special security line (e.g. a WTMD set at a higher setting or one with millimeter wave technology). At the traditional bag check, patrons can be randomly selected for an x-ray bag check, an explosive swab, or to test liquid contents. (However, if the venue adopts a policy such as the NFL’s bag policy, it is unlikely that an x-ray check would do any more than glancing at the contents from the outside of a clear bag or opening a small clutch and quickly looking through it.) At the WTMDs, patrons can be randomly selected for wanding, a second bag check, an x-ray check of a bag, an explosives swab, or liquid testing. WTMDs can also have their security level increased at certain times or after a certain number of patrons have been screened, or they can be increased randomly at certain lanes (which can change by day/event). For venues

without a budget to screen everyone with a WTMD, they can randomly select patrons to be screened.

Additional Ways to add Randomization:

- Roaming Equipment - *Venues could start with choosing a piece of equipment to perform higher security (e.g. a portable explosive swab machine), and have it randomly move between locations – either change lanes, or change which component of security it is in.*
- CCTV - *When not being used to monitor one specific area, CCTVs can display randomly selected areas; it is also possible to randomly assign which staff members watch which displays.*
- Venue inspections prior to event - *Come up with schedules of paths, and then randomly choose one.*
- Employee Entrance Security - *Staff can either be randomly chosen to have their bag checked by an x-ray machine in addition to usual bag check; or with 100% x-ray screening of bags, some bags could be randomly chosen for additional hand screening.*
- Staff Assignments to Jobs / Locations - *Randomly assign staff to jobs/locations they are trained for.*
- Demonstration of Skill - *Randomly select an employee to demonstrate each component of screening (WTMD, wanding, bag check) before each event.*
- Equipment Check prior to event - *e.g. for WTMD, venues could either randomly select WTMDs to check, or could randomly select a set of tests to use to check the machines.*
- Badge Checks Inside the venue for employees - *Facial recognition could be used at random locations or at random times along with badge scans.*
- Randomly assign patrons to gate entry lanes
- Red Teams – *staff not known by front-line security can be assigned to attempt to carry in contraband at randomly selected gates and times.*
- Social Media Monitoring - *Randomly look through social media posts when not a major alert or intel, or randomly pick who monitors when.*
- Inspections outside the venue - *Randomly look in trash cans, planters, near bushes, etc.; randomly pick staff to do the checks.*
- Vendors - *Check vendor deliveries randomly; check vendor vehicles for explosives at least randomly; randomly check with vendor company that vendor employee is still active.*
- Media - *Randomly use x-rays for media bag check or if using 100% x-rays, randomly select bags to hand search; random explosive swab of bags/equipment.*

Reasons for Not Trying Randomization. Early in the project, we asked practitioners what randomization ideas they had tried and, if none, why they hadn't tried any. In explaining why they hadn't tried randomization, the following were among the reasons given:

- Security should be based on intel and risk assessment.
- You cannot give contract security much latitude.
- The leagues mandate that security should be done in a certain way.
- We are waiting for the league to say it should be done.
- Changing security would be confusing to the part-time, minimally trained employees.
- We are really interested but too busy to think about it.
- We have limited resources for security and randomization could take away from something else that resources could be used for.
- Randomization might lead us to miss a real threat.
- How do we justify where and how we do randomization (versus 100%) in the event that there was a real incident?

We also asked in interviews what randomization had been tried.

What has been Tried:

Patron Inspection: Mostly randomization was at an early stage of instituting screening. For example, one venue did randomized wanding when they first started screening: Every *n*th person, with *n* changed randomly every day and the day's *n* not known to staff or patrons. However, they then went to 100% screening. Another venue started with randomized screening, but then went to 100% WTMDs because they didn't want patron complaints about leaving some people unscreened. Another venue instituted random screening when there was high threat, then went to 100% screening. (It is always a good idea to design your security around threat assessment, intel, etc.) In another venue, while all bags are searched, they randomize WTMD, wanding, and pat-downs. They feel that this is more effective – WTMD may be set too low in order to increase throughput and some things are only detected by pat-down. We asked if venues vary WTMD sensitivity levels. None we talked to does it randomly (though we are working with a venue about to try it).

Rotating Job Assignments (to Protect Against Insider Threat). One venue rotates job assignments without notice to combat potential threat from collusion between patron and screener. However, other practitioners suggested that if one only changes employee assignment from one line to another, patrons could self-select the line where their accomplice was working. However, things like switching the parking staff with the traffic staff, player access with staff access could work, provided the employee has the appropriate training. The positives of rotating job assignments include that employees learn more than one skill, they are kept more alert/less bored, and there is a level of obfuscation. The negatives include that one loses the first-hand knowledge of patrons gained from regular interaction with them.

Red-teaming. This is commonly used, with several teams at each gate. It keeps the staff engaged. Providing incentives (rewards) for staff that succeed in catching a red teamer seems to help.

Pre-event Sweeps (with or without K-9s). This is common. Venues vary where the sweeps start, where they look, the team doing the sweeps. They also vary the sweep protocol, but sometimes need to follow the protocol dictated by a performer.

CCTV. In one venue, CCTV is watched by different people at different times; there is some random redundancy in monitoring. Another venue's protocol is to continually check access points when patrons enter, then to switch to monitoring interior spaces and the crowd – a kind of randomness.

Miscellaneous. Other things that have been tried or are in use are to randomly check trash cans, randomly drop in on broadcasters (who have their own security), and randomly check near fence lines where people might throw something over the fence into the venue area.

Note: This section does not have specific recommendations. Recommendations about best practices for randomization are reserved for Sections 2.7 and 3.1.

2.4. Assessing the Effectiveness of Randomization

As noted under Section 1.1, we heard about many anecdotal benefits of increased deterrence, though as noted deterrence is hard to measure. The effectiveness of randomization could be measured by the amount of contraband detected. However, as noted in Section 1.1, if randomization is working to deter attempts, counts of contraband or fare beaters, etc., might go up for a while and then go down. This gives rise to a restatement of Recommendation 1.1.5.

Recommendation 2.4.1: *In assessing the effect of randomization as a deterrent, take into account that, at least after an initial increase, concrete measures such as contraband caught might decrease.*

There are other subtleties in using metrics to assess effectiveness of randomization.

Recommendation 2.4.2: *In using metrics to assess the effect of randomization, take into account relevant factors such as size of crowd, level of effort devoted to screening, and the weather.*

Simulation is a tool that could be used to measure effectiveness of randomization, and we have used simulation to do so (see Section 2.5). For instance, increased percentage of detections in screening if randomized secondary screening is introduced would be one metric that a simulator could estimate. However, simulation is only as good as the data put into it, and the detection rate depends on the number of "attempts" to do something bad, which depends on very small probabilities, resulting in large statistical uncertainties.

Some of the metrics that can be estimated by simulation of screening are: Throughput, average and maximum waiting time; number and percentage of patrons who were secondarily screened; maximum queue length; total in queue at game time; maximum time a patron had to wait; when did the queues clear; and number of people chosen for random screening components. Of importance from a security perspective, simulation can reveal the largest size of the unprotected crowd. Simulation can be used to gain an understanding of the potential practical impact of a security initiative before it is implemented. It was for this reason that CCICADA developed a Stadium Simulator, designed initially to assist a partner venue in determining how many WTMDs to purchase.

Recommendation 2.4.3: *Utilize simulation and other tools to understand the potential practical effect of a security initiative before implementing it, as well as to understand the potential practical impacts of implementation.*

If a venue is introducing a new security initiative, randomization adds costs, but not as much as using the initiative 100% of the time. The number of employees required would then be one possible metric for effectiveness in keeping the budget for security at a desired level. In screening applications, one could consider the ratio between amount of contraband found and number of employees used. (Or, better yet, the ratio between contraband found and the product of number of employees used and number of patrons screened. This metric takes into account the size of the crowd screened, not just the number of workers.) In general, as mentioned in Sec. 2.1, feedback we have received is that randomization should not replace doing something 100% of the time if the latter can be afforded. Still, as also noted in Sec. 2.1, randomization adds a deterrent effect and adds a measure of obfuscation that makes it more risky for an adversary to try something, which means that in some situations, it might be viewed as more effective than doing something all the time. When randomization is performed on something like secondary screening then it adds value that somehow needs to be assessed by the expected increase in detection rate. See Recommendation 2.1.6.

Red-teaming is widely used to measure the effectiveness of security practices, and could be used specifically to measure the effectiveness of randomization.

The issues about drone experiments mentioned in Section 1.1 are relevant here as well, even though they do not concern randomization. As noted in that section, it is important to identify effectiveness goals, threat tolerances and metrics for satisfactory performance before testing a new system. This is a best practice for assessing effectiveness. See Recommendation 1.1.1.

2.5. Randomization in Patron Screening: Simulation Experiments Help Understand Effects and Effectiveness of Randomization

In Section 2.7, we discuss 25 randomization ideas (see Appendix) that arose during this project, and review the responses of SMEs to a survey about them. Many of these involve screening. As discussed in Section 2.4, before actually trying out a new technology in practice, it helps to develop analytical tools to estimate the impact of that technology on things like maximum queue length, queue clearance time, detections, false alarms, etc. to assess the potential value/effectiveness of a randomization protocol and to reassure a security director that the expected impact of such a measure will not create security vulnerabilities or require significant extra resources. CCICADA's Stadium Simulator was developed for this purpose. Here we discuss the results of experiments performed with the Stadium Simulator to gain an understanding of the effects and effectiveness of randomization. The main point is that, whether it's a tool like the Stadium Simulator or something else, some analysis of potential effectiveness and potential desired/undesired effects should precede implementation whenever possible. (See Recommendation 2.4.3.)

Inputs to Stadium Simulator. To use the Stadium Simulator, we have over the years gathered basic data such as typical processing times (distribution of screening times) and false alarm rates. Using these, we completed the next phase of the development and testing of our Stadium Simulator tool. This tool permits the user to vary many parameters, such as the detection and false alarm rates, the arrival rates at different time periods, the percentage of people carrying contraband, and the distribution of the (random) screening time associated with each inspection station, and with a number of layers of defense (such as bag check; WTMD; secondary screening; ticket check).

Stadium Simulator Enhancements. At the suggestion of practitioners and the result of early experimentation, many additional options have been added to the Stadium Simulator to make it easier for us and practitioners to use and to cover many more processes/procedures than before. We added the possibility of bag size and other checks at the outer perimeter, bag contents checks at the inner perimeter, and added randomized screening options such as explosive swab checks. These all reflect changes that venues are making. In addition, we have added the capability to have two different rates of patron arrivals (switching from one to the other at a specified time), and also adding random screening before the bag size check at the outer perimeter, before bag contents check, and randomly selecting patrons at the WTMDs for additional screening. There is also the option of having two different screening protocols (at different lanes) and having patrons randomly assigned to these lanes. Thus the WTMDs may have different settings, or there may be a more comprehensive bag contents check or bag size check in some lines. We may also create special lanes with special processes for certain types of patrons, e.g., those without bags, or season ticket holders or the disabled. Many of these are changes that, to our experience, have not yet been tried very much at sports and entertainment venues, but should be experimented with. Finally, we have integrated the possibility for randomization at all steps of the patron screening process.

Randomization Experiments with the Stadium Simulator. We developed a large number of randomization protocols to experiment with through our Stadium Simulator, then limited the number to those we felt would provide the most useful feedback and reflected reasonably practical randomization options. For each, we measure the effect on throughput, detection rate, false alarm rate, etc. The experiments performed include: add additional random security to the outer perimeter (e.g., wanding, bag contents check, or explosives swab check); randomly select people at the WTMD step for an additional security check (wanding, etc.); and randomly select patrons to go to some WTMDs which will be set at a higher security level.

To understand the impact of a security initiative, one has to compare it to a "baseline." A typical experiment would modify a standard protocol or add a new one, perhaps with randomization.

Also, because there are probabilities involved, one has to run the simulation multiple times to get a feeling for the random variation, and an overview of what might be happening. Then, the results of the runs for the baseline can be compared to the runs for the experimental change. The venue security director will need to decide what information will be most helpful. Does he or she want to see the result of each run? Or the average value of the outcomes (e.g., average time spent in security) on each baseline run vs. on each experimental run? Or the "worst case" (longest time spent in security) on each baseline run vs. on each experimental run?

Here we discuss a sample experiment, not because the numbers and results mean a lot, but because they illustrate what we have in mind. In this experiment, there were 10 security lines at a gate, each with a WTMD, and we increased the security level at one of those WTMDs. Just for the sake of experimentation, we assumed that the detection rate of "contraband" (knife, brass knuckles, etc.) increased from 80% with the standard WTMDs to 95% with the one WTMD with higher security setting. We assumed that 1% of the patrons had some form of contraband. These parameters may not be realistic but suffice to illustrate the use of simulation to investigate the effectiveness of a security initiative involving randomization. We also made assumptions about the patron arrival rate, the distribution of times spent in different steps in the security process, etc. For the baseline, the average (mean) of the average times spent in security was 2.54 minutes. For the experimental case, this went up to 3.22 minutes. Given such numbers, the security director would have to decide if such an increase would be acceptable in terms of potential effect on patron satisfaction – of course depending in part on the increased detection rate obtained. (An increase of about 30 seconds might not seem too bad. However, perhaps more information would be helpful, e.g., average time spent in security if entering 30 minutes before event start.) But the average detection rate over the runs only went up slightly, from 86.3% for the baseline case to 87.1% for the experimental case. This seems like a minor increase compared to making people wait longer. We also calculated the maximum number of people in security lines at any one time in each run – a measure of vulnerability resulting from patron inspection processes. The average maximum was 941 in the baseline case and 1087 in the experimental case. In sum, a security director looking at these experimental results might be tempted to say that the extra detection rate is not worth the extra inconvenience to patrons or the extra vulnerability to them. (It may also be worth noting that the average wait time in the line with the higher security setting was 9.34 minutes but the detection rate on that line averaged 94.3%.) On the basis of this one experiment, we are not by any means concluding that the strategy of setting the security level on one or more WTMDs higher is a bad idea. The conclusion depends heavily on the parameters we used in reaching this conclusion. We just use this example to illustrate the point that such experimentation before rolling out a new security initiative is a good idea.

There was another interesting thing that happened when we did this experiment. We looked at queue clearance time, the time after event start ("kickoff time") that the last person in line got into the event. This increased dramatically from 6.60 minutes after event start to 15.70 minutes. In the latter case, we wondered why there was such a big increase, and this led us to see that our simulation model was doing something unrealistic; it was not allowing patrons to switch from a longer line to a shorter one, but instead assumed that the random assignment to a line was permanent. In this way, the experimentation taught us something about what is and what is not realistically possible. We would certainly find pushback from patrons if we forced them to stay in the line we randomly chose for them and that line moved so much more slowly than others.

Among other things, in this project we have also studied incentives for early arrival and how crowds arrive under event day conditions of giveaways (see Section 1.2) and these too can be tested using the Stadium Simulator. For example, if we have not one peak of patron arrivals around event time, but instead have two peaks (an added earlier one), we can use the Stadium Simulator to explore the impact that the incentive may have on the maximum number of patrons waiting in line, etc.

2.6. Randomization in Employee Background Checks

As a case in point to mitigate threats from insiders, we looked at employee background checks, and in particular randomization of the timing of repeat checks. While our study was ongoing, after the 2017 Ariana Grande attack at the Manchester Arena, employee background checks as a mitigation strategy for entertainment venues received considerable added attention.

Other Sectors. We surveyed open literature about repeat background checks and randomization in other sectors. Mostly, these have an emphasis on basic criminal checks and drug/alcohol testing. Our review looked at sectors including Commercial, Healthcare, Government Facilities, Transportation, Nuclear, Chemical, Energy, Communication, Financial Services, and Defense.. One of the more interesting developments is the use of rap-back systems, which store fingerprints in a database used to check employees. There seems to be improved efficiency in utilizing fingerprint-based checks to allow for continual checks against criminal history databases. In cases where the employee is arrested or convicted of a crime following the initial background check, employers are notified of the arrest or conviction. Rap-back systems are relatively inexpensive and have been implemented by a variety of agencies.

Random Rechecks in the Sports and Entertainment Venue Community. No one we talked to in the sports and entertainment venue community uses randomized repeat background checks. People we talked to cite the costs, contracts, and questionable value as reasons. Some regularly do 100% repeat background checks, some as frequently as monthly. Some repeat background checks on all seasonal employees at the beginning of each season. We were told by one venue security manager that rather than doing repeat checks on the front office, they look for behavioral changes. Some cited the lack of thorough information in background checks: e.g., arrests don’t show up in records until after court proceedings. However, things may be changing: One venue security manager told us he is exploring a new procedure of using a background check service that provides bulk screening on a recurring basis and alerts him any time one of his staff members gets arrested – a rap-back system. He views that as more cost effective than random checks. Interviewees emphasized the strong need for standardization of background check rules/regulations/procedures.

Selected Best Practices for Randomization and Background Checks

Recommendation 2.6.1: *Ensure that the organization has necessary legal authority to conduct repeat (random) background checks.*

Recommendation 2.6.2: *Conduct randomized rechecks over a defined time period, ensuring that each employee is selected at least once by the end of the period.*

Note that to implement this in practice requires some subtlety. Suppose every employee has a one third chance to be picked even if they were picked last year – which is a best practice. Suppose we *randomly* do a background screening on 1/3 of our 300 employees every year. Year 1 misses 200 of them, Year 2 misses about 2/3 of that 200 or about 133 of them, and Year 3 still misses about 2/3 of that 133 or about 86 of them. So, in 3 years, ~86 are *never* checked. Thus, perhaps one needs some sort of hybrid plan that requires checking those who are omitted by the randomization

Recommendation 2.6.3: *Each employee should have equal chance of selection during a testing period. (Do not remove an employee from the testing pool because they were selected in a previous pool.)*

It is often a good idea to modify this to say there is an equal chance for all employees in a certain job title or risk category. Indeed, the depth and frequency of repeat background checks might be related to security functions.

Recommendation 2.6.4: *Randomly select employees for more in-depth background screening.*

Recommendation 2.6.5: *Randomly verify that third party vendors/contractors are conducting required background checks.*

Recommendation 2.6.6: *Have a developed and clearly defined process and written policy concerning conducting background checks.*

Recommendation 2.6.7: *Random selection methods should be scientifically valid and the randomness of the selection method must be verifiable.*

Recommendation 2.6.8: *Ensure employee privacy.*

Recommendation 2.6.9: *Do not discard a selection without adequate explanation.*

Recommendation 2.6.10: *Distribute the tests reasonably throughout the year.*

Recommendation 2.6.11: *Refresh the pool of employees before each random selection.*

Recommendation 2.6.12: *Retain and maintain records and maintain testing pool.*

2.7. Best Practices for Randomization

Randomization Ideas. Our team developed ideas for randomization in a variety of areas, as a way to make better use of security resources and to increase levels of deterrence by making it more expensive for an adversary to guess a defensive strategy. These were based on practitioner interviews, literature reviews, on-site observations, and our own experience. We then organized these ideas into groups, clarified them, removed overlapping ones, and prepared a final set of proposed practices that were presented to SMEs for feedback. The list of the final 25 candidate practices is included in the Appendix .

Survey of SMEs about Randomization Ideas. We surveyed SMEs about the 25 candidate practices. For each practice, we asked the participant whether or not they have had ***experience*** with it, i.e., actually used it (not necessarily at their present venue). We then asked whether it was ***important***: Should the practice be part of any venue's approach to security and will adding it significantly strengthen security? We also asked if the practice was ***feasible***: Can the practice be added to present policies without major costs or personnel challenges? And we asked if it was ***sustainable***: After a successful and effective launch, will the practice avoid "decay" in its implementation, while it remains relevant, due to various factors such as cost, physical/stamina capabilities of staff, stadium or crowd dynamics, equipment wear-and-tear-or failure, follow-up auditing, complacency, etc.? Participants were also asked to list practices they felt should be added to the list.

Survey Results

Our survey was limited to twelve respondents, so the number of respondents who gave a randomization practice some rating is not as important as the overall impression we got from these experts. Here are a few general observations:

- Many SMEs seem unfamiliar with these notions of randomization, and possible implementations. This suggests that some program of publicity, education, and training could be useful.
- Few of the candidate randomization practices are in widespread use (i.e., at more than 75% of the venues represented by the SMEs).
- There is substantial support for the notion that such practices are important and feasible. Thus, in particular, many more security practices were judged important than had been tried. It appears that the field is moving to adopt them, but has to work out many practical and logistical issues in order to fit randomization into existing work practices, and employee capabilities and training.

Recommendation 2.7.1: *There is a continued need to identify practical and logistical issues to aid venues in finding ways to initiate randomization.*

Recommendation 2.7.2: *There is a need to develop procedures for security director and event staff training in randomization practices.*

Only eight of the 25 practices are used by 2/3 or more of the respondents. They are listed below in Recommendation 2.7.3. (In decreasing order of actual use, using codes from the Appendix and Recommendation 2.7.3, they are S10, Q1, P2, E4, E2, P3, S5, and E7.) All are also considered important by at least 3/4 of the respondents.

Review of the overall results of this study suggests that, because randomization is not widely used, it will continue to be difficult to gather useful information on the “weight of evidence” for particular recommendations. Ideally, one wants to be able to say that a specific practice is being used by some large fraction of the venues, and is found to be effective, by whatever standards each venue is applying. Given the present state of the art, we can do no more than report these results that indicate that expert security practitioners judge randomization to be an important aspect of security, but do not have enough experience with it for these findings to rank some specific practices as being more important than others.

Examples of the randomization practices (that were judged important by a strong majority of respondents but only in use infrequently are given in Table 1.

Table 1: Randomization Practices Judged Important but Rarely in Use

E5.	Randomly audit some fraction of the ID badges against access management database.
S2.	In a highly visible way, conduct random searches in the parking lot.
S9.	Strengthen the outer perimeter from just visual check, by randomly selecting people or bags for some kind of higher level screening.

Since eight of the 25 randomization practices had been tried by at least two thirds of the respondents and considered important by a large majority of them, it seems reasonable to recommend that this is a representative list of practices with which to initiate randomization.

Recommendation 2.7.3: *A list of potential randomization practices with which to initiate randomization at sports and entertainment venues consists of the following practices:*

E2. Randomly check personnel IDs during the working day.
E4. Randomly check person matches face on badge.
P2. Have security management randomly visit various posts and functions.
P3. Randomize perimeter patrols with qualified personnel.
Q1. Schedule red teaming probes randomly by location.
S5. If there are explosive-detecting canines, have them walked randomly through parking lots.
S8. At a checkpoint randomly select some cars for explosives check (by under-carriage mirror or canine)
S10. Schedule visible law enforcement presence near venue, and request random pattern, timing or location to increase deterrence and avoid countermeasures.

As a general rule, SMEs did not distinguish feasibility from sustainability. All of the eight practices above were considered feasible and sustainable by a majority of the SME respondents.

Section 3: Practical Implementation of Simple Randomization for Patron Screening

The process of screening patrons before they enter a large sporting venue may be a deterrent to terrorist activity at the venue. However, the screening process can be time consuming, may annoy patrons, and may cause queue buildups that may create vulnerabilities. A simple design that randomly selects some patrons for extensive screening, but has other patrons go through quicker, less extensive checks, should be considered. However, the practical implementation of a simple random selection process presents challenges.

3.1 Best Practices for Implementation

Among the issues related to implementation of randomization are: the need to keep things simple given the many duties of line security staff and the minimum time/ability to train them in sophisticated methods; the need to be transparent so there is no likelihood of being accused of profiling; and the explanation/signage to go along with the process. Again, as discussed after Recommendation 1.2.6, it is important to advertise that a random process is in use but equally critical that the specific process not be disclosed.

Concepts for Implementation of Randomization. In the earlier stages of our project, based on interviews, literature review, and our own informed ideas, we developed concepts for implementation of randomization. Perhaps the simplest tool for implementing randomization may be to count every so many people and then choose the next one. Human counts, used by some venues, and choosing every n^{th} person, may not be ideal, even if n is varied from day to day. These are hard to implement, not transparent to patrons, and don’t leave an audit trail. Using a deck of cards from which a patron chooses is transparent, but perhaps time-consuming to implement if used repeatedly unless the card is chosen while the person is waiting on line.

Another tool for implementing randomization in patron screening could be to use a visible random device (e.g., a touch device that patrons can activate) to pick a certain fraction of the people for the practice; use a hidden random device to pick a certain fraction of patrons (e.g., a photocell or other counter on a WTMD). Specifically for the case of secondary screening, perhaps the most effective method may be to utilize a built-in feature that WTMDs have to make a random selection for additional screening even if the WTMD detects no metal on a patron. We have also researched alternative implementation methods such as using random number generators on an iPad or tablet with patrons tapping the screen; or using a foot-operated device that patrons would step on as they leave the WTMD.

Other types of implementations of randomization would be to use a random approach to decide whether to do a specific practice (from a Playbook) on a given day; or a random approach to choose which prepared plan to use on a given day.

Just to clarify: A Playbook contains a number of security configurations (e.g., enhanced secondary inspections of patrons, use of K-9s in a given area of the loading dock) and allows the user to randomly select an entire security configuration. A prepared plan is specific to a single aspect of security, e.g. how you would use K-9s on a given day.

One venue security manager emphasized that however randomization is implemented, the human element comes into play. Having a clear and easy way to implement process is important for that reason.

Survey of SMEs on Implementation of Randomization. Along with the ideas for randomization discussed in Section 2.7, our team developed ideas for implementation of randomization in practice, and included five final ones in our survey of SMEs. See Appendix. Three of these were for screening and two for randomly choosing from a collection of security practices to implement on a given day. As with randomization practices, we asked the SMEs to provide information about experience, importance, feasibility, and sustainability for these implementations. When participants said that they had used a practice, we asked them to describe the method to achieve randomization.

Survey Results:

Results of the survey indicated a finding similar to that with the 25 randomization practices: Few SMEs had personal experience in the basic processes of constructing and implementing randomization practices and few had any experience with any of the five practical methods of implementing randomization. The SMEs were not familiar with using even very simple methods such as selecting every *n*th patron, or using a table of random numbers to implement randomization practices. Thus, we cannot identify any practices that had been tried by at least half the respondents.

To gain further insight into what the SMEs have done, we examined their detailed responses to see how they did the specific random practices that they have actually used. The practice with which the most SMEs had experience was to select persons by counting. Even here only 1/3 of the respondents had tried it. There was only one SME who had experience with the practice of selecting a specific plan, randomly, on the event day, though an analysis of specific comments showed that this person mentioned this idea 15 times, more than twice the number of times any other randomization practice was mentioned. The responses show that the total penetration of randomness into the security space is very low.

Our recommendation is to start with any of the patron screening processes that seems easiest to implement and to start with one of the Playbook ideas for randomization of choice of practices on a given day.

Recommendation 3.1.1: *There is a continued need to identify practical and logistical issues to aid venues in finding ways to implement randomization in practice.*

Recommendation 3.1.2: *There is a need to develop procedures for security director and event staff training in randomization implementation methods.*

Recommendation 3.1.3: *Venues should use an implementation procedure for randomized screening (secondary screening) that is easiest to implement in their context and achieves the goals of minimizing patron perception of bias.*

Recommendation 3.1.4: *Venues should experiment with the idea of developing a set of security practices/protocols (a Playbook) that are available for random implementation on a given day/event.*

3.2. Patron Perception

As noted in Section 1.2, venues do not report many examples of complaints about profiling. However, one venue security manager told us that there is no way people will not think that they are being profiled if there is randomization. We reviewed the social science literature for definitions of the concept of perception of bias, its relation to group identification and its relation to "dispositional inference" – when do "I perceive that you have acted against me, in a biased way?" We also interviewed practitioners about their experience with accusations of bias and ways to avoid such accusations. This led us to practices that reduce the perception of bias and ways to more effectively train staff to avoid such perception.

Recommended Practices to Avoid Perceptions of Bias

Recommendation 3.2.1: *Brand and insert into the organizational culture (and continually reinforce) that the organization and its security procedures are "just, fair, protective, etc."*

This means that, whenever possible, in correspondence, appeal to a patron's sense of/need for safety, security, justice and fairness for all patrons. It means ensuring that the organization's commitment to the safety and respect of all patrons is apparent in all pre-event marketing materials. During events, it means having information available and distributed (on television screens, in pamphlets, etc.) about the organizational values of safety and security. This cannot be feigned; it must be sincere and truly adopted by leadership and the system culture.

Recommendation 3.2.2: *Keep patrons informed about and engaged in security protocols and procedures.*

This means that, prior to events, detail security protocols and procedures in marketing materials. It means that during events, use media and personnel to quickly and efficiently explain upcoming processes. It also means to obtain feedback from patrons, using incentivized randomized surveys, about their experiences during security-related processes.

Recommendation 3.2.3: *Minimize risk of perceived bias through employment of a perceptibly diverse security staff and ensuring that the selection process (for additional screening) is easy to understand and "predictably unpredictable" (i.e. random).*

Recommendation 3.2.4: *Ensure that the staff consistently receives diversity and de-escalation training and encourage personnel to be personable and friendly as they explain imminent security procedures.*

As one reviewer of this report pointed out, one aspect of diversity and de-escalation training is to teach employees that they must completely understand the importance of people's civil rights and base their thought process and actions on behavior analysis rather than race, ethnicity, gender, or religion.

3.3. Behavioral Issues

While the emphasis in this study has been on using random selection for patrons to receive screening or extra screening, there is certainly an important role for the use of suspicious behavior triggering screening or additional screening. Behavioral interactions among patrons also have an impact on screening, e.g., when patrons arrive in a group, a family group or a school group.

Use of Behavior Triggers. We have gathered anecdotal behavior on how venues can use some trigger behaviors (avoiding a screener dog; wearing weather-inappropriate clothing; avoiding areas where there is a "show of force;" etc.) to invoke heightened screening. One venue has behavioral assessors intercept patrons well away from the venue (e.g., leaving public transportation), engage them in conversation, and ask them to open their bags; refusal leads to their being followed and further assessed.

Recommendation 3.3.1: *Use of behavioral triggers for enhanced patron screening can begin well away from the venue itself.*

Recommendation 3.3.2: *Implementation of behavioral triggers for enhanced patron screening can involve processes other than specific screening protocols such as use of WTMDs, wands, or explosive swabs.*

Recommendation 3.3.3: *Because the "science" and the "practice" of using behavioral indicators is changing, venue security directors should seek to get the latest information before utilizing them.*

Handling Groups of Patrons. We have gathered observational and anecdotal data on how diverse venues deal with the need to keep family and other groupings together. This may tend to enhance security as, for example, when all the members of a family are directed to a higher security lane if any one of them is randomly selected. We also note that family groups present special problems of vulnerability, e.g., through reluctance to subject children to extra screening. Certainly there is concern that the adversaries might plant weapons or other contraband on children if they are not going to be inspected or to be inspected with lower probability. In sports and entertainment venues, with packed crowds and rapidly moving lines, the decision of where to place the rest of a family becomes an issue. It can easily be seen that the screening approach to families and children could present patron satisfaction issues that may not exist with individual or small groups of adults. Training of the security staff is important to avoid such situations.

The issue of how to handle other groups of patrons is also important. For instance, what about a marching band? Do all members get screened in the same way, or does randomization apply to such a group as well? What about groups of patrons arriving together on a bus? Sometimes such groups are given special screening on the bus before the group is admitted. Would that limit the possibility of randomization? Teams of athletes arriving together, e.g., on a team bus, might have a special entrance, but are also given some kind of screening. Would randomization apply here as well? What if one member of a group of friends arriving together is disabled. There are special procedures for screening disabled people such as those in a wheelchair, but how would randomization work if a group had a disabled member? These are all issues that need to be considered.

Recommendation 3.3.4: *Venues need to be aware of vulnerabilities potentially caused by protocols for family group screening.*

Recommendation 3.3.5: *If groups arrive together and one member of the group is chosen for secondary screening, the venue needs a carefully-thought-out policy for where other members of the group stand during the secondary screening so as not to interfere with other screening activities.*

We do note from our field observations and interviews that the age distribution of and other characteristics of attendees do seem to correspond to the event type. Security directors are keenly aware of the patron differences based on event and can adjust group, family and children-related security protocols based on the anticipated volume within each patron type. However, some venues have gotten negative feedback for changing security protocols based on anticipated attendee characteristics, which makes implementation of different security strategies that are dependent on patron characteristics more challenging.

APPENDIX: Randomization: Potential Best Practices and Ideas for Implementation in Practice

Here we present the list of potential best practices for randomization and implementation of randomization that we used in the survey.[1]

Randomization: Potential Best Practices

Employees and Insider Threats

E1 - At some fixed interval (say, every 3 - 0 minutes) swap employees from one task (or lane, or CCTV monitor) to another. Make the swaps unpredictable (random).

E2 - Randomly check personnel IDs during the work day.

E3 - Randomly check that employees are where they should be, e.g., Facial Recognition.

E4 - Randomly check person matches face on badge.

E5 - Randomly audit some fraction of the ID badges against access management database.

E6 - Randomly audit some fraction of ID badges against the event.

E7 - Randomly monitor event-time social media.

Pre-event and Within-event Sweeps

P1 - Have a list of many routes for a pre-event sweep (a "playbook"), and randomly choose one each event.

P2 - Have security management randomly visit various posts and functions.

P3 - Randomize perimeter patrols with qualified personnel.

P4 - During event continue random perimeter controls.

P5 - Randomize areas covered by CCTV.

Red Teaming

Q1 - Schedule red teaming probes randomly by location.

Q2 - Schedule red teaming probes randomly by time.

[1] To be consistent with language adopted in this report, we make minor edits to the actual language used in the survey: changing "worker" to "employee"; changing "police" to "law enforcement"; changing "today" to "on a given event day"; changing "parking areas" to "parking lots"; and changing "red teaming probes of quality" to "red teaming probes."

Screening Patrons, Vehicles, Bags

S1 - At a normal bag check table randomly select some bags for an added check, using available technology (explosives screening; liquid scanner; x-ray; canine).

S2 - In a highly visible way, conduct random searches in the parking lot.

S3 - Whatever the principal screening is, randomly (in whatever way) select some patrons for screening in another way (pat down; explosive swab; x-ray; etc. according to budget).

S4 - Instead of having all WTMDs set at the same level the whole time for a specific event, use some kind of randomization (by time, by lanes, etc. This is easier with networked WTMDs).

S5 - If there are explosive-detecting canines, have them walked randomly through parking lots.

S6 - Use a license plate reader on a vehicle randomly circulating in parking lot.

S7 - Use license plate readers randomly placed at some vehicle check points.

S8 - At a check point randomly select some cars for explosives check (by under-carriage mirror or canine).

S9 - Strengthen the outer perimeter from just visual check, by randomly selecting people or bags for some kind of higher level screening.

S10 - Schedule visible law enforcement presence near venue, and request random pattern, timing or location to increase deterrence and avoid countermeasures.

S11 - Randomly use other available information (credit record; social media) about each patron to put the patrons in different "risk classes."

Randomization: Ideas for Implementation in Practice

R1 - Use counting every so many people, and then use the specific practice to screen the next one.

R2 - Using a visible random device or numbers to pick a certain fraction of the people for the practice.

R3 - Using a random device the patrons cannot see, to pick a certain fraction of the people for the practice.

R4 - Use a random approach to decide whether to do a specific practice on a given event day.

R5 - Use a random approach to choose which prepared plan to use on a given event day, such as what number of people to count – every 5th or every 7th -- or what path to follow in a sweep.