Journal of Air Law and Commerce

Volume 82

2017

Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them

J. Peter Greco
Kirstein & Young, PLLC, me@jamespetergreco.com

INSIDER THREAT: THE UNSEEN DANGERS POSED BY BADGED AIRPORT EMPLOYEES AND HOW TO MITIGATE THEM

J. Peter Greco*

I. PROBLEM STATEMENT

Security breaches involving badged airport employees[1] are a growing risk in today's commercial aviation industry. Currently, at almost every commercial airport in the United States, employees of airports, airlines, purveyors, and other tenants enjoy unfettered access to the airport's Security Identification Display Area (SIDA), sterile, and secured areas. In recent years, there have been several high profile incidents deriving from this freedom of movement and lack of oversight which have resulted in the introduction of dangerous contraband into the aviation system.

Several alternatives can be implemented to combat this problem. What is perhaps the most effective of these is also the most expensive: promulgating regulations that require 100 percent screening of all airport employees entering the SIDA. Other proposals include increasing background investigations into airport badgeholders, increasing penalties for violations of airport security rules as a means of preventing at-risk employees from

* Pete Greco is a Spring 2017 graduate of the Antonin Scalia Law School at George Mason University in Arlington, Virginia. Currently, he works as an associate at Kirstein & Young, PLLC, an aviation law firm in Washington, D.C. Prior to attending law school, Mr. Greco earned a Bachelor of Science degree in Aviation Business Administration from Embry-Riddle Aeronautical University in Daytona Beach, Florida and worked as an Airfield Operations Specialist at Orlando International Airport in Orlando, Florida. Mr. Greco is an FAA-certified private pilot with instrument rating and is licensed to practice law in the State of Florida.

[1] It is important to note that, for the purposes of this analysis, "airport employees" refers not just to the employees who work for the airport operator itself but to any employee that works at a given airport and holds an airport identification badge from that airport.

ever obtaining a SIDA badge, or deterring such badgeholders from misusing their access media.

Risks involving airport badgeholders grow more prevalent by the day. Immediate change and rulemaking is needed if our commercial aviation system is to remain as safe and secure as it is today.

II. BACKGROUND

To properly understand this subject, a brief history of airport security regulation is required. In the early years of commercial aviation, airport security was almost entirely non-existent.[2] Passengers could walk straight from the curb to their aircraft without passing through any sort of inspection station, and today's concept of a so-called "sterile" area—the area beyond the security-screening checkpoint—had not yet been created.[3] As a result, even non-ticketed persons could walk onto any aircraft parked at the gate, into the gate area itself, and—due to the lack of screening—carry with them virtually anything.[4] Naturally, because airline passengers were unrestricted as far as security was concerned, airport employee security concerns were irrelevant: no one was inspected unless they exhibited suspicious behavior; thus, there was no risk of an employee using their access privileges to circumvent such inspection.[5]

Then, between 1968 and 1972, the number of hijackings of commercial air carrier flights increased sharply.[6] These hijackings were largely nonviolent, with hijackers generally requesting the aircraft be rerouted to Cuba before some sort of peaceful conclusion to the incident was reached.[7] However, these incidents drew attention to the security concerns facing commercial aviation and, on January 5, 1973, the Federal Aviation Administration (FAA)—as the federal regulatory agency governing aviation—promulgated 14 C.F.R. § 107, for the first time laying out

---

[2] Bryan Gardiner, *Off with Your Shoes: A Brief History of Airport Security*, WIRED (June 14, 2013, 6:30 AM), https://www.wired.com/2013/06/fa_planehijackings [http://perma.cc/9L5N-B58J].

[3] *Id.*; *Booking a Flight for the 'Golden Age of Hijacking'*, NPR (Dec. 27, 2013, 4:11 PM) www.npr.org/2013/12/29/257659576/booking-aflight-for-the-golden-age-of-hijacking.

[4] *Id.*

[5] Gardiner, *supra* note 2.

[6] *Id.*

[7] Brendan I. Koerner, *How Hijackers Commandeered Over 130 American Planes – in 5 Years*, WIRED (June 18, 2013, 6:30 AM), https://www.wired.com/2013/06/love-and-terror-in-the-golden-age-of-hijacking/ [http://perma.cc/SJ6Y-XVVY].

detailed and specific requirements for aviation security.[8] Part 107 contained requirements for airport operators insofar as mandating some degree of background checks on employees and the installation of access control devices at airports.[9] It also required that all airlines hire private security contractors to screen every departing passengers, as the government did not yet serve this function.[10] However, these security measures contained many deficiencies and presented many opportunities for exploitation, as will be explored further *infra*.

Airport security regulation remained relatively stagnant until the terrorist attacks of September 11, 2001. Immediately thereafter, on November 19, 2001, the Aviation and Transportation Security Act was passed,[11] creating the Transportation Security Administration (TSA) and shifting responsibility for aviation security away from the FAA.[12] Originally, this agency operated under the Department of Transportation until it was transferred to the Department of Homeland Security in 2003.[13] Unlike under the FAA's Part 107, TSA employees themselves—with the exception of a number of airports who have opted to supply their own screeners—handle the majority of passenger screening operations.[14] Additionally, the requirements set forth under the TSA's 49 C.F.R. § 1540 and § 1542 are substantially stricter than all prior precedent: (1) the "sterile" area post-security screening was created and limited to only ticketed passengers; (2) the SIDA—or the non-public areas of an airport where display of an airport ID badge is compulsory—was created; the so-called "3-1-1 rule" was created; (3) enhanced x-rays and millimeter-wave detection systems began to be utilized; and (4) permitted items onboard aircraft were substantially reduced, to name just a few examples.[15]

---

[8] Theresa L. Kraus, *The Federal Aviation Administration: A Historical Perspective, 1903–2008*, at 48–49 (U.S. Dep't of Transp. 2008), https://www.faa.gov/about/history/historical_perspective/media/historical_perspective_ch4.pdf (Chapter 4: New Challenges – New Duties) [http://perma.cc/CEC9-5X6L].

[9] 14 C.F.R. § 107 (2016).

[10] *Id.*

[11] Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101, 115 Stat. 597 (2001).

[12] 49 U.S.C. § 40101 (2012).

[13] *Transportation Security Administration*, FEDERAL REGISTER, https://www.federalregister.gov/agencies/transportation-security-administration [https://perma.cc/P6AX-LTMF].

[14] 49 U.S.C. § 40101.110(b).

[15] 49 C.F.R. §§ 1540.105, 1540.107, 1540.111, 1542.103 (2016).

Under the current regulatory framework, each and every commercial airport certificated by the FAA under 14 C.F.R. § 139 must also comply with the provisions of Part 1542.[16] Part 1542 lays out a number of requirements that airports must meet in order to serve commercial air carrier operations. Paramount to these is the requirement to create, maintain, and follow a TSA-approved Airport Security Program (ASP) which lays out in great detail how the airport will comply with each of the requirements of Part 1542.[17] Airports are also required to appoint an Airport Security Coordinator who is charged with enforcing Part 1540, Part 1542, and the ASP on all airport users.[18]

Airports are also required to: (1) create a unique, color-coded badging system that limits airport access based upon employment needs; (2) designate areas of the airport as the SIDA, sterile, and secured areas; train employees on security policies and practices; (3) maintain a CCTV system; (4) conduct random audits and testing; and (5) facilitate background investigations on SIDA badge applicants.[19] In doing such background investigations, airport operators must conduct both TSA-administered Security Threat Assessments as well as FBI-administered Criminal History Records Checks (CHRC).[20] If a SIDA badge applicant has committed one or more of the TSA-designated twenty-seven disqualifying offenses, the applicant is ineligible to receive a SIDA badge.[21]

Badged employees may use their access cards to bypass the TSA passenger checkpoint; however, they must submit to screening at that checkpoint should they choose to report to work through the main sterile area entrance.[22] Additionally, airports deploy a wide range of access control technologies, ranging from a numeric keypad with a personal identification number (PIN), all the way to biometric security systems.[23] Badgeholders flying out of the airport on commercial flights must submit to normal passenger screening.[24] Airport ID badges

---

[16] *Id.* §§ 1542.3, 1542.101 (2016).

[17] *Id.* § 1542.103 (2016).

[18] *Id.* § 1542.3 (2016); *see also* Telephone Interview with Justin T. Grindell, A.C.E., K-9 Handler, Greater Orlando Aviation Authority (Nov. 29, 2016) [hereinafter Telephone Interview with Justin T. Grindell] (on file with author).

[19] Telephone Interview with Justin T. Grindell, *supra* note 18.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

can be deactivated remotely at any time in the event of a lost or stolen card, repeat security violations, or a disgruntled former employee who has declined to return his or her ID badge.[25] Violations of local airport security policies or federal security regulations carry a range of penalties, ranging from a temporary badge suspension or a small fine payable to the local airport operator to civil penalties assessed by the TSA or criminal penalties including jail time and a substantial fine.[26]

Having presented a background on the state of airport security in general, it is now possible to detail the security concerns that exist with airport and airline employees (or badgeholders). The most prudent means of accomplishing this is by analyzing the highest profile and most serious incidents that have occurred as a result of a badgeholder misusing his or her access privileges in some way.

One of the earliest of these such incidents occurred just over ten years following the FAA's promulgation of Part 107.[27] It involved PSA Airlines Flight 1771 on December 7, 1987. Flight 1771 was a scheduled flight from Los Angeles to San Francisco.[28] It was operated by a British Aerospace BAe 146-200 and was carrying forty-three passengers and crewmembers.[29] David Burke was a disgruntled former employee of then-called USAir, the parent company of PSA.[30] He had recently been terminated by USAir on allegations of stealing from the proceeds of in-flight cocktail sales, but he had not surrendered his USAir employee identification badge. Using this badge, Burke was able to smuggle a .44 Magnum revolver onto Flight 1771 undetected, and when the aircraft was at cruising altitude, shot and killed both pilots and several passengers, resulting in the aircraft crashing and the deaths of all onboard.[31]

---

[25] *Id.*

[26] *See, e.g.*, 49 U.S.C. § 46314(b) (2011); 49 U.S.C. § 46301(a)(4) (2016).

[27] Ed Magnunson, *David Burke's Deadly Revenge*, TIME (June 24, 2001), http://content.time.com/time/magazine/article/0,9171,145653,00.html.

[28] Eric Malnic, *Report Confirms That Gunman Caused 1987 Crash of PSA Jet*, L.A. TIMES (Jan. 6, 1989), http://www.latimes.com/la-me-report-gunman-caused-1987-psa-crash-19890106-story.html [https://perma.cc/66GQ-TKDQ].

[29] *Id.*

[30] *Id.*

[31] Michael Taylor, *PUBLIC SAFETY: Preventing Air Crime: Better Security Won't Stop Determined Terrorists, Experts Say U.S. Still Has Not Done Enough*, SFGATE (Feb. 10, 2002, 4:00 AM), http://www.sfgate.com/news/article/PUBLIC-SAFETY-Preventing-Air-Crime-Better-2874548.php [http://perma.cc/22MK-2D4Q].

Seven years later, another high profile aviation incident involving a disgruntled airline employee occurred. On April 7, 1994, Federal Express Flight 705, a McDonnell Douglas DC-10 aircraft on a scheduled flight from Memphis, Tennessee to San Jose, California, was hijacked by Auburn Calloway, a FedEx flight engineer who was facing termination for lying on his employment application about his total flight time.[32] Calloway bypassed security screening and accessed Flight 705 as a deadhead passenger.[33] In his guitar case, he carried several hammers and a speargun.[34] His plan was to disable the DC-10's cockpit voice recorder, kill the crewmembers with hammers to simulate injuries consistent with an aircraft crash, and fly the aircraft into the ground so that his family would be able to collect on a $2.5 million life insurance policy provided by the company.[35] However, despite the horrific injuries inflicted upon them by Calloway, crewmembers were able to subdue him and land the aircraft safely.[36]

Fortunately, due to updated regulations promulgated as a result of these two incidents that require the full screening of all employees traveling outbound on commercial flights as a passenger, incidents as severe as these have not occurred again. However, security issues involving airport badgeholders are still very prevalent, and in recent years, incidents involving these individuals have been on the rise. These "new wave" breaches are designed to be well disguised and are extremely different in nature than the two discussed *supra*.

Perhaps the most notable of these modern employee security breaches occurred between May and December 2014 at the William B. Hartsfield-Jackson Atlanta International Airport (Atlanta International Airport) in Atlanta, Georgia.[37] Atlanta International Airport is the busiest airport in the world, and as such, a major breach in security there is particularly troubling. Two men, one a Delta Air Lines employee and the other a non-employee accomplice, worked together to smuggle over 153 guns

---

[32] Penny Rafferty Hamilton, *Life Changer – The Horrific Story of FedEx Flight 705*, ST. AVIATION J. (Oct. 30, 2011), http://stateaviationjournal.com/index.php/news/life-changer-horrific-story-fedex-flight-705 [https://perma.cc/JXE7-3EM3].

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Ashley Fantz et al., *DA: Guns Smuggled on Planes in Atlanta an 'Egregious' Security Breach*, CNN (Dec. 30, 2014, 10:50 PM), http://www.cnn.com/2014/12/23/us/delta-employee-gun-smuggling/index.html [http://perma.cc/HS29-RK6R].

and ammunition on several commercial Delta Air Lines flights.[38] Eugene Harvey, the Delta employee, used his SIDA badge to bring the suitcase full of guns and ammunition around the security checkpoint and up to the sterile area, where his accomplice, Mark Quentin Henry, would meet him in the bathroom after clearing the TSA passenger checkpoint.[39] Henry would then take the suitcase full of contraband from Harvey and board flights bound for New York, which he did at least twenty times.[40] Two assault rifles and 129 handguns were supplied altogether using this technique.[41] Several of the handguns were loaded while being transported by Henry in the aircraft's overhead compartments.[42]

Prior to the Atlanta incident, in March 2007, now-defunct Comair Airlines employee Zabdiel J. Santiago Balaguer used his SIDA badge at Orlando International Airport in Orlando, Florida to smuggle guns and drugs aboard several Delta Air Lines flights to Puerto Rico.[43] Santiago Balaguer would bring the contraband with him through the airport's unmonitored perimeter gates and hand it off to his accomplices in the sterile area of the airside terminals after they cleared the TSA security checkpoint.[44] Over fourteen weapons and twenty-eight pounds of marijuana were smuggled throughout the life of the operation.[45] In July 2007, yet another smuggling operation was uncovered at Orlando International Airport when JetBlue Airways employee Hiram Rivera-Ortiz used his SIDA badge in a similar fashion to smuggle four pistols and two submachine guns onto flights to Puerto Rico for a payment of $4,500.[46]

Just one month after the 2014 Atlanta incident was uncovered, an FAA aviation safety inspector used his SIDA badge to bypass the TSA checkpoint and board a flight from Atlanta to

---

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Airport to Screen Workers After Guns, Drugs Smuggled Onto Florida Flight*, Fox News (Mar. 14, 2007), http://www.foxnews.com/story/2007/03/14/airport-to-screen-workers-after-guns-drugs-smuggled-onto-florida-flight.html.

[44] *Id.*

[45] *Id.*

[46] Henry P. Curtis, *Orlando Airport's Efforts Fail to Prevent Gun, Drug Smuggling*, Orlando Sentinel (Jan. 28, 2008), http://articles.orlandosentinel.com/2008-01-28/news/oiasecurity28_1_orlando-international-airport-puerto-rico-commercial-airport [https://perma.cc/YZB2-DUX7].

New York with a loaded handgun in his carry-on luggage.[47] Earlier in 2014, five airline employees at Boston's General Edward Lawrence Logan International Airport were charged with using their SIDA badges to smuggle more than $400,000 in cash.[48]

Narcotics smuggling by airport badgeholders is another major risk that has come to light in the past several years. Unlike gun smuggling, which poses a direct threat to security, narcotics smuggling is not by itself immediately dangerous. However, such incidents must be taken seriously, for the means by which employees use their SIDA badges illegally to smuggle drugs are the same means used to introduce dangerous items into the system that *can* impact safety and security. In 2015, Southwest Airlines employee Michael Videau was one of three baggage handlers at Oakland International Airport in Oakland, California charged with smuggling marijuana onto commercial flights in a fashion similar to the 2014 Atlanta incident discussed *supra*.[49] Videau would bring the narcotics into the sterile area using his SIDA badge to bypass the TSA checkpoint and then hand off the contraband to his accomplices after they cleared the security checkpoint as passengers.[50] In March 2016, JetBlue Airways flight attendant Marsha Gay Reynolds attempted to use her airline employee ID at the Known Crewmember (KCM) checkpoint—a TSA program that allows flight attendants and pilots to bypass security screening unless randomly selected—to smuggle sixty-eight pounds of cocaine onto a commercial flight.[51] However, Reynolds happened to be selected for random screening that day at the KCM checkpoint and upon being informed of this, took off running, leaving her bag filled with cocaine behind.[52] She was arrested shortly thereafter.[53]

---

[47] Scott Mayerowitz, *TSA Increases Screening of Airport and Airline Employees*, USA TODAY (Dec. 29, 2015, 7:34 AM), http://www.usatoday.com/story/travel/flights/todayinthesky/2015/12/29/tsa-increases-screening-airport-and-airline-employees/78008538 [http://perma.cc/4FGK-9H9M].

[48] *Id.*

[49] *Former Southwest Airlines Employee at Oakland Airport Pleads Guilty to Smuggling Marijuana*, CBS (Aug. 3, 2016, 10:08 PM), http://sanfrancisco.cbslocal.com/2016/08/03/former-southwest-airlines-employee-at-oakland-airport-pleads-guilty-to-smuggling-marijuana [http://perma.cc/7M3Z-WDWN].

[50] *Id.*

[51] Eliott C. McLaughlin & David Shortell, *Feds: Flight Attendant Left 68 Pounds of Cocaine at LAX Checkpoint*, CNN (Mar. 25, 2016, 12:16 AM), http://www.cnn.com/2016/03/24/us/flight-attendant-cocaine-smuggling-case [http://perma.cc/U5SJ-5PUF].

[52] *Id.*

[53] *Id.*

Above and beyond issues involving badgeholders using their SIDA badges in violation of airport security rules and federal security regulations, in the past few years, several individuals have been issued airport identification badges when they likely should not have been due to some type of disqualification. For instance, in 2016, a Freedom of Information Act request identified that seventy-three badged employees at forty different commercial U.S. airports had been flagged for having ties to terrorist groups.[54] Moreover, in September 2014, a former badged airline employee died in Syria fighting for ISIS.[55]

III. DISCUSSION

The risks pertaining to airport badgeholders either misusing their privileges or slipping through the cracks of the vetting process have been clearly demonstrated. As history has proven, disastrous consequences may follow from abuse of the freedom given to airport badgeholders. While the overall security of the system today is significantly better than on September 11, 2001, and before, it is clear that there is still a lot of work that must be done in order to ensure that the security of commercial aviation continues. Some potential modifications that can be made to security regulations are simple, while others are extremely complicated and complex for several reasons. There are four possible changes that can be made to the current system to rectify the risks that still exist in the modern airport security system. These alternatives are: (1) instituting 100 percent employee screening; (2) a multi-layered and more thorough background check process; (3) random Explosives Detection Canine Team (EDCT) K-9 sweeps of non-public employee areas; and (4) supplemental random employee screening on ramp areas near air carrier aircraft. Each will be addressed in turn.

When analyzing any of the alternatives requiring employee screening or additional employee screening, one threshold consideration that must be made is constitutional concerns. Under Amendment IV to the Bill of Rights in the U.S. Constitution, individuals have the right "to be secure in their persons, houses,

---

[54] *2 Employees at Logan Airport Flagged for Potential Terrorism Ties*, FOX (Mar. 15, 2016, 11:34 AM), http://www.fox25boston.com/news/2-employees-at-logan-airport-flagged-for-potential-terrorism-ties/161897263 [http://perma.cc/2K2Q-V9TR].

[55] Amanda Vicinanzo, *Major Gaps in Airport Employee Screening Threaten Homeland Security*, KATHLEEN RICE (Feb. 6, 2015), http://kathleenrice.house.gov/news/documentsingle.aspx?DocumentID=29 [http://perma.cc/3KFH-8X5T].

papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[56]

It is important to note at the outset that the Fourth Amendment only applies to those searches and seizures conducted by government employees or agents.[57] What exactly constitutes "state actors" for the purposes of the Fourth Amendment is a notoriously confusing area of the law.[58] Perhaps, however, for the purposes of airport employee screening, the answer is less obscure. Airports in the United States are owned either by the federal government, the state government, or the local government (city, town, or county). In many cases, instead of the government operating the facility themselves, they instead create through legislation a quasi-governmental public corporation to operate the facility, such as an airport authority or a port authority.[59] This is the case at airports such as Orlando International Airport in Florida, owned by the City of Orlando but operated by the Greater Orlando Aviation Authority (GOAA).[60]

Even still, some airport owners or airport authorities decline to actually run the facility themselves and instead hire a wholly private contractor to handle all aspects of the airport's management and operation. One example of this is at Albany International Airport in New York, owned by the City of Albany but operated entirely by AFCO AvPorts, Inc.[61] As an added wrinkle, regardless of the governmental status of the airport itself and as discussed *infra*, any supplemental employee screening operations would almost certainly be conducted by a private security contractor instead of direct employees of the airport operator itself.

Despite all of this confusion, for the purposes of the Fourth Amendment, it is actually quite straightforward. Several courts

---

[56] U.S. CONST. amend. IV.

[57] *See, e.g.*, United States v. Barth, 26 F. Supp. 2d 929, 935 (W.D. Tex. 1998).

[58] *See* Jackson v. Metro. Edison Co., 419 U.S. 345, 349–50 (1974).

[59] *See AvPorts Services: Comprehensive Airport Management*, AVPORTS, http://avports.com/services/comprehensive-airport-management [http://perma.cc/7U4J-GPPV] (last visited Oct. 18, 2017).

[60] *See About Us*, ORLANDO INT'L AIRPORT MCO, https://orlandoairports.net/about-us/ [http://perma.cc/9AP3-84P2] (last visited Oct. 18, 2017).

[61] *Albany International Airport*, AVPORTS, http://avports.com/airport/albany-international-airport-alb [http://perma.cc/YB7U-Z38H] (last visited Oct. 18, 2017).

have held that, for the purposes of determining the Fourth Amendment's "state action" requirement, the source of the searcher's paycheck is immaterial, and instead, the public or private nature of the facility at which the search takes place must be considered, including the source of the facility's operating funding.[62] As a result, it seems clear that, in relation to airport badgeholder security screening, the individuals conducing that screening—regardless of whether they are legally public or private employees—must be considered "state actors" for the purposes of a Fourth Amendment analysis.

That being said, in a situation where airport badgeholders are required to submit to screening before reporting to work, while working, or while sitting in their break areas, the privacy protections of the Fourth Amendment would be implicated. In the pivotal case of *Katz v. United States*,[63] Justice Harlan's concurring opinion laid out the framework for determining if a search has occurred.[64] Specifically, Justice Harlan articulated a two-prong test, stating that a search occurs only when government action violates privacy that an individual has "exhibited an actual (subjective) expectation of," and when that expectation is one "that society is prepared to recognize as 'reasonable.'"[65] Only if, by that test, a search is found to have occurred, does an inquiry into the existence of probable cause and the possession of a search warrant need to be considered in assessing an alleged Fourth Amendment violation.[66] It has been well-established that any person accessing an airport—indiscriminate of that individual's purpose for being there—has a reasonable expectation of privacy as to the items on their person or in their baggage.[67] As a result, at least facially, it would seem that the only way airport screening would be possible is with probable cause and a search warrant. However, as any passenger who has flown commercially in the past several decades is aware, this is not the case.

As discussed *supra*, airport screening—at least from a passenger perspective—has been in place since the early 1970s.[68]

---

[62] *See, e.g.*, Stroeber v. Comm'n Veteran's Auditorium, 453 F. Supp. 926, 931 (S.D. Iowa 1977) (holding that private security officers "acting to provide security for a public facility financed by public monies, [constitutes] 'state action'"); Tampa Sports Auth. v. Johnston, 914 So. 2d 1076, 1078 (Fla. Dist. Ct. App. 2005).

[63] 389 U.S. 347 (1967).

[64] *Id.* at 361 (Harlan, J., concurring).

[65] *Id.*

[66] *Id.* at 360–61.

[67] *See, e.g.*, United States v. Skipwith, 482 F.2d 1272, 1275–77 (5th Cir. 1973).

[68] Gardiner, *supra* note 2.

When passenger screening first came into existence, it was met with constitutional challenges, namely on the grounds that a suspicionless search was being conducted without a warrant.[69] However, in the wake of several high profile hijackings and threats, courts quickly ruled that airport searches fall within the "administrative search" component of the "special needs" exception to the Fourth Amendment's probable cause and warrant requirement.[70] Special needs searches are unique in that they are conducted with no probable cause or suspicion of wrongdoing whatsoever. As a result, their acceptability is determined using a balancing test of reasonableness.[71]

Specifically, the Fifth Circuit held this requires courts to balance the public necessity, the efficacy of the search, and the degree and nature of the intrusion on the individual's Fourth Amendment rights.[72] The public necessity prong is easily satisfied by the serious threat of public injury and the high likelihood of occurrence should no type of passenger screening be conducted.[73] The efficacy of the search is similarly satisfied by the high likelihood the search will mitigate the potential harm.[74] The success rate of a traditional magnetometer satisfied at least one court of the efficacy requirement,[75] and modern equipment used today, such as millimeter-wave detection systems, only increases the likelihood of detection. The degree and nature of the intrusion caused by airport security screening is mitigated largely by the fact that a hundred percent of passengers are screened, eliminating any risk of embarrassment.[76]

---

[69] *See, e.g.*, United States v. Edwards, 498 F.2d 496, 499 (2d Cir. 1974); *Skipwith*, 482 F.2d at 1276; Downing v. Kunzig, 454 F.2d 1230, 1232–33 (6th Cir. 1972).

[70] *See* United States v. Aukai, 497 F.3d 955, 958–59 (9th Cir. 2007) ("where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings"); United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973) (holding that airport screenings are considered to be administrative searches because they are "conducted as part of a general regulatory scheme" where the essential administrative purpose is "to prevent the carrying of weapons or explosives aboard aircraft.").

[71] *See* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) ("Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers.").

[72] *Skipwith*, 482 F.2d at 1275.

[73] *Id.*

[74] *Id.*

[75] United States v. Albarado, 495 F.2d 799, 804 (2d Cir. 1974).

[76] *See, e.g.*, Wheaton v. Hagan, 435 F. Supp. 1134, 1146 (M.D.N.C. 1977).

Moreover, the actual invasion of privacy is minimal as there is no physical search unless the screening device alarms, at which point reasonable suspicion is created for a *Terry*-style pat down.[77]

The Ninth Circuit framed the reasonableness standard of the airport exception in slightly different terms, finding such searches constitutionally permissible so long as the searches are "no more extensive or intensive than necessary, in the light of current technology, to detect weapons or explosives[,] . . . [are] confined in good faith to that purpose[,]" and "passengers [may] avoid the search by electing not to fly."[78] The technology used today to screen passengers and luggage is designed to do so with the smallest intrusion possible, and in keeping with the requirement that such searches are confined to detecting weapons and explosives, TSA personnel are decidedly not afforded law enforcement powers.[79] Further, as discussed in the following paragraph, passengers are under no obligation to submit to TSA screening: they may simply choose not to fly.

Outside the special needs exception, courts have similarly ruled that, at least in some cases, airport security searches may be permissible as consent searches.[80] In these cases, courts have reasoned that because flying is a choice and is not compulsory, individuals impliedly consent to such searches when they arrive at the security checkpoint in order to board their flight.[81] Courts have consistently ruled that, while for security reasons, once screening has begun a passenger may not leave the checkpoint until it is complete; this does not render the search involuntary.[82]

It seems clear that searches of airport SIDA badgeholders, at least to the extent that the Fourth Amendment is involved, are

---

[77] *Albarado*, 495 F.2d at 806–07; United States v. Dalpiaz, 494 F.2d 374, 376–77 (6th Cir. 1974).

[78] United States v. Aukai, 497 F.3d 955, 961–62 (9th Cir. 2007).

[79] Everett Potter, *Five Myths About the TSA*, USA TODAY (Nov. 10, 2014, 7:57 AM), https://www.usatoday.com/story/travel/flights/2014/11/10/transportation-security-administration-pre-check/18658691/ [http://perma.cc/4Z6V-U85G].

[80] *See Dalpiaz*, 494 F.2d at 376–77 (magnetometers and luggage searches are constitutional as consensual if a person has the opportunity to avoid the search by choosing not to fly).

[81] *See, e.g.*, United States v. Freeland, 562 F.2d 383, 385–86 (6th Cir. 1977) (a luggage search is valid even as an implied consent search even though the defendant was not advised that he could ask to have his luggage returned rather than have it searched).

[82] *See, e.g.*, People v. Heimel, 812 P.2d 1177, 1181–82 (Colo. 1991).

no different than those of airline passengers. As discussed *infra*, searches of employees prior to entering the secured area or SIDA are akin to searches of passengers accessing the sterile area through the security checkpoint. In fact, many airport badgeholders arrive to work through the main TSA checkpoint and submit to the same screening the passengers receive. An employee arriving through an employee-only access point would be completely justified in departing the area prior to being screened or not reporting to work at all. An employee's "need" to work is no more substantial than a passenger's "need" to fly, and as a result there is no material reason that such a search should not be considered consensual.[83] Consent becomes irrelevant once the employee enters the secured area, as TSA regulations (under Part 1540.107) stipulate that all persons and property are subject to search at any time within restricted areas.[84]

Beyond clustering employee searches under the consent-search category, searches of airport badgeholders logically fall within the special needs exception category of searches as well. Under case law such as *Aukai*[85] and the balancing test laid out in *Skipwith*,[86] the public necessity of screening employees is just as great if not greater than the public necessity of screening passengers. Employees with unfettered access to ramp areas and vehicles can certainly inflict more damage to aircraft by loading dangerous devices than can passengers who are restricted to dangerous items that may fit inside their carry-on luggage. Furthermore, the efficacy of the search would be identical to that involving passengers at the TSA checkpoint as the same equipment would necessarily need to be used for passengers and employees alike. Finally, because all employees would be screened when arriving to work, the search would not be more intrusive than the passenger searches at the TSA checkpoint. For employees randomly selected for supplemental screening on the ramps, the provisions of Part 1540 discussed *supra* would similarly apply. Moreover, one might argue that at least to the extent that dangerous and deadly items might be smuggled onto the jobsite, airline employees have a reduced expectation of privacy while at

---

[83] *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 224–30, 234 (1973) (holding that a search is consensual even if an individual feels they have no choice in the matter).

[84] 49 C.F.R. § 1540.107 (2016).

[85] United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

[86] United States v. Skipwith, 482 F.2d 1272, 1275 (5th Cir. 1973).

work compared to that of an average individual, similar to railroad employees.[87] If this were true, even searches of badgeholders arriving at work that are more intrusive than those conducted on passengers could be justified.

Beyond constitutional issues, an additional legal consideration is shared by all employee screening possibilities. That consideration is equal employment, specifically relating to the Equal Employment Opportunity Commission (EEOC). The EEOC is responsible for "enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age (specifically forty years or older), disability or genetic information."[88] Perhaps the most significant federal law under the purview of the EEOC is the Civil Rights Act, which prohibits discrimination based upon these so-called protected bases.[89] While the EEOC might seem facially relevant to employee screening, this potential legal conflict is easily resolved for three main reasons.

First, the Civil Rights Act only relates to adverse employment decisions or actions made on the grounds of one of the statute's listed protected bases, as reproduced above.[90] Clearly, no such employment action occurs in the context of employee security screening, making the statute inapplicable. Second, the Civil Rights Act applies only to actions taken by *employers*, defined by the statute as "a person engaged in an industry affecting commerce who has fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person."[91] It cannot be disputed that the airport operator or its agents are not the employers of the vast majority of those passing through the checkpoints, meaning that, again, the statute is rendered inapplicable. Even if, *arguendo*, they were, the Civil Rights Act would still not be implicated due to the following point—there is simply no discrimination being practiced in employee security screenings. As discussed *supra* in the context of the Fourth Amendment, *each and every* employee would be required to sub-

---

[87] *See, e.g.*, Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 627–28 (1989).

[88] *About EEOC*, EQUAL EMP'T OPPORTUNITY COMM'N, https://www.eeoc.gov/eeoc (last visited Oct. 18, 2017) [http://perma.cc/REL9-TLQ4].

[89] Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241 (1964).

[90] 42 U.S.C. 2000e-16a-b (2012); 42 U.S.C. 1983 (2012).

[91] 42 U.S.C. 2000 (2012).

mit to screening before entering the SIDA and secured areas, *regardless* of their gender, race, national origin, or any other factor. There would be no special selection practices or policies, and screening would be the same for all employees. As a result, it cannot validly be concluded that there would be any sort of discrimination present that would violate the Civil Rights Act or any other law under the jurisdiction of the EEOC.

With the constitutional and legal framework for the three alternatives presented related to screening, each may be looked at in specificity. The first of these alternatives is the introduction of "100 percent-employee screening."[92] In essence, 100 percent employee screening is where each and every SIDA badgeholder at an airport is required to submit to an inspection of their person and any personal belongings they may have with them every time that employee enters the sterile area, secured area, or SIDA. As discussed *supra*, the majority of commercial airports today contain a system of doors, gates, and hallways where, using their SIDA badge, employees can bypass the TSA security checkpoint and enter into restricted areas with no screening whatsoever. In a 100 percent employee screening environment, a security checkpoint is set up at each door or access point where an employee can use his or her badge to transition from the public areas to the SIDA or secured area, functionally equivalent to a TSA passenger security checkpoint. Currently, only three out of approximately 291 commercial airports in the United States require any sort of employee screening: (1) Miami International Airport; (2) Orlando International Airport; and (3) Atlanta International Airport.[93] And out of those three, only Orlando International and Miami International require true 100 percent employee screening.[94]

To operationalize this term, it is useful to look at an example of how the process works at a 100 percent employee screening

---

[92] *See* DEP'T OF HOMELAND SEC., OFFICE OF INSPECTOR GEN. OIG-09-05, TSA's SECURITY SCREENING PROCEDURES FOR EMPLOYEES AT ORLANDO INTERNATIONAL AIRPORT AND THE FEASIBILITY OF 100 PERCENT EMPLOYEE SCREENING at 2 (2008).

[93] *Few Airports Require Employee Screening Before Work*, FOX NEWS (Apr. 11, 2016), http://www.foxnews.com/politics/2016/04/11/few-airports-require-employee-screening-before-work.amp.html [https://perma.cc/2XCV-AJCS].

[94] Scott Zamost & Drew Griffin, *Despite Security Gaps, No Full Screening for Airport Workers*, CNN (Apr. 21, 2015, 12:53 PM), http://www.cnn.com/2015/04/20/travel/airport-workers-security-screening/index.html [http://perma.cc/Z598-SL4V].

facility, Orlando International Airport.[95] Orlando is currently the thirteenth busiest airport in the United States, serving approximately forty-two million passengers in the 2016 calendar year.[96] Design-wise, Orlando is somewhat unique among airports because it follows a "landside-airside" layout. Unlike traditional airports where the main terminal is physically connected to the concourses that house the airline gates, at Orlando the two parts of the terminal are separated by waterways and vegetation as well at approximately one mile in distance. Orlando has one main landside terminal and four airside terminals, each with approximately thirty gates. Passengers transfer from the main terminal to the airside terminals using automated "people movers" suspended as an above ground train (AGT). Two such trains service each airside.

Below each airside's AGT track runs a small vehicular roadway leading into the main terminal. These roadways are used by airline tugs to tow inbound checked passenger luggage between the aircraft and the baggage claim. Conversely, they are also used to tow outbound checked passenger baggage from the TSA baggage inspection equipment to the departing aircraft at the airsides. Access control doors with employee security screening checkpoints are located throughout the baggage claim areas that provide access to this inbound and outbound baggage processing area inside the main terminal building.

Due to the landside-airside layout of Orlando, many employees enter the SIDA not through the main terminal but through exterior, remote employee screening checkpoints, each located at one of the vehicle access gates. After employees are initially screened, they must be screened again if they exit the SIDA and later return.

A 100 percent employee screening setup has many positives that make it a desirable option. For one, it is undoubtedly the most effective of all the alternatives presented. In a true 100 percent employee screening environment, there is simply no way that an employee can abuse their SIDA badge to smuggle con-

---

[95] The following specific information regarding Orlando International Airport is based off of factual, non-privileged information the author gathered during his employment as an Airfield Operations Specialist for the Greater Orlando Aviation Authority from May 2013 to July 2014.

[96] Press Release: Orlando International Airport Ends 2016 with Record Domestic and International Traffic, Orlando Int'l Airport MCO (Feb. 10, 2017) [hereinafter Orlando Press Release], https://orlandoairports.net/press/2017/02/10/orlando-international-airport-ends-2016-record-domestic-international-traffic/.

traband onto aircraft. The employee's physical person, vehicle, and carried belongings are thoroughly checked prior to being permitted to enter the SIDA or secured area. Under these conditions, it would be all but impossible for an incident like those discussed *supra* to occur.

Of course, this type of arrangement also has several downsides. For one thing, 100 percent employee screening is expensive to set up and operate. For instance, Orlando's operation cost approximately $5 million to outfit.[97] This included purchasing five mobile x-ray scanners totaling over $600,000.[98] Besides this up-front cost, over 150 contract security personnel needed to be hired to fill a 24/7 schedule.[99] Initially, TSA screeners conducted both passenger and employee screening, but GOAA subcontractors took over employee screening operations shortly thereafter.[100] Additionally, federal funding is currently unavailable to aid airport operators in setting up and operating employee security checkpoints, meaning all funds must be taken from the airport's operating budget.[101] Despite this fact however, there is no shortage of security contractors willing to contract with airports to provide employee screening, and several such contractors are Department of Homeland Security SAFETY Act designees.[102] From an economic perspective, this certification results in a greater number of suppliers, ultimately tending to drive the cost of such security services downward.

Another negative to 100 percent employee screening, as outlined in a TSA report on the topic, is that such screening "is incapable of determining a person's motivations, attitudes and capabilities to cause harm, among other limitations. No single measure can provide broad-spectrum protection against risks or adversaries. Therefore, risk-based, multi-layered security offers the greatest ability to mitigate risks through the application of flexible and unpredictable measures to protect commercial aviation."[103] In other words, even if 100 percent employee screening were mandated nationwide, it would likely just be a matter of

---

[97] Curtis, *supra* note 46.

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] Telephone Interview with Justin T. Grindell, *supra* note 18.

[102] *SAFETY Act: Approved Technologies*, U.S. DEP'T HOMELAND SEC., https://www.safetyact.gov/jsp/award/samsApprovedAwards.do?action=searchApprovedAwardsPublic [http://perma.cc/8BZE-NT5G].

[103] Zamost & Griffin, *supra* note 93.

time until loopholes are found and exploited. Resultantly, at least according to the TSA, the better tactic requires taking action that focuses on the motivations behind employee breaches, as opposed to catching such employees in the act. This alternative is discussed in more detail *infra*.

Moreover, requiring all employees to stop for security screening while performing their job functions clearly impacts productivity. For instance, if an employee rushing late-checked bags from a remote baggage handling facility to a departing aircraft gets held up in a line of other employees waiting for screening, not only could that departing flight be delayed, but, numerically speaking, that employee will also be able to make fewer runs between the terminal and the baggage facility during his or her shift than would be possible absent employee screening. Relatedly, the relationship between airports and airlines could potentially become strained should an airport operator be interested in voluntarily moving to 100 percent employee screening model, but airlines oppose it due to productivity concerns. Ultimately, in such a case, a cost-benefit analysis must be completed by all interested parties to determine the best course of action.

Another alternative pertaining to employee screening involves the random, supplemental screening of employees in the secured area. This alternative can be implemented either in conjunction with a 100 percent employee screening program or on its own, at airports unable to facilitate the screening of every employee at all times. Under this type of system, TSA or airport operations personnel would patrol the terminal areas within the SIDA and secured area, and randomly select airport employees for on-the-spot screening. The selections would be based upon an unpredictable and random logarithm, perhaps focusing each day on different employers, different shifts, or otherwise. In such a system, a magnetometer wand would be used to conduct a quick sweep of an employee, with a pat down following any alarm activation. In addition, any personal belongings of employees within the secured area would also be subject to inspection.

The positives of such a system are similar to those of a 100 percent employee screening. Would-be employee wrongdoers are more likely to be caught in the act if a crime similar to those carried out in Atlanta and Orlando were attempted. Moreover, random security checks increase deterrence as would-be offenders are unsure when or if a screening will take place. This functionally serves as a tier in a multi-layered security plan, the

approach to airport security endorsed by the TSA.[104] In addition, random screening reduces the ability for wrongdoers to find gaps in the system; a fluid system is, by definition, ever-changing, meaning there are no routine patterns. A final positive of randomized employee screening is that from a legal standpoint, 100 percent employee screening and random employee screening are effectively indistinguishable. To be sure, randomized screening would also clearly meet the constitutional reasonableness standards set out in cases discussed *supra*, such as *Aukai*,[105] and to the extent that EEOC issues are implicated, such a system would not violate statutes such as the Civil Rights Act, as the screening would not be conducted by employers or in a discriminatory fashion. Instead, the randomized screening, as mentioned, would follow an automated logarithmic sequence.

The negatives to a randomized employee security screening system are also similar to those of 100 percent employee screening. A marked decline in productivity would likely occur during an employee's shift, albeit a smaller one than in a 100 percent screening environment. Additionally, costs would increase for airport operators because of the necessity of hiring extra employees to execute the random screening policy. Finally, as with any random security screening policy, there might also be claims of discrimination insofar as certain races or ethnicities being singled out for random screening.

The final alternative solution involving the screening of employees involves utilizing Explosive Detective Canine Team (EDCT K-9) units to conduct periodic and random sweeps of restricted, employee-only areas such as breakrooms, internal hallways, and locker rooms. Most large, commercial airports like Orlando, Miami, and Atlanta have either their own on-site K-9 teams or a TSA K-9 team dedicated exclusively to the airport. In this alternative, these EDCT K-9 teams would randomly walk through employee-only areas—not just the SIDA and secured areas but also leased tenant spaces within these areas—conducing free air sniffs of employees and their personal belongings for explosives.

---

[104] Statement of Transp. Sec. Admin., U.S. Dep't of Homeland Sec. Before H. Comm. on Oversight and Gov't. Reform (May 13, 2015), https://oversight.house.gov/wp-content/uploads/2015/05/TSA-Statement.pdf [http://perma.cc/GES6-SHLB].

[105] United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007).

It is well-settled law that these so-called free air sniffs do not constitute searches for Fourth Amendment purposes, as individuals do not have a reasonable expectation of privacy in the air around them in public places.[106] As a result, the Fourth Amendment need not be considered in this type of operation. Further, the office spaces and employee break rooms located on the ground level of airport terminal buildings are functionally "public" in nature, despite the flying public's restriction from accessing them, for anyone with an airport ID badge may access those areas, and ultimately, the space is owned by the airport operator. Beyond this, most commercial lease contracts allow the landlord—in this case, the airport operator—to enter the leased area to conduct periodic inspections.[107] Lastly, because TSA regulations authorize the search of employees and their personal effects any time they are within the SIDA, and because the free air sniffs would focus entirely on those two things, Fourth Amendment considerations would not be implicated under per the special needs administrative search doctrine discussed in detail *supra*.[108] In the SIDA, no location is truly "private."

There are many positives to a K-9 sweep program. First, K-9s are substantially more effective than humans at detecting explosives.[109] As a result, an airport security employee using a K-9 unit can, with impressive reliability, search an entire room in a fraction of the time it would take a human to perform the same task.[110] Additionally, due to the sensitivity of K-9 noses, explosives hidden deep from view—even inside walls or under flooring—could be detected.[111] Second, using K-9s for random sweeps shares the benefits of random searches in general as discussed *supra*, in that a would-be wrongdoer would have no way of knowing if and when such a sweep would occur and would be unable to exploit a repetitive hole observed in the system. Third,

---

[106] *See, e.g.*, United States v. Place, 462 U.S. 696, 707 (1983) ("exposure of respondent's luggage, which was located in a public place, to a trained canine—did not constitute a 'search' within the meaning of the Fourth Amendment.").

[107] Janet Portman, *Landlord Rights to Enter Tenant's Commercial Rental Space*, NOLO, http://www.nolo.com/legal-encyclopedia/clb-landlord-rights-enter-commercial-space.html [http://perma.cc/R9NE-43ZK].

[108] *See* Aukai, 497 F.3d 955.

[109] Susan L. Nasr, *How Bomb-Sniffing Dogs Work*, HOWSTUFFWORKS, http://science.howstuffworks.com/bomb-sniffing-dog1.htm (last visited Oct. 18, 2017).

[110] Catherine Savoia, *12 Fun Facts About Bomb Dogs,* MSA SECURITY (June 25, 2015), http://www.msasecurity.net/security-and-counterterrorism-blog/12-fun-facts-about-bomb-dogs [http://perma.cc/YD5Q-HWKY].

[111] *Id.*

using K-9s instead of humans, while likely more expensive up front, presents a cost savings over time as the amount of work one K-9 can do in a day is equivalent to at least that of several humans. In fact, EDCT K-9 teams at airports are fully funded by TSA, meaning that airport operators themselves would feel no impact from the addition of such teams.[112] Lastly, many employees would likely find K-9 screenings less intrusive than magnetometer screenings or pat-downs, potentially increasing employee morale.

As with every alternative, there are also several negatives, although few in comparison. One negative could be a feeling of distrust by badgeholders of the airport operator for coming into their workspace and running K-9s. An additional negative is the risk of false positives and other reliability issues with the K-9s themselves. K-9s have limitations, and unless directed specifically to a bag or an individual, some K-9 units might have trouble detecting odor. A final negative with this system is that it does not work well, or at all, unless combined with another means of employee screening: conducting random sweeps of employee work areas does not guarantee that all contraband potentially carried into the SIDA by employees will be detected. Certainly, if an employee is able to bring something into the SIDA because he or she was not screened during entry, there would be other places for that employee to store the contraband besides in their office space—perhaps even directly on an aircraft.

Outside the realm of alternatives pertaining to employee screening, one final alternative directly impacts airport employee security concerns: a multi-layered and more thorough employee background check process. As discussed *supra*, prior to receiving a SIDA badges, employees must be investigated.[113] Currently, this constitutes a badge application requiring a modest amount of background information, a CHRC, and a security threat assessment.[114] Recently, following the smuggling operation uncovered at Atlanta, TSA modified their policies to require a CHRC every two years and to conduct random, "real time," security assessments of badged employees.[115] Yet, more is

---

[112] Telephone Interview with Justin T. Grindell, *supra* note 18.

[113] 49 C.F.R. § 1544.229 (2016).

[114] *Id.*

[115] Melvin Carraway, *TSA's Efforts in Enhancing Airport Access Control*, TRANSP. SEC. ADMIN. (Apr. 30, 2015) https://www.tsa.gov/news/testimony/2015/04/30/tsas-efforts-enhancing-airport-access-control [https://perma.cc/2QMM-9RYA].

still needed: specifically, a more thorough badge application, combined with interviews of the SIDA badge applicant and several of his or her references. While the current system is effective at detecting potential threats to the system by prohibiting those who have committed relevant crimes from obtaining a badge and comparing applicant's names to the various watch lists, the current system is single-layered and not comprehensive. That is, the current system fails to investigate employees beyond what is on paper, as it declines to look into the employee's personality, ties, and mentality. For a system to be truly multi-layered, both types of investigations are required.

The positives of this type of investigative policy are largely self-evident. The ability to interview an applicant and several references would allow for background investigators to determine if an individual poses a risk *despite a paper-based approval*. In essence, such a practice would allow an employee's application answers to be corroborated face-to-face. In theory, even if someone is cleared based upon their electronic background checks, that person still might not pass the interview phase, similar to the process of obtaining a government security clearance. A smaller, secondary benefit is the deterrence that an interview policy would have on would-be wrongdoers. Finally, because the background checks and interviews would be conducted by TSA and run against every applicant in the same way, no EEOC-related issues would arise.

Despite its benefits, a policy of conducting interviews for each and every employee based on thorough application questions has one major negative: it would be extremely cumbersome and costly. Some airports employ upwards of 18,000 badgeholders,[116] and to conduct a number of interviews for each would be a massive undertaking, likely requiring the hiring of many employees to assist in its execution. This issue could be somewhat mitigated by correlating the level of interviewing for each employee with their SIDA badge's level of access: restaurant employees who do not have access to the secured area, for instance, would not require as much personal background checking as an airline ramp agent with direct access to aircraft.

IV. RECOMMENDATIONS

With a comprehensive analysis of four possible alternatives that may be undertaken by airport operators and the TSA to

[116] *See* Orlando Press Release, *supra* note 95.

mitigate risks posed by SIDA badgeholders complete, it is now possible to recommend one of these options. While it seems that the positives of each of the four presented alternatives outweighed their negatives, all but one of the alternatives are not self-sufficient. That is, only one of the alternatives—standing alone and without any additional measures being taken in conjunction—would likely have the most significant impact on the risk. That alternative is the 100 percent employee security screening model, and therefore is the recommended policy change.

The rationale behind this recommendation embodies many of the positives discussed *supra*. A 100 percent employee security screening provides an exhaustive approach to mitigating the carriage of contraband by employees into the SIDA, secured area, and sterile area. Each employee, each time he or she enters one of these areas, must submit to a full search of his or her person and personal belongings. In so doing, airport operators reduce, to a high degree of certainty, the possibility that an employee carries something nefarious with them. This type of system is relatively easy to set up and to maintain and requires little transition time or training. As discussed *supra*, Orlando International Airport set up its program in just a few weeks. Theoretically, in a 100 percent employee screening facility, every person in the SIDA has been screened. Thus, unlike the majority of airports in the United States where only the passenger boarding areas are sterile, at 100 percent employee screening airports, the *entire facility* is sterile, with the exception, of course, of work tools that employees are permitted to carry with them.

Critics to this model often claim that such screening does not actually reduce the possibility of a security breach from occurring because it becomes predictable to employees arriving to work each day.[117] While this argument has some merit, it is important to remember that 100 percent employee screening would become another layer to the wedding cake of airport security and would not exist independently. Any amount of predictability that might create the potential for exploitation would be overcome by the multitude of currently-existing security procedures that are both in place and continue to be added. Un-

---

[117] Cindy Drukier, *TSA Won't Be Screening All Airport Employees Despite Insider Threats,* EPOCH TIMES (Apr. 21, 2015, 2:40 PM), http://www.theepochtimes.com/n3/1328514-tsa-wont-be-screening-all-airport-employees-despite-insider-threats/ [http://perma.cc/FG5S-3YNZ].

derneath the 100 percent employee screening layer lie several additional layers of security procedures to bridge the gap. 100 percent employee screening would simply ensure that everyone accessing the airport's most sensitive areas are screened, while preserving other TSA programs that currently serve a similar purpose.

Critics also state that a 100 percent employee screening model is prohibitively expensive and, therefore, not practical as a TSA mandate.[118] However, the security of the civil aviation system is not something a price tag should be placed upon, especially after weighing how much is at risk against how effective a 100 percent screening can be. Surely, funding can be derived from a multitude of sources, budgets can be adjusted, and other cost-cutting measures can be taken in less critical areas of an airport to compensate for the added expense. Moreover, TSA could institute a federal funding program for airports to get an employee screening system running and staffed, much like the FAA has done in grant programs such as the Airport Improvement Program.[119] The FAA could also collaborate with the TSA to extend the permissible uses of Passenger Facility Charges—up to $4.50 in fees that the FAA authorizes airport operators to collect from each passenger's ticket to cover various airport operating expenses[120]—to include covering cost of the 100 percent employee screening program, or TSA could simply come up with its own similar program, passing a nominal airport security fee on to passengers. Finally, and as a last resort, TSA could promulgate regulations only requiring Category X airports—the highest of TSA's classification of airports by passenger volume[121]—to institute 100 percent employee screening policies and require lower-classified airports to institute some of the other and less expensive alternatives that have been discussed *supra*. Doing this would ensure that the nation's most attractive target airports—all of which necessarily have the funds to finance a 100 percent employee screening operation—are given

---

[118] *Id.*

[119] *Airport Improvement Program: Overview*, FED. AVIATION ADMIN., https://www.faa.gov/airports/aip/overview [http://perma.cc/3SVQ-J5KQ] (last visited Oct. 18, 2017).

[120] *Airports: Passenger Facility Charges*, FED. AVIATION ADMIN., https://www.faa.gov/airports/pfc [http://perma.cc/GR8R-Z3NF] (last visited Oct. 18, 2017).

[121] *TSA Reveals High-Security Category X Airports*, AVIATION WK. (Oct. 10, 2002), http://aviationweek.com/awin/tsa-reveals-high-security-category-x-airports [https://perma.cc/7C89-XJ2A].

the highest level of employee security procedures possible, while less busy airports still implement additional employee security measures, but to a degree more proportional to their traffic volumes.

Because the 100 percent employee screening model is exhaustive, constitutional, legal, effective, independent, and necessary, it is the recommended and best alternative to combat the growing problem of security breaches, threats, and risks involving airport SIDA badge-holding employees.