NATIONAL SAFE SKIES ALLIANCE

Program for Applied Research in Airport Security
PARAS 0007 Project Summary

Project Title:	Quick Guide for Airport Cybersecurity
Program Officer:	Jessica Grizzle 865-738-2080 Jessica.Grizzle@sskies.org
Research Agency:	Synergy Solutions, Inc.
Principal Investigator:	David Morrow
Contract Time:	15 Months
Effective Date:	April 6, 2016
Funds:	$350,000

BACKGROUND

According to the US Department of Homeland Security (DHS):

> Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.[1]

In addition to the generalized cyber threats to our nation's infrastructure, the airport and aviation sector remains a prime target for terrorists. Airports also face the ongoing threat from criminals seeking to use the airport system to facilitate illegal activities and enter via perimeter, access controls, or machine controls. Both the terrorist and criminal threats to airports and the aviation system are further complicated by the potential for "insiders"—those employed at the airport that have access to secured areas—to use their access to conduct criminal or terrorist activities. Compounding this insider threat is the vast number of individuals across the US airport system that have access to airport secured areas and security systems, each a potential actor, facilitator, or even an unwitting accomplice to a cyber-attack on an airport's security system that would leave it vulnerable to terrorism or criminal activity.

Given the increasing potential for cyber-attacks on airports, combined with the increasing sophistication and daring of cyber-attackers, it is critically important that airports be adequately prepared. For airports with limited IT technical or security resources and knowledge, this includes meeting existing cyber-threats as well as ongoing information exchange, training, and planning to meet potential new cyber

[1] http://www.dhs.gov/cybersecurity-overview, September 2015

threats. While multiple sources of information exist, it is often difficult to determine what actionable steps to take to establish and/or enhance their cybersecurity posture.

OBJECTIVE

The objective of this research is to develop guidance to establish and/or enhance a cybersecurity posture for safe operations of airports, along with an accompanying interactive tool to facilitate implementation. The concepts and practices in the guidance should be usable by varying levels of airport operators, scalable to airport types and sizes, and system agnostic. Innovative approaches to the methods and processes outlined are encouraged to make it as simple and intuitive as possible for the user.

The guidance should at a minimum:

- Provide a basic step-by-step method to assess the current state of airport practices within various areas of operations, where cyberspace challenges interconnected and/or isolated systems (Reference Appendix B of Airport Cooperative Research Program [ACRP] Report 140)
- Provide a basic step-by-step method to evaluate security risks associated with cyberspace
- Be presented in a phased, prioritized approach
- Provide successful practices for mitigating known threats and vulnerabilities as well as maintaining security posture as threats and vulnerabilities evolve
- Present visual representations of the critical concepts to enhance comprehension and understanding
- Include an appendix of relevant resources
- Include checklists, flowcharts, and templates for ease of use
- Include customizable presentation for use by airport operators to introduce the importance and applicability of cybersecurity
- Include a glossary of commonly used cybersecurity industry terminology and acronyms, in addition to those referenced in the guidance

The accompanying tool should be intuitive, vendor agnostic, and developed in a commonly available, open source, and portable format (not web hosted) that derives a response from the information entered. At a minimum, the tool should:

- Gather data from the basic step-by-step assessment of the current airport practices within various areas of operations where cyberspace challenges interconnected and/or isolated systems (Reference Appendix B of ACRP Report 140).
- Gather data from the basic step-by-step evaluation of security risks associated with cyberspace
- Serve as a data repository for information gathered during the assessment(s), with an option to export data in a useable format
- Use a simplified, standardized scoring methodology that maps to industry best practice (e.g., Forum of Incident Response and Security Teams' *Common Vulnerability Scoring System*, NIST *Guide for Conducting Risk Assessments*, ISO/IEC 27005:2011 *Information Technology—Security Techniques—Information Security Risk Management*, and US-CERT's *Operationally Critical Threat, Asset, and Vulnerability Evaluation*)
- Present assessment results in a phased, actionable approach
- Generate useful customizable reports and a tailored, initial cybersecurity plan