NATIONAL SAFE SKIES ALLIANCE

Program for Applied Research in Airport Security
PARAS 0010 Project Summary

Project Title:	Guidance for Protecting Access to Vital Systems Impacting Airport Security
Program Officer:	Jessica Grizzle 865-738-2080 Jessica.Grizzle@sskies.org
Research Agency:	Faith Group
Principal Investigator:	Royce Holder
Contract Time:	10 Months
Effective Date:	April 25, 2016
Funds:	$150,000

BACKGROUND

Airports house and utilize many vital systems that are critical to daily operations. For example, video management/surveillance systems, access control systems, credentialing systems, and server rooms all play a key role in many US airports. Access to these systems and physical spaces must be controlled to guard against nefarious activity.

A growing area of concern is the administration and management of authorized access—how it is granted, tracked, monitored, and revoked. Currently, there is little guidance to assist airport operators in effectively and efficiently administering and managing such access.

Research is needed to provide guidance for airport operators to mitigate risk associated with unauthorized access to these vital systems.

OBJECTIVE

The objective is to develop a guidebook of principles, considerations, lessons learned, and successful practices for administering and managing access to vital systems (e.g., video management/surveillance systems, access control, and credentialing) and physical spaces where those systems reside. The guidance should be scalable to airports of all types and sizes.

The guidance should include, at a minimum:

- Security control considerations to be addressed during system design, redesign, expansion, and upgrades
    - External and remote connectivity
    - System administration and oversight
    - Identification of system components
    - User levels and security permissions
    - Physical access to spaces and equipment
- Best practices for granting, administering, and managing access locally, remotely, and externally to include:
    - Which systems should be included?
    - Who controls the system and grants access?
    - What criteria are used for determining access?

  - Who should retrieve information?
  - Who should alter system coordinates and parameters?
  - Who should access physical space and equipment?
  - How should access to physical space and equipment be controlled?
  - How should access be monitored?
  - How should unauthorized/unusual activity be detected?
- Sample policies for granting, administering, and managing access
- Guidance for identifying/determining current roles and responsibilities for system administration and management, which may include process mapping
- Glossary of commonly used terms
- Suggested future research