# Philadelphia Int'l Develops Separate

PHL PHILADELPHIA INTERNATIONAL AIRPORT

## FACTS&FIGURES

**Project:** Security Master Plan

**Location:** Philadelphia Int'l Airport

**Implementation:** 2011-2016

**Timeframe:** 5-year horizon, based on changing regulations, technology & staffing/personnel

**Lead Consultant:** Faith Group

**General Recommendations:** Improvements to overall security infrastructure, cargo areas, access control system, CCTV coverage, emergency operations center

**Projects Underway:** Access Control System Upgrades

**Resident Consultant Project Manager:** Arora Engineers

**Electrical Contractors:** Armour & Sons Electric; E.J. Electric

Between international turmoil, nationwide security challenges and the headlines that invariably follow, Philadelphia International Airport (PHL) is implementing an autonomous security master plan.

RENEE TUFTS

As security manager at PHL, Renee Tufts is accustomed to playing in the big leagues. If a security incident occurs at a small, rural airport, news may trickle around the nation or industry; but if a similar issue occurs at a large airport, the floodgates swing wide open, Tufts explains.

Seven major airports, including PHL, received unwelcome national coverage last spring when an Associated Press report noted that collectively, they accounted for more than half of the 268 perimeter breaches at 31 of the busiest U.S. airports from 2004 through 2014. The investigation for the report was reportedly prompted by the highly publicized 2014 incident when a teenage boy hopped the fence at San Jose International (SJC) and flew to Hawaii stowed away in an airliner's wheel well.

Notably, John F. Kennedy International, LaGuardia Airport, and Newark Liberty International (all run by the Port Authority of New York and New Jersey) along with Boston Logan International refused to provide data for the report.

In response to the coverage, Tufts noted that PHL, like all airports, constantly evaluates and addresses its vulnerabilities. SJC, for instance, raised its perimeter fence from 6 feet to 10 feet.

Reproach in the general media notwithstanding, airport insiders often turn to PHL for advice and guidance about security issues. Its installation of exit lane technology

Photo: Kenneth D. Aston Jr., Philadelphia Int'l Airport

# Master Plan Strictly for Security

BY NICOLE NELSON

in June 2009 was considered to be cutting-edge, and the airport continues to stay at the forefront of new security challenges as they emerge. Recently, it has been broadly praised as an industry leader for creating a formalized master plan strictly for security.

Tufts recalls the process beginning about five years ago, with a top-down evaluation of the airport's security program by Mark Gale, PHL's chief executive at the time; Deputy Director of Aviation, Operations and Facilities Keith J. Brune; and herself.

"We did not have a roadmap that we could refer to in order to see if our technology was 'keeping up with the Joneses,' so we decided to document where we were and where we wanted to be," Tufts explains. "We wanted to see where we stood nationwide with benchmarking studies: What do we do that other airports do not do? What can we do better? And what do we do just fine?"

Creating a comprehensive plan that documents specific security needs allowed the team to secure funding for projects by folding them into the capital development planning process, she elaborates.

## Picking a Partner

PHL engaged its on-call security contractor, Faith Group, as lead consultant for the security master plan project.

"I think every airport has done security planning in the past because they have to look forward," says Faith Varwig, principal of Faith Group. "But it is only in the past few years that there has really been a formalized process."

FAITH VARWIG

Creating a standalone master plan for security is definitely a trend that is catching on and growing, she adds. That said, Varwig cautions operators that security master plans have a much shorter shelf life than traditional airport-wide master plans or master plans for other specific areas such as environmental sustainability or terminal construction.

"(Security master planning) has to be refreshed on a regular basis because of regulatory changes and technology changes," Varwig explains. "The whole process is a little more challenging, because it is not so set. It is not easy to get your arms around security from a long-term standpoint. The best we can usually do is put a three-year to five-year roadmap out there, and those roadmaps need to be adjusted every year."

Faith Group began PHL's comprehensive security assessment and master plan design with a baseline study of existing conditions, with team members evaluating physical and electronic systems alike.

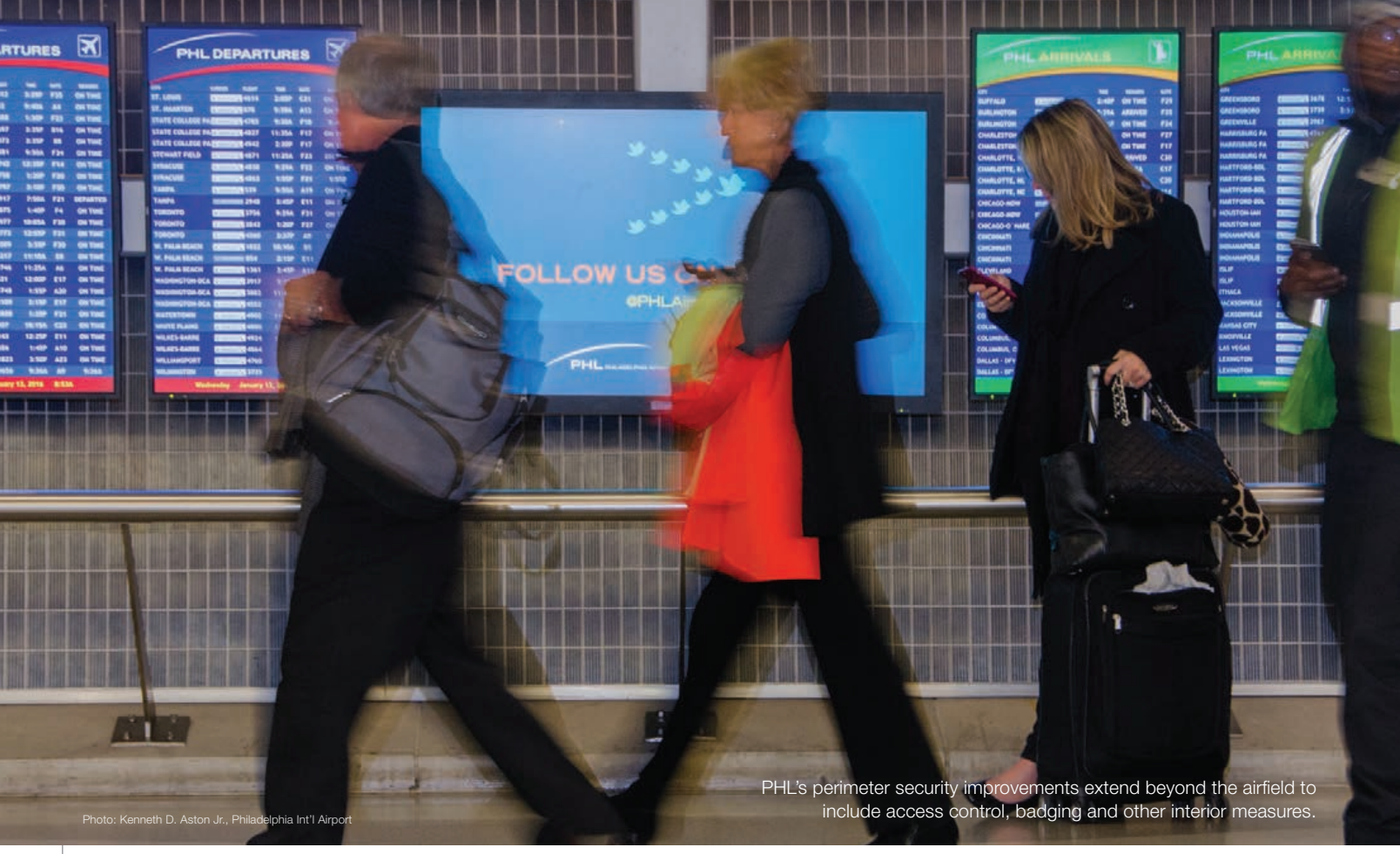


Photo: Kenneth D. Aston Jr., Philadelphia Int'l Airport

PHL's perimeter security improvements extend beyond the airfield to include access control, badging and other interior measures.



"We surveyed all the rooms – all the network and technical infrastructure that supports all the access control and CCTV (closed-circuit television) and other security elements that the airport utilizes on a daily basis," Varwig recalls. Next, the team benchmarked PHL in relation to other airports, researched current industry trends and factored in likely future regulatory requirements before brainstorming about ways to improve the airport's security posture.

Faith Group shared its findings with PHL executives in January 2015. General categories of recommendations included improving overall security infrastructure, updating cargo areas and critical infrastructure, upgrading the access control system, enhancing CCTV coverage and improving the emergency operations center.

"Now I have a complete review of where our strengths and weaknesses are," Tufts reflects. "We broke it up into three parts: our existing conditions, gap analysis and recommendations for a six-year roadmap."

Before the 2015 presentation, the airport's annual budget included $10.9 million of access control system improvements to be completed in multiple phases.

"Technology is ever-advancing and ever-changing," Tufts comments. "We wanted to make sure that we can get to the end of the pipeline; so we started with an upgrade to our access control system. That will bring us to the latest, greatest technology."

Kalpesh Trivedi, an employee of Arora Engineers since 2003, works with PHL's engineering department as a resident consultant project manager. Trivedi has been instrumental in ushering the security projects designed by Faith Group through the city procurement process and managing the associated implementation and construction.


KALPESH TRIVEDI

"At present, we are upgrading the 20-year-old access control system throughout the airport," Trivedi reports, noting that the entire program was broken into three stages. "We already completed Phase I and are in progress with Phase II. We just went through the procurement process and are about to award the contract to an electrical contractor to start Phase III."

Photo: Kenneth D. Aston Jr., Philadelphia International Airport

Meanwhile, other elements of the plan have graduated from master planning to conceptual development, where they become identified capital improvement projects. A secure perimeter — both physical and procedural — has emerged as the airport's top focus, reports Tufts.

Perimeter security not only includes protecting planes and equipment on the airfield, but also the airport's access control systems, badging systems and other security programs, he specifies.

## Now & Later

Varwig currently sees a huge emphasis on perimeter security improvement throughout the industry, even though such initiatives are generally not federally funded projects. Most are funded through individual airport capital improvement programs, which are frequently fluid. As an airport's priorities change, work sequences are adjusted and projects flow into a new calendar year/annual capital improvement budget, she explains.

"It (perimeter security) is obviously something we recommended as part of our master plan for PHL; it just wasn't short-term," Varwig informs. "You have what needs to be in a bucket for the next couple years, and then what needs to be funded in the three- to five-year timeframe."

Beyond prioritizing projects, Varwig considers it vital to continue working closely with PHL to ensure that recommendations can be realistically deployed.

"You want to look under all the rocks. You want to try to get as many viewpoints as you can. It is hard to self-assess," Varwig reflects. "Working in a team environment with the client is the best approach to assuring that the final recommendations consider all the stakeholder requirements. It is about the full spectrum – policy, procedures, technology and staffing – and how you balance all of those things together to make a recommendation that makes sense."