MISSISSIPPI DEFENSE DIVERSIFICATION INITIATIVE

Defense Technologies for the Safety and Security of Commercial Sports and Entertainment Facilities

The University of Southern Mississippi

Prepared by:

Derek Halbasch, Graduate Research Assistant, MDDI

Elizabeth Voorhees, PhD, NCS4, Director of Certifications and Compliance

PROMOTING INNOVATION, DIVERSIFICATION AND COOPERATION IN THE MISSISSIPPI DEFENSE COMMUNITY

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

MSDEFENSE.NET

AA/EOE/ADAI UC 78138 3.18

ACKNOWLEDGEMENTS

The lead researcher wants to express appreciation to the following individuals who contributed to the New Technologies for the Safety and Security of Commercial Sports and Entertainment Facilities report:

The University of Southern Mississippi Trent Lott National Center
Dr. Shannon Campbell, Director, Trent Lott National Center
Heather N. Brown, Research Analyst

The University of Southern Mississippi Department of Economic Development
Dr. Chad Miller, Associate Professor
Andy Kilgore LTC(R), Mississippi Defense Diversification Initiative
Dan DeMott, Mississippi Defense Diversification Initiative
Shane Chadwick, Research Assistant
David Jordan, Research Assistant

The National Center for Spectator Sports Safety and Security (NCS4)
Dr. Louis Marciani, Director NCS4

This study was prepared under contract with the, National Security Technology Acceleration Support and Economic Diversification Efforts for the State of Mississippi, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the National Security Technology Acceleration Support and Economic Diversification Efforts for the State of Mississippi and does not necessarily reflect the views of the Office of Economic Adjustment.

TABLE OF CONTENTS

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

EXECUTIVE SUMMARY

Providing safety and security for commercial sports and entertainment facilities is a large and growing global industry. Technology developed to meet the needs of the Department of Defense (DoD) can often be directly applied to the needs of sport and event security. This report highlights some of the key Commercial Facility Sector security technologies and defense technologies that meet these needs. However, selling into this industry differs from the defense procurement process. Each of the three market segments that includes Facility Owners/Security Managers; Sports Leagues/Venue and Event Management Companies; and Emergency Managers (e.g. police, fire and rescue) have different procurement processes. Since security is often perceived as an extra cost, the industry tends to be price sensitive. Additionally, the industry has its own trade shows, trade journals, and certifications that defense contractors need to adopt. The event safety and security industry presents significant diversification opportunities for defense technology, but first the specialized nature of the industry must be understood.

INDUSTRY SNAPSHOT

Projected Sports Industry Revenue by 2021

$78.5 Billion

(PwC Sports Outlook December 2017)

Estimated Spending by Sport Event Organizers per year

$2-6 Billion

(Hall, Cooper et al., 2012)

(AP Photo/Mel Evans)

(Levis Stadium)

Estimated Cost Super Bowl 51 Security

$5.5 Million

(D'Allegro, 2017)

Estimate Cost 2016 Rio Olympics

$4.6 Billion

(Haddon, 2016)

Estimated Sport League Revenues (FY2016-17)

NFL	$14 Billion	(Kaplan, 2017)
MLB	$10 Billion	(Brown, 2017)
NBA	$ 8 Billion	(Bohlin, 2016)
EPL	$5.1 Billion	(Conn, 2017)
NHL	$3.7 Billion	(Amoros, 2016)
MLS	$461 Million	(Amoros, 2016)

(Tannen Maury/European Pressphoto Agency)

2017-18 U.S. Sports Attendance Figures

NCAA Men's Final 4	76,168
Super Bowl 52	67,612
Indianapolis 500	300,000
Daytona 500	250,000
Kentucky Derby	170,500

INTRODUCTION

Since the September 11, 2001 terrorist attacks in the United States, there has been a focus by the federal government and its agencies on protecting "soft targets" such as stadiums, arenas and outdoor event venues. Safety and security for the Commercial Facilities Sector (designated under Presidential Policy Directive 21), which includes sports stadiums, arenas and areas for public assembly, has grown exponentially over the last two decades. This growth has created partnerships between sports and entertainment event stakeholders, safety and security technology businesses, and federal government entities.

GOAL

Provide information to DoD technology companies about technology applications in the Commercial Facilities Sector

The Commercial Facilities Industry is one of the fastest growing sectors in the United States and around the world. Security for sports and entertainment events is a multi-billion-dollar industry, with significant growth potential because of the increasing popularity of mega-sporting events such as the FIFA World Cup, Olympic Games and the Super Bowl. The growth of these events, coinciding with the growing foreign and domestic terrorist threats, has forced venue operators and event managers to invest in new security technologies to protect people, property, infrastructure and sensitive information. Sporting events and entertainment facilities are likely terrorist targets because of the high media visibility, and social/economic impact that these industries provide to a community.

The diversification and cross-platform capabilities of Department of Defense (DoD) technologies into a sector of the Department of Homeland Security (DHS), is an important mission for the Office of Economic Adjustment (OEA), and the Mississippi Defense Diversification Initiative (MDDI). The goal of this document is to provide information about the Commercial Facilities Sector to DoD technology providers. The MDDI and the National Center for Spectator Sports Safety and Security (NCS4) surveyed Commercial Facilities Sector stakeholders about their technology requirements, needs and purchasing power. Research was also conducted through key informative interviews with those within the Commercial Facilities Sector. This Commercial Facilities Sector report is focused on advanced technologies such as biometric, cybersecurity and closed-circuit television (CCTV) equipment that help detect and deter the criminal/terrorist threats that pose a risk to sports and entertainment events. The report also addresses the investment of new and emerging technologies such as improved security lighting, vehicle barriers, and bomb detection (IED/VIED) tools, which aid the human security element on the ground.

Industry Definition

According to DHS, there are over 4,000 establishments related to spectator sports in the United States. The Commercial Facilities Sector is one of DHS's "16 Critical Infrastructure Sectors," with subsectors that consist of casinos, motion picture studios, hotels/motels, retail centers, and professional sports leagues. "The Commercial Facilities Sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within the sector operate on the principle of open public access, meaning that the public can move freely without the deterrent of highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities" (DHS, 2017). Sports and entertainment events and venues are one aspect of the Public Assembly Subsector, which falls under the broader Commercial Facilities Sector for DHS.

Commercial sport and entertainment facilities are susceptible to disruptions to their daily modes of operation. The different threats to this sector are diverse, from natural disasters, cyberattacks, theft, pandemics, terrorist threats, armed attackers and geopolitical events. The requirements by DHS are that owners, operators and security professionals understand their threat environment at all times. Preferably, stakeholders should develop business continuity strategies that will help build redundancy into operations and mitigate facility and asset risks by implementing sound security practices. When stakeholders in the Commercial Facility Sector are able to assess individual risks and establish internal plans to mitigate those risks, they are better able to respond to disruptions (DHS, 2015). The Sports League and Public Assembly Subsectors identified by DHS are closely related to each other, and together encompass many of the same infrastructure (e.g., command centers, security personnel) and safety requirements (e.g., Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) certification).

(Getty)

Main Activities of Sports Security

Facility and event managers, along with security managers and other stakeholders, conduct numerous activities before, during and after an event. The primary activities of Facility Management, Parking Lot Security, Crowd Management, Network Security Monitoring, Legal and Regulatory Activities, and Incident Management are just a few of the many operational elements required for the planning and execution of a safe and secure environment during sporting or special events. Each of these activities are potential avenues for the application of DoD technologies in the Commercial Facilities Sector.

Facility Management

- Oversees the risk management process of a facility or event
- Multiagency collaboration with individuals, agencies and stakeholders involved in security management
- Manage internal/third-party security personnel
- Ensure concession and retail organization and safety

Parking Lot Security

- Parking Lot Attendants are responsible for safely moving vehicles entering and exiting a venue
- Alcohol consumption in parking areas poses a risk for deviant behavior
- Large crowds moving through high vehicle traffic areas are a risk for security personnel
- Parking lots are a threat for vehicle-borne improvised explosive devices (VBIED)

Crowd Management

- Security, ushers, ticket takers, concessions staff, and guest services representatives play a role in crowd management
- Staff and volunteers must be observant, and report unusual or inappropriate fan behavior
- Communication with fans is imperative, as communications are slower and more complicated with larger crowds

Network Security Monitoring

- Cyber protection is a major part of game/event day planning
- Cybersecurity plans are required at most facilities, and are supported by DHS and the FBI
- Cybersecurity technologies and techniques must protect Personal Identifying Information (PII)
- Facility infrastructure such as HVAC, lighting, video boards, etc., are protected from cyber intrusions

Legal and Regulatory Activities

- Facilities have to be compliant with regulatory requirements from local, state and federal agencies
- Legal issues can arise from inadequate security, or improper handling of ejections or arrests
- Certifications such as the SAFETY Act, and Sport Event Security Aware (SESA), may reduce venue insurance premium costs

Incident Management

- Natural disasters such as storms and lightning are some of the problems for facility operators
- Coordination during an incident bewteen security staff and first responders, some from different jurisdictions, is key for a facility manager
- Resource management, business continuity plans, and after action reporting (AAR), are important considerations before, during and after an incident

Defense Technology Applications Examples

Sport Security Activity		Associated Defense Technology
	Facility Management	Northrop Grumman's Automated Biometric Information System (ABIS)
	Parking Lot Security	Northrop Grumman's Fire Scout Unmanned Aerial Vehicle (UAV)
	Crowd Management	Cleveland Electric Laboratories fiber optic sensors for security applications and monitoring
	Network Security Monitoring	Qualcomm Technologies, Inc. Actionless Multifactor User Authentication
	Legal and Regulatory Activities	Radiance Technologies' Force Protection Alert Tool (FPAT)
	Incident Management	Defense Information Systems Agency Joint Incident Management System (JIMS)

Product Utilization

The product utilization section gives DoD technology providers a greater understanding of the products currently being utilized within the Commercial Facilities Sector. A snapshot list of the most widely used security tools within the industry and their uses are listed below. What is important to note about these products is that DoD technologies are easily transferrable to this safety and security sector as long as they meet certain requirements of security stakeholders.

Biometric Scan Software: The use of biometric scanners that control access to secure sites within the arena or facility has slowly increased over the last decade. Fingerprint, iris scan, and facial recognition software are utilized to secure restricted areas and monitor access control. Biometrics are already in use at some venues to ease ticket taking wait times, and the future of biometrics will allow fans to make purchases at concession stands simply by using their thumbprint. Biometrics will also have a major role in deterring criminal activity and identifying potential threats to a facility and people attending an event. The Biometric Scan Software industry generated an estimated $5.5 Billion in revenue for FY16, and due to the reliance on the technology from government agencies such as DHS, the industry is estimated to have 5.2% in annual growth from 2017-2022 (Curran, 2017). DoD investments in biometrics over the last decade have transformed the fight against terrorism in Iraq and Afghanistan. The Automated Biometric Information System (ABIS) developed by Northrop Grumman is one tool of the fight that has helped soldiers identify persons of interest with prior history of criminal activity within their area of operations (AO). "The Federal Bureau of Investigation, the Department of Homeland Security, and the National Ground Intelligence Center interface with ABIS to identify biometrics matches in support of U.S. criminal cases, border control, and intelligence watch lists, respectively" (DOT&E, 2013).

Electronic Access Control Systems: Facility stakeholders utilize access control products in a variety of different ways. Facility and event managers use access control systems to secure site sensitive areas, and concession staff use control systems to gain access to their work and supply areas. The most common access control product utilized is Personal Identity Verification (PIV) cards, which are important for identity management within a facility because of the simplicity and controllability of the technology and data used to control access. Access control data should be encrypted and tightly controlled in the event of a terminated/departing employee leaves a facility and to reduce the chances of insider threats. Event and facility security specialists are required to understand how their PIV systems are utilized, who has access, and work closely with their Chief Information Officer to integrate the PIV system. Electronic Control System Manufacturing industry revenue is expected to rise annually by 1.4% over the next 5-years, with rising profits leading to an estimated $3 Billion in revenue by 2022 (Rivera, 2017). One DoD technology example is of a new pilot program within the DoD for FY 2018 that is focused on replacing Common Access Cards with newer technologies that will also include biometric access control. A few of the uses these cards allows service members is to have access control to computer systems and restricted security areas. "The Department of Defense has awarded Qualcomm's Cyber Security Solutions (QCSS) division a contract to establish a pilot program for the Defense Information Systems Agency (DISA) to enable DoD users to access key IT systems using action-less authentication. The authentication is performed with Qualcomm's hardware-anchored device attestation and continuous multi-factor authentication capabilities on the Qualcomm Snapdragon Mobile Platform, integrated with DISA's Purebred and Public Key Infrastructure systems" (Burt, 2018).

Cybersecurity Tools: Identifying information technology (IT)-based vulnerabilities is a key activity of stakeholders within the sports security industry. "The US Justice Department estimates that more than 4,000 ransomware attacks have occurred each day since the beginning of 2016, meaning hackers engineer software programs that prevent employees from accessing their computer systems until a ransom total is paid" (O'Connor, et al, 2017). Each facility, particularly larger sports and entertainment venues, are required by law to have a cybersecurity plan in place. The DHS and the FBI can provide input and support in developing cybersecurity plans for facility managers if needed. Some of the most critical elements of a cybersecurity plan include protecting Personal Identifying Information (PII), HIPAA information, closed-circuit television (CCTV) data, and other personal and/or confidential information. Because nearly all of this information is stored in the cloud the need for security software publishing and IT consulting within the industry will be critical as investments into cybersecurity protection become more important for facilities and sports leagues/organizations. New Defense Federal Acquisition Regulation Supplement (DFARS) rules regarding cybersecurity safeguarding and cyber incident reporting that were implemented late in 2017, could generate opportunities for DoD technology providers to assist commercial facility security professionals in navigating these new rules and implementing safe practices of handling cybersecurity threats and reporting.

Protective Lighting: Consideration of proper lighting around facilities acts as a deterrent to criminal behavior. Concourses, entry/exit ways, and parking areas need to have proper lighting to enhance security, which can reduce the potential for litigation. Proper lighting also helps with the egress of spectators from a facility and helps prevent stampeding during a mass evacuation. In addition, pairing CCTV video equipment and various security lighting technologies acts as a force multiplier and offers more protection for infrastructure, spectators, and participants. The DoD has conducted research on improved applications of lighting for the military and military bases, however, currently no research exists on the strategic application of protective lighting in the sports safety and security industry, notwithstanding legal liability cases establishing precedent for lighting requirements.

Third-Party/Contracted Security: In the Commercial Facilities Sector, private companies usually own the venue hosting major sporting events. A significant part of security planning involves private security staff, who support law enforcement and venue/event security teams. Private security staffing companies also play a specific role in access screening, traffic control, crowd control issues, and crisis management. Regardless of the exact responsibilities assigned to private security companies, law enforcement is prepared to collaborate with these organizations to enhance the overall safety of the facility before, during, and after the event. Technology equipment specifically geared towards private security should be easy-to-use, solve a specific problem that cannot be solved using conventional means, and affordable for the third-party security firm or the facility management team.

Bomb Detection Tools: Perimeter security is vital to the safety and security of a facility. With underground parking garages available at some facilities, as well as numerous broadcast/media vehicles, team buses, and other credentialed vehicles that belong to players and staff, securing the inner, middle, and outer perimeters from Improvised Explosive Devices (IED) can be a difficult task. Typically, vehicle inspections performed at sport and entertainment facilities are conducted manually by visually inspecting the inside and outside of the vehicle using undercarriage mirrors to aid in the outside inspection. There is also an assist from law-enforcement bomb detection dogs, and similar third-party bomb-sniffing canines. Technology aimed at neutralizing a bomb/IED at a sporting venue should be easy-to-use, unobtrusive in size, and modular.

Market Segments

The market for the sports and special event security sector can be broken into three segments, each with a different procurement process, but they are the drivers of the purchase of new security technologies:

1. Facility Owners/Security Managers
2. Sports Leagues/Venue and Event Management Companies
3. Emergency Managers

Facility Owners/Security Managers: These are drivers of the sports security industry, who are focused on taking a proactive approach to safety and security. Owners and security managers work closely together to develop security plans for events and facilities. Both parties recommend security budgets for new safety technologies and security contracts. Considering the inherent risks posed to sports and special events, facility owners and security managers have a legitimate concern for the safe and secure operations of their site(s) because of the potential financial, legal and economic consequences resulting from a security breach or emergency incident. Careful consideration for the types of safety and security technology and procedures that are implemented which, in most cases, depends on the facility's specialized threat assessment. Technology costs is the major driver of this segment.

Sports Leagues/Venue and Event Management Companies: This segment of the market is different in a few areas from Facility Owners and Event Managers. Safety and security guidelines put out by sports leagues and venue and event management companies (i.e., AEG, SMG, and Live Nation) are mandatory requirements for facilities hosting their respective events, regardless of the facility's threat assessment. Marketing to this segment requires heavy vetting of the new technology before reaching out to the security offices of the respective league because leagues are inundated with new security technologies every year, going through NCS4's National Sport Security Laboratory (NSSL) may be the better option for companies looking to bring their products to major league facilities. Sports leagues and venue and event management companies will differ from each other in their respective groups (i.e., the NFL has different safety rules from MLB); because of this variation research is needed to see what best practices leagues and companies are currently following. Sports leagues also rely on multiagency collaboration to host bigger sporting events such as the NFL's Super Bowl. These collaborations involve meetings, trainings, and exercises with key external agencies such as the FBI, DHS, local law enforcement agencies, third-party security companies, hazardous materials experts, EMS, etc.

Emergency Managers: This group represents EMS, fire and government agencies such as the FBI and DHS, who plan for, protect against, respond to, and mitigate the potential consequences of all-hazard type incidents. Emergency Managers are looking for equipment that can protect people and infrastructure, assist in training, and have an easy-to-use interface that can be transferrable between different sports and special events. The technology should also be transferable between national, state and local safety officials. Marketing to this segment can be difficult based on the acquisitions process required by local or state laws, which in some states and local communities require third-party approval for acquiring new safety products. Emergency managers are more accessible to new security technologies through trade shows that can display a provider's technology capabilities, and this segment uses the RFI/RFP process to acquire technology above a certain price point.

Key External Drivers

The sports and special event security industry is steadily growing as corporate profits within those business sectors continue to increase. With a continual emphasis on supporting a safe and secure environment from stakeholders, government agencies and public safety agencies, there will be a need for new and proven technologies to enhance security levels currently seen at sports and special events. As the number of large sport and entertainment, events increase worldwide, stakeholder demand for additional crowd control and infrastructure protection measures will continue to see unparalleled growth. DoD technology companies should understand that each external driver is going to push industry stakeholders to seek out new or existing products to expand their security footprint.

Facility Construction/Renovation: Professional sports venues, and a growing number of collegiate athletic departments, are reaching the end of new facility construction that has been a key driver of the sports safety and security industry over the last two decades. Since 1996, more than $32 Billion was spent on 83 venues across the five major sport leagues (PwC, 2017). This construction boom coincides with league and collegiate athletic department television revenues skyrocketing at the turn of the century, and the importance placed on new revenue streams such as stadium naming rights and premium seating options. "The availability of public funding sources and financing options were also key drivers to realizing the current generation of venues serving the five major leagues in North America. Public sources have funded more than 40 percent of the aggregate cost to develop major league facility projects since 1996" (PwC, 2017). With investment from revenue streams into new stadiums and infrastructure comes investment into security technologies for those facilities.

League Expansion: Expansion of the five major sports leagues in the United States has increased the need for more security, as these new franchises begin to draw larger crowds and major events to their facilities. While expansion of sport leagues takes considerable time, Major League Baseball (MLB), National Hockey League (NHL), and especially Major League Soccer (MLS), have all expressed interest in expanding their respective leagues over the next decade. MLS particularly will be looking to expand by four new franchises by 2022. League expansion also includes the monetization of digital media rights in the US and overseas, as international expansion continues to be seen as a growth market for sports leagues and franchises. "With a potential global market size of more than $1 Billion by 2025, immersive sports media will remain a nascent market relative to other media segments, but a viable source of prospective sports market expansion" (PwC, 2017).

Increase in Crime/Terrorism: A steady increase in crime and terrorist activity has contributed to the need for additional protections and greater security technologies. For instance: terrorist acts such as the Manchester Arena bombing, where 23 people were killed and hundreds more injured after a concert, led to changes in security protocols and egress procedures. As mega-sporting events continue to garner more visibility around the globe, there is an even greater appeal to criminals and terrorists to target these types of events.

Fan Engagement: Sports leagues across the country have reported decreased attendance over the last decade as television access to games has increased during the same period. Event promoters and other facility stakeholders have begun to strengthen the fan experience at sporting events, which has created new challenges for security managers to address. These fan engagement areas have increased the need for easy-to-use mobile security products, in addition to more private or third-party security, as the

security footprint of a facility expands to include fan engagement areas. Sports leagues are set to engage with fans in new and exciting ways that will be important to the future growth of sports around the world. Digital products that immerse the fan in the sporting experience will be one avenue, "With a potential global market size of more than $1 Billion by 2025, immersive sports media will remain a nascent market relative to other media segments, but a viable source of prospective sports market expansion" (PwC, 2017).

Current Industry Performance

With a continual emphasis on supporting a safe and secure environment from industry stakeholders, government agencies and emergency managers, there will be a continuous need for new and proven technologies to improve security levels currently seen at sport and special events. As the number of big sporting events are increasing in popularity worldwide, stakeholder demand for technologies that support safe crowd control operations, and protection of critical infrastructure, will require technology advancements that are common with DoD technologies currently in use.

Industry Outlook

The sports security industry is going to continue to see year-to-year growth as external factors continue to bring corporate profitability to the sports business sector. U.S. sport league expansion, and new television revenue streams, will provide funding industry stakeholders to improve facility design features and enhance fan engagement with assistance from facility security departments. Competition within the technology market is continuing to push technologies in the sports security sector. Ease-of-use technologies implemented at facilities around the world in place of staffed security services will be a key industry driver. Staffed security services will still play an active role in facility and event security, acting as a deterrent for crime and strengthening loss prevention. The use of technology will also facilitate easier access to events, deter fraudulent behavior, and shorten wait times at concessions, which are all important to industry stakeholders in providing quality guest services.

Industry Demand

Industry demand is built largely on the security needs of sports leagues, venue and event management companies, federal agencies, emergency managers, and security managers. Security measures are not the same for every event or venue, and will depend on multiple factors including, but not limited to, the size of the event, identified risks, and available resources. As large sporting events continue to expand internationally, this newfound worldwide platform presents sporting event stakeholders with unique security issues. The business of sports and entertainment events offer companies willing to enter this industry a huge opportunity to diversify and grow in many different areas that ultimately meet the demands of the global sport and special event industry.

Industry Supply Chain

Buyers

Facility Operators
Federal Agencies
Emergency Managers

Selling Industries

Part-time Security Services
Audio & Video Equipment Services
Cloud Based Computer Services
Metal Detection Providers
Biometric Identificaion Companies
Security Lighting Copmanies
Bomb Detection Services
Contracted Security Service Providers
Social Media/GIS Monitoring Companies

Major Industry Markets

Sports Leagues: Sports venues and teams are tasked with implementing game day security parameters established by their leagues. Each major sport league has its own set of guidelines or "best practices" that direct safety and security operations, (i.e., the National Football League has different safety and security best practices than the National Basketball Association). A new business looking to enter the Commercial Facilities Sector through this market needs to be in contact with each respective league's security office, to understand their individual security needs and best practices.

Facilities: Facility design features, including security upgrades and enhancements, are the largest market driver of the commercial facilities sector. A new business in this sector should remember that what works for one facility might not work at all facilities. Consistent communication with facility security directors and customization capabilities are paramount. Products must be affordable, easy-to-use, and transferable to be considered for use.

Government Entities: This market operates under strict governmental budgets, and new technologies need to solve an immediate problem to be considered for purchase. New technologies need to provide ease-of-use, operate on a mobile platform if needed, and be secure from hacking. Purchases need to be delivered in a timely manner to offer training and support of those using the product in the field.

International Sport Governing Bodies: International sporting events such as the Olympics and FIFA World Cup present special challenges to security managers. The size of the audiences, number of participants, and different event locations, are just a few examples of the security complexities that security managers must deal with when planning for these types of events. The level of exposure that international sporting events bring presents very credible terrorist threats to facilities, crowds, and participants. Spending on security for these events has continuously increased for the host nation. For example, in 2012 London spent $1.6 Billion on security for the Summer Olympics, just four years later in Brazil nearly $4.6 Billion was spent on security and security technologies.

Small Business Partnerships: Small businesses that can provide a security solution to address the unique problems found in the sports security sector can develop and flourish within the industry. A small business' ability to meet customization needs, and the flexibility to design platforms that meet the needs of the different environments (between small and large venues for instance) is an advantage in meeting the demands of stakeholders within the industry.

SAFETY Act Certification: Becoming SAFETY Act designated by the DHS enables security solution providers to have a competitive edge in the marketplace and gets their product to consumers in the commercial facilities sector faster. The SAFETY Act's intentions are to provide incentives for the development and deployment of anti-terrorism technologies. For more info go to: https://www.safetyact.gov

National Sport Security Laboratory (NSSL) certification: The NSSL is the link between safety and security experts in the field with manufacturers and solution providers. NSSL is the research and development arm of the National Center for Spectator Sports Safety and Security (NCS4) and is an important piece for businesses that want to enter the industry to have their products tested by industry practitioners and students from the University of Southern Mississippi's Sport Security Management program. For more info go to: https://www.ncs4.com/labportal

Market Share Concentration

Market share concentration in the Commercial Facilities Sector is currently MEDIUM. There is a growing trend to bring small business solutions to the industry if the solution makes sense financially and has a simple easy-to-use platform.

Key Success Factors

Easy-to-use Products

Industry products should be user friendly for security staff to set-up and effectively use. Products should also be easy-to-use for spectators if they are the end-user.

Cost Effective Technologies

Clients operate under tight financial restrictions. Industry products need to secure people, facilities, and infrastructure without breaking the budgets of their respective security departments.

Modular Products

Industry products that can effectively secure a facility and transported easily to other areas around the facility are in demand. The ability for a product to be dual-use is also an advantage for a product.

Proper Certifications

If the product or service is SAFETY Act certified by the DHS and meets all federal safety requirements, those products are considered for purchase over those that are not certified.

Procurement

Safety and security professionals in the industry will occasionally use Request for Information (RFI) or Request for Proposal (RFP) to procure new security technologies, services or products. Of the 14 responses to our industry marketing survey, eight of them said they use this process of procurement. Most RFI/RFPs do not require a minimum pricing point, but there are some that require this method if it is $15,000 or above for a new product of service. This is similar to the DoD who uses the RFP process for tradeoff source selection. Tradeoff source selection allows the Federal Government to use RFPs to evaluate other than lowest price or highest tech rated technologies, when the technologies offer superior performance, lower risks or innovative and technologically superior solutions (DoD, 2016)

The purchase of new technologies within the DoD is a bureaucratic process, that can take months to years for the final purchase of the technology. DoD point of purchases are usually sole source procurement, procurement under an existing multiple award contract, or normal procurement. Sole source is when there is only one business to fulfill the obligations of the awarded contract, and the Federal Government documents this extensively because this point of purchase is so rare. Multiple award contracts are a type of contract that is awarded to several contractors from a single RFP or solicitation. Normal procurement is used for simplified procurement (which are contracts below $25,000), and purchases over $25,000. Purchases over $25,000 are publicized on the Federal Business Opportunities (FBO) website, where RFP documents are available for download and review.

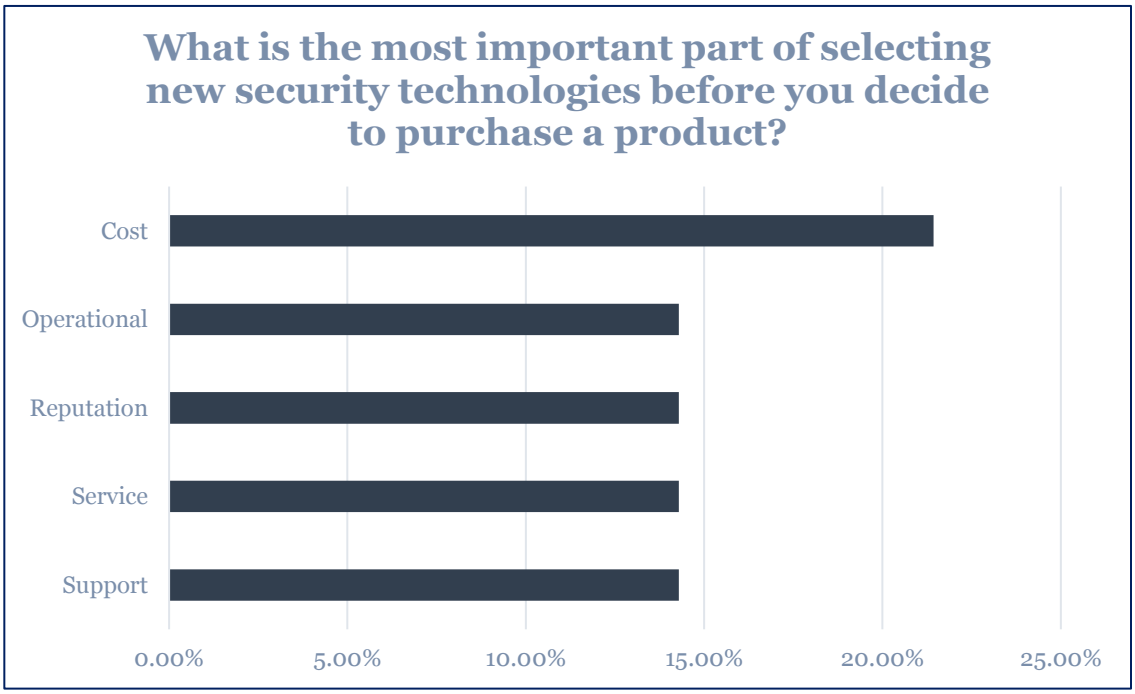
Pricing

Pricing Strategy

Pricing within the DoD is controlled by the Defense Pricing (DP) process. The Director of Defense Pricing reports to the Office of the Secretary of Defense (OSD) to oversee the OSD Better Buying Power Initiatives and ensure that the Federal Government is receiving the best pricing available for the procurement of new defense system technology and programs. In the Commercial Facilities Sector, pricing is the most important part of selecting new security technologies for purchase. Consumers in the Commercial Facilities Security Sector are price sensitive; Figure 1 is from the marketing small business technologies to the Commercial Facilities Sector survey sent to industry professionals. The prime aspect of selecting a new security technology, or the difference in winning the bid on a project, relies on the cost of the product to the consumer. Budgets for professional sporting venues are the largest in the industry, but for collegiate and smaller commercial facilities, budgets are tighter which means there must be clear value provided by the product to be selected for purchase.

A key pricing strategy that could be effective for a new company entering the Commercial Facilities Sector would be using the penetration pricing strategy. New technology providers should look to penetration pricing as they first enter the market with lower prices in mind to develop a brand within the sports security industry. Reputation is relatively important to stakeholders as well, and new technology providers should keep that in mind as they enter the marketplace using penetration pricing. Penetration pricing is one method that develops a strong reputation with customers, especially if the product can be customized and priced affordably. Something to keep in mind for technology providers as they price their product to the Commercial Facilities Sector, is that federal grants are available for some facility security professionals to help fund the purchase of new technologies. The key to acquiring these grants is that the technology must have a direct tie-in to preventing terrorism. It can be for prevention, preparedness or response, but there must be a clear link to preventing terrorism. Warranties for new technology security products should last longer than 12-months and have the proper certifications and designations.

Figure 1

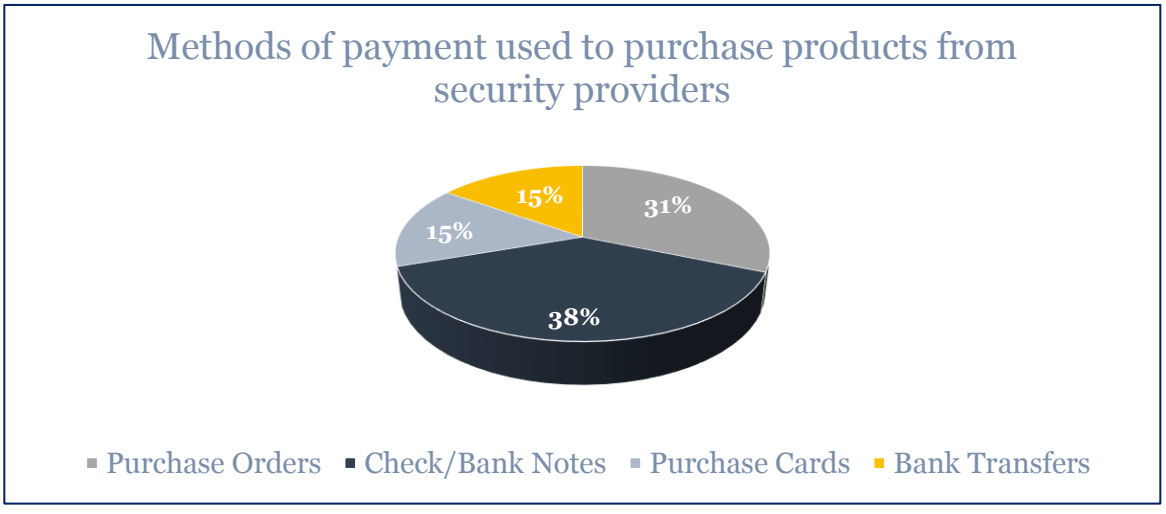


(Marketing small business technologies to the Commercial Facilities Sector survey, 2018)

Methods of Payment

For the DoD, receiving payments for goods and services from contracts can be a lengthy process. DoD uses the Defense Finance and Accounting Service (DFAS) to make transferrable payments to businesses under contract with the department. Safety and security professionals in the Commercial Facilities Sector use a variety of methods to pay for safety and security technology. Figure 2 represents the percentage of responses received from our group of industry professionals on the methods they use to pay vendors. Check/Bank notes are the most common of the 14 responses we received, and another method industry professionals use to complete purchases with vendors is the use of purchase orders.

Figure 2



(Marketing small business technologies to the Commercial Facilities Sector survey, 2018)

Placement

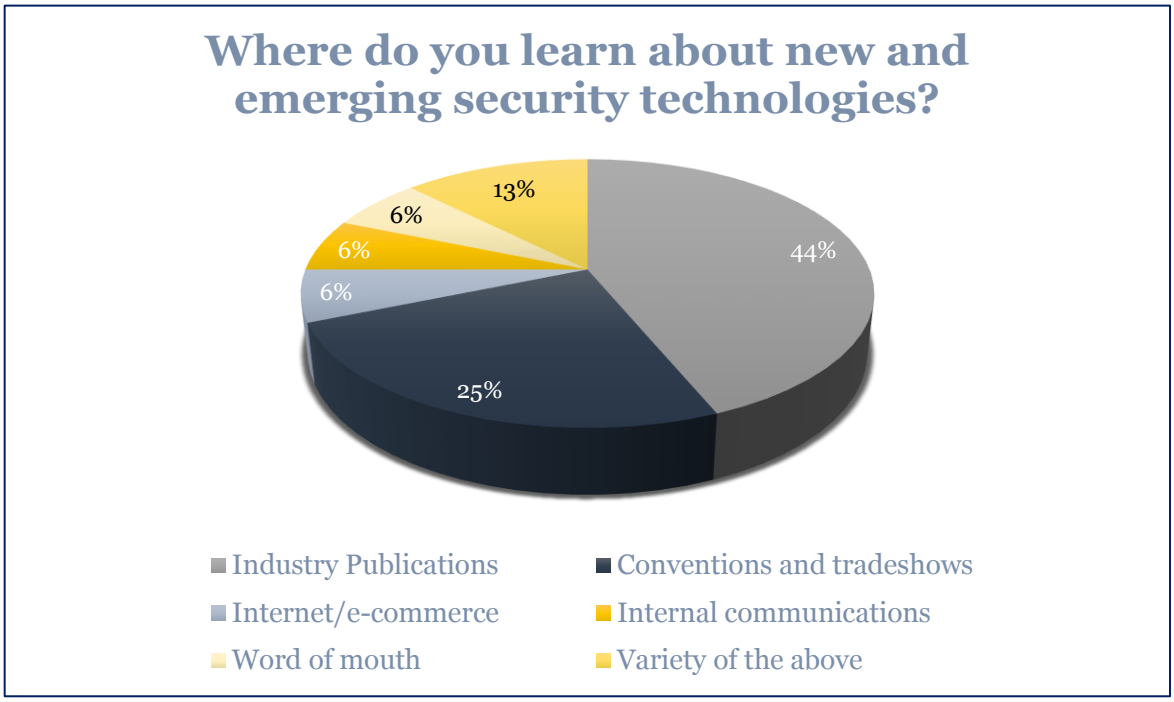
Direct sales are the most common method of engagement with security technology customers. Direct selling requires one-on-one marketing and selling of a product between a producer and a consumer, that is away from a fixed retail location. The most common points of purchase for new products and technologies for commercial facility security professionals are at trade shows or industry conferences, such as NCS4's National Sports Safety and Security Conference or Commercial Sport and Entertainment Facilities Summit. These points of purchases are done using company sales representatives, who can engage customers, provide a demonstration of their products, and schedule further demonstrations at their commercial facilities. Internet sales are common within the industry as another method of direct sales to customers, but the engagement between customers and sales people are the most important aspect of selling a product to the commercial facilities safety and security sector.

Industry Conferences and Trade Shows	Conference Info
NCS4 National Sports Safety and Security Summit NCS4 Commercial Sport and Entertainment Facilities Summit NCS4 Intercollegiate Summit NCS4 Marathon Summit NCS4 Interscholastic Summit	https://www.ncs4.com/events
International Security Conference & Exposition West/East	http://www.iscwest.com/ISC-Events/
International Association of Venue Managers Venue Connect	https://www.iavm.org/
Stadium Managers Association Annual Seminar	https://www.stadiummanagers.org/

Promotion

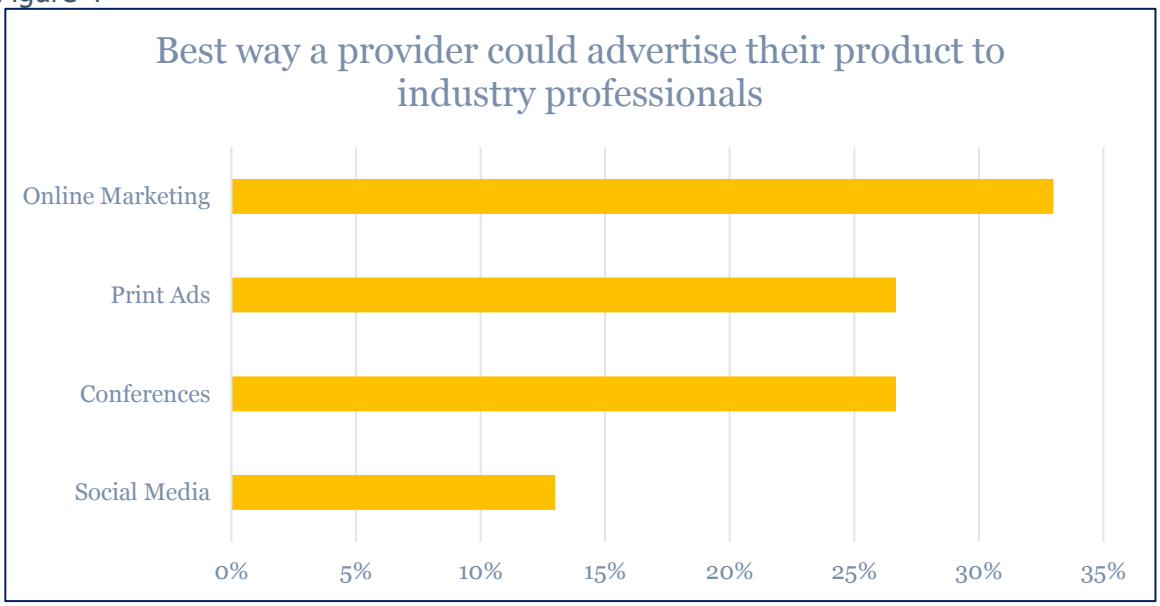
Promotion of security technology to the Commercial Facilities Security sector involves being active at industry conventions and tradeshows and promoting in industry publications (e.g., Athletic Business, Gameday Security Magazine, etc.). Both of these promotional avenues are the most popular avenues to gain exposure to industry decision makers on the procurement of new security technology. Figure 3 shows the percentage of professionals surveyed within the commercial facilities industry for this document, and how they are exposed to new and emerging security technologies. The best way to advertise to the commercial facilities security sector is through print ads in industry publications, social media engagement, online marketing such as website sponsorship and electronic mail outs, and in-person at conferences and trade shows (see Figure 4).

Figure 3



(Marketing small business technologies to the Commercial Facilities Sector survey, 2018)

Figure 4



(Marketing small business technologies to the Commercial Facilities Sector survey, 2018)

Conclusion

The conversion from a DoD technology provider to a Commercial Facility Sector security technology provider is a seamless transition. Many DoD technologies currently are being utilized at sporting and special event facilities across the country. Technologies must meet the safety objectives of the facility, event and security managers, and emergency services, and meet the certification requirements of the DHS. Potential technology providers need to be conscious of their pricing of products to the industry because stakeholders are particularly price sensitive. Having a strong online and print advertisement marketing presence and participating in industry-wide conferences will lead to connections within the industry, which will assist in the research and development of new products and lead to implementation of new technology in facilities. The Commercial Facility Sector is showing steady growth that parallels the growth and expansion of sporting events and leagues in United States and around the world. DoD technology providers can diversify into this market and find themselves at the forefront of innovation for the safety and security industry of sports and special events.

References

Amoros, R. (2016). Which professional sports leagues make the most money. *How Much*. Retrieved from https://howmuch.net/articles/sports-leagues-by-revenue

At the gate and beyond: Outlook for the sports market in North America through 2021. *PricewaterhouseCoopers*. Retrieved from https://www.pwc.com/us/en/industry/entertainment-media/publications/assets/pwc-sports-outlook-2017.pdf

Bohlin. M. (2016). NBA revenue projected to reach $8 billion next season. *CBS Sports*. Retrieved from https://www.cbssports.com/nba/news/report-nba-revenue-projected-to-reach-8-billion-next-season/

Brown, M. (2017). MLB sets record revenues in 2017, increasing more than $500 million since 2015. *Forbes*. Retrieved from https://www.forbes.com/sites/maurybrown/2017/11/22/mlb-sets-record-for-revenues-in-2017-increasing-more-than-500-million-since-2015/#31ade84f7880

Burt, C. (2018). Qualcomm awarded DoD contract for IT system access protection pilot. *Biometric Update*. Retrieved from https://www.biometricupdate.com/201801/qualcomm-awarded-dod-contract-for-it-system-access-protection-pilot

Commercial Facilities Sector (2017). *Department of Homeland Security*. Retrieved from https://www.dhs.gov/commercial-facilities-sectorc

Commercial Facilities Sector-Specific Plan (2015). *Department of Homeland Security*. Retrieved from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf

Conn, D. (2017). Premier League remains world's richest courtesy of huge TV revenue growth. *The Guardian*. Retrieved from https://www.msn.com/en-gb/sport/premier-league/premier-league-remains-world's-richest-courtesy-of-huge-tv-revenue-growth/ar-BBEg3xi

Curran, J. (2017). IBISWorld Industry Report OD4530: Biometric Scan Software in the US. *IBISWorld*. Retrieved from www.ibisworld.com

D'Allegro, J. (2017). Super Bowl billions: The big business behind the biggest game of the year. *CNBC*. Retrieved from https://www.cnbc.com/2017/01/20/super-bowl-billions-the-big-business-behind-the-big-game.html

Defense Federal Acquisition Regulation Supplement Procedures, Guidance and Information (2016). *Department of Defense*. Retrieved from https://www.acq.osd.mil/dpap/policy/policyvault/USA004370-14-DPAP.pdf

DoD Automated Biometric Information System (ABIS). *The Office of the Director, Operational Test and Evaluation*. Retrieved from http://www.dote.osd.mil/pub/reports/FY2013/pdf/army/2013dodabis.pdf

Haddon, A. (2016). Is hosting the Olympics ever worth the cost? *Quartz.* Retrieved from https://qz.com/753250/rio-2016-is-hosting-the-olympics-ever-worth-it/

Hall, S., Cooper, W., Marciani, L., & McGee, J. (2012). *Security management for sports and special events: An interagency approach to creating safe facilities*. Human Kinetics.

Kaplan, D. (2017). NFL revenue reaches $14B, fueled by media. *Sports Business Journal*. Retrieved from https://www.sportsbusinessdaily.com/Journal/Issues/2017/03/06/Leagues-and-Governing-Bodies/NFL-revenue.aspx

O'Connor, C., Lifschutz, M., Hadad, J. (2017). Cybersecurity challenges: Industries affected by cybercrime. *IBISWorld*. Retrieved from https://www.ibisworld.com/media/2017/09/08/cybersecurity-challenges-four-industries-affected-by-cybercrime/

Rivera, E. (2017). IBISWorld Industry Report OD4477: Electronic Access Control System Manufacturing in the US. *IBISWorld*. Retrieved from www.ibisworld.com