

Best Practices in Perimeter Security - Intelligence-Led Layered Security

Presenters



- Brandon Michael Collins, Intelligence Coordinator
- Developed a robust, viable and interconnected intelligence program at the Houston Airport System
- Graduate of the US Army's Military Intelligence Advanced Course and current student at South Texas College of Law
- Military Intelligence Captain, US Army Reserve

Presenters



- President of New Age Security Solutions.
- Former Director of Security at Tel Aviv Ben-Gurion International Airport and the Israel Airport Authority and is currently
- World-leading security expert on aviation, maritime and law enforcement with more than 30 years of Israeli and worldwide security-related experience

The Best Perimeter?

HOSPITALITYLAWYER.COM PRESENTS
2011 THE GLOBAL CONGRESS
ON LEGAL, SAFETY & SECURITY
SOLUTIONS IN TRAVEL
AUGUST 25-28, 2011 HOUSTON



<http://www.inetours.com/Pages/SF-photos/Alcatraz/Columbus-Alcatraz.html>

Overview

- Intelligence drives operations
- The Four D's of effective perimeter defense (Gruber, 2006)
- Public vs. Secure Facilities
- Incorporation of security layers to harden a “soft” target

Intelligence drives operations

- Threat Vulnerability Assessment (TVA)
 - Establish a Common Operation Picture (COP)
 - Establish a statement of intent
- Priority Intelligence Requirements
 - Who, What, Where, When, Why, How
 - Guide the intelligence process to meet intent
- Purpose
 - Build or upgrade facility with threat in mind

The Four D's to effective perimeter defense (Gruber, 2006)

- Deter
 - Visual Deterrence
 - First line of defense
- Deny
 - Ultimate goal is to deny
 - Push attackers as far away as possible



The Four D's to effective perimeter defense (Cont'd)

- Detect
 - Must be done quickly
 - Combine layers to accomplish
- Delay/Respond
 - Delay suspect for apprehension
 - Multiply layers needed



Public vs. Secure Facilities

- Public Facility (Hotel, Mall, Movie Theater, etc.)
 - Most difficult to protect
 - Multiple high-population facilities in every town
 - The open access is key to facility's survival



Public vs. Secure Facilities (Cont'd)

- Public/Secure Facility
- (Airport, train/subway, etc.)
 - “Blended areas”
difficult to defend
 - Long history of
attacks and future
attacks planned
 - Public access is key
to survival
 - Not ONE answer



Incorporation of security layers to harden a “soft” target



- Access-Control Roster
- Access-Control Card Readers
- Closed-Circuit Television with Digital Video Monitors
- License Plate Recognition
- Mounted Patrol
- Old Fashioned Fencing
- Additional Options

Houston's Layered Approach

Technology

- Extensive CCTV
- Access control is limited to those who need access for their specific job

Outside of Airport Proper

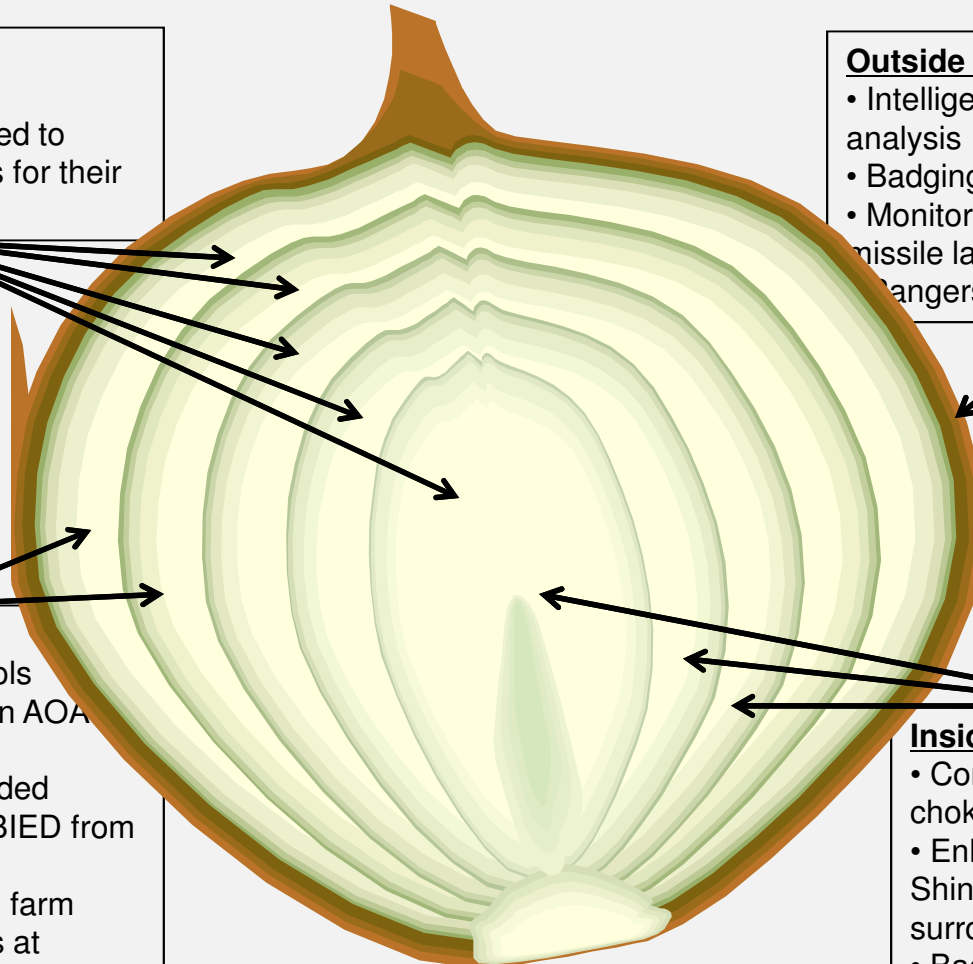
- Intelligence gathering and analysis
- Badging of Employees
- Monitor sites for possible missile launch
- Rangers patrol on horseback

Airport Proper

- Perimeter Fence patrols
- Vehicle/Foot patrols on AOA
- Traffic control
 - No vehicle unattended
- Bollards to prevent VBIED from attacking lobby
- Patrol /monitoring fuel farm
- Inspections for LVIEDs at loading docks
- Extensive coordination with HPD/FBI/TSA/CBP etc

Inside Airport

- Conduct BPR at chokepoints
- Enlist Sky Caps and Shoe Shiners to be aware of surroundings
- Badge challenges
- Threat Containment Unit at checkpoints



Questions?



© Houston Airport System

Factors & best practices in terminal security

Presented by
Rafi Ron
CEO
NASS



Introduction

- The shift from traditional Law Enforcement to Security.
- Terrorists & criminals. Are they the same breed?
- The regulatory perspective. Is it enough?
- The role of local and Federal government.
- Responsibility & Authority

Security planning

- Define the threats.
- Develop a policy paradigm.
- Carry out a Risk Analysis.
- Develop a Security Master Plan

- Create Design Guidance Criteria

- Build and commission.

- Create a full detailed security program
- Manage .

Pillars of terminal Security

- Organization
 - Design
 - Technology
 - Operations
- Information management

The Security Organization



- Responsibility
 - Authority
 - Accountability
- Daily management
- Emergency management

Security design factors

- Structure Blast resilience
- Non structural blast mitigation.
 - Fire Safety
 - Ventilation control
 - Evacuation options

Security Systems

- Access Control
- Surveillance & Video Analytics
- CBR Detection
- Special sensors
- LPR
- **C4I & Situation awareness platforms.**

Information Management



- Situation awareness
- Data bases
- Sensors
- Operational procedures
- BPR
- CAD & Technical information
- Reports

Operations

- Procedures
 - Staffing
 - Skills
- Behavior Pattern Recognition™

Terminal Security principles

- Deterrence
- Detection
- Interdiction
- Incident management
 - Rescue
 - Recovery

Coordination

- Local Law Enforcement
 - First responders
- Tenants & concessioners
 - Federal agencies

The Security Culture

HOSPITALITYLAWYER.COM PRESENTS
2011 THE GLOBAL CONGRESS
ON LEGAL, SAFETY & SECURITY
SOLUTIONS IN TRAVEL
AUGUST 25-28, 2011 HOUSTON


NASS
New Age
Security
Solutions

- Motivation
 - Training
 - Discipline
 - Leadership

Summary

- The importance of proper planning.
- The security upgrade.
- The intelligence approach to security.
- Information integration
- Deterrence, Detection & interdiction.
- Preparedness & emergency management

Thank you for your attention

New Age Security Solutions
45025 Aviation Drive 3rd floor
Dulles VA 20166

Email hq@nasscorp.com

Website www.nasscorp.com