NATIONAL SAFE SKIES ALLIANCE

Program for Applied Research in Airport Security
PARAS 0030 Project Summary

Project Title:	Guidance for Access Control System Transitions		
Program Officer:	Jessica Grizzle	865-738-2080	Jessica.Grizzle@sskies.org
Research Agency:	LAM LHA		
Principal Investigator:	Andrew Goldsmith		
Effective Date:	July 1, 2020		
Contract Time:	13 Months		
Funds:	$174,479		

BACKGROUND

Access control systems at airports are made up of both physical and logical components. Physical components are the hardware and software installed at portals that grant or deny access through that portal based on established permissions. Logical components refer to IT networking permissions, parameters, and other means of secure access, and the transfer of data across a network. The components may be integrated with other related systems, such as an Identity Management System (IDMS) or Video Management System (VMS), or may be stand alone and operate independently of any peripheral systems. If integrated, some level of communication and data movement between the systems is required, along with other IT-related functions, which would be impacted by changes to system components. Even if no integration exists, changes to physical components would still impact the overall system through user requirements, training, and transition planning.

Changes to an access control system may consist of an upgrade to an existing system or include the design and installation of a new system. Any such change, no matter the scale, will have an impact on the remainder of the system. In order to make well-informed and effective procurement decisions, airports must understand the reach of the access control system, and the potential effects of change to other components and users of the system.

OBJECTIVE

The objective of the research is to produce guidance detailing considerations, pitfalls, and lessons learned during access control technology selection, procurement, and implementation. At a minimum, topics should include:

- Components of access control systems and potential integrations
    - Credential readers
    - System infrastructure and communication protocols
    - Servers
- Considerations to determine upgrade or replacement, including:
    - Status of existing access control system, e.g., end of life, adding an authentication factor, or governance (procurement requirement)
    - IT requirements
    - Existing infrastructure
    - Stakeholder needs
    - Integration with existing systems, such as IDMS and VMS
    - Legal implications – PII, etc.
    - Regulatory requirements
    - Cost/benefit
- Considerations and potential pitfalls during procurement/selection

- Considerations during transition, including:
  - Potential technology interference/operating parallel systems
  - Stakeholder identification and coordination
  - Operational Readiness and Acceptance Testing
  - Device naming
  - Pitfalls and lessons learned during transition
- Future planning
  - System expandability
  - Enhancement options
  - Potential regulatory changes

The outreach should be comprehensive and the resulting guidance scalable so that airports of all sizes and resource levels can benefit.