[redacted]

Transportation Security Administration

Office of Security Technology

Airport Perimeter Security Projects for FY08-09

FINAL REPORT

Tri-Cities Regional
Tennessee/Virginia Airport (TRI)

CyberLock Electronic Access Control Solution

U.S. Department of Homeland Security
Transportation Security Administration
Office of Security Technology
Advanced Surveillance Program
701 South 12th Street
Arlington, VA 20598-6016

[redacted]

OVERVIEW

INTRODUCTION

In fiscal year (FY) 2006, the Transportation Security Administration (TSA) announced opportunities for general perimeter security enhancement projects at airports with typical configurations and existing barriers, such as fencing and concrete barricades. The announcement requested information from airport authorities on existing airport perimeter security vulnerabilities and proposals to mitigate those vulnerabilities through the inventive use of available technologies at intended perimeter access points (such as vehicle gates), perimeter boundaries, and terminals.

In FY 2008, TSA reissued the Airport Perimeter Security (APS) announcement to all airports, along with a second announcement addressing small to medium-sized airports with few or no barriers around their perimeters. The second announcement was for the Virtual Perimeter Monitoring System (VPMS) project intended to test a more elaborate solution that would better fit a smaller airport. The VPMS solution was developed by the Navy.

TSA requested airports provide white papers explaining the security deficiencies to be addressed and proposals, including technologies to be deployed and full life-cycle project cost estimates. 65 airports responded to the FY 2006 request and 35 airports responded to the FY 2008 requests. The airports proposed projects of varying complexity, from installation of a single piece of equipment to sophisticated, integrated systems.

Six airports were selected in FY 2006 to participate in the APS projects. In FY 2008 and 2009, TSA selected six additional airports for participation in APS and three airports for VPMS projects.

The attached report covers the test results of only one of the 15 total test sites. TSA plans to release each report singularly as the test results are completed and made available.

IMPLEMENTATION

This project pertained to the evaluation of the CyberLock electronic access control solution at the Tri-Cities Regional Tennessee/Virginia Airport (TRI). The CyberLock solution is a proprietary product of Videx, Incorporated of Corvallis, Oregon. This innovative lock system converts existing mechanical cylinder locks into an access control system. The combination of electronic lock cylinders, programmable CyberKeys, and CyberAudit software is intended to create a solution capable of tracking and controlling access to every lock at the facility's perimeter. This solution is unique in that there is no need for additional power or communication resources, which normally are unavailable in remote perimeter areas without intensive infrastructure upgrades. The CyberLock solution was installed, operated, maintained, and evaluated as a

[redacted]

security enhancement solution for outer-perimeter gates for access control and monitoring of usage activity.

National Safe Skies Alliance (Safe Skies) provided independent verification and validation (IV&V) services and operated along with airport authorities to verify that the CyberLock system enhancements met the airport's security expectations. The IV&V was concluded November 20, 2009.

System maintenance and lost or stolen keys are issues of concern to airport security personnel. Under the CyberLock system, the loss of a master key would require one person to reprogram a single key, which would take approximately 15 minutes, and then reprogram the individual locks in the field. The total time required to reprogram the locks in the field is directly dependent on the number of locks and their locations. The estimated labor to reprogram all 18 locks at TRI is approximately 3 hours. The CyberLock system can be electronically refreshed instead of being replaced, which eliminates the need for new hardware in the case of lost keys or the institution of service contracts for maintenance needs. Reprogramming the perimeter locks at TRI requires the labor of a single person to complete the task.

The Safe Skies Lead Test Engineer (LTE) generated a site survey document based on a preliminary survey of the locations prior to the deployment of the security technology improvements. The LTE developed operational testing procedures used as the basis for determining if the system met the security requirements of TRI airport authorities. Representatives of TSA, Safe Skies, and TRI convened to discuss and verify the system requirements prior to the implementation of evaluation procedures. The resulting operational data was analyzed by the Safe Skies statistical team and combined with the site survey information to generate the final report.

SUMMARY

From the data presented in the final report, it is clear that the CyberLock system had a positive effect on the TRI perimeter security efforts. [redacted] The system performed to a 100% success rate on scheduling and recording accuracy (time audits). Reviews from daily users were positive, with the exception of the CyberKey being larger than traditional keys. No operational troubles were indicated by the officers or contract personal interviewed.

Reviews of the systems administrative functions were positive. The system allows administrative personnel to investigate key and lock activity through data filtering options. Complete audit reviews were possible within minutes and could be arranged according to individual people, groups, locks, dates, or specific time ranges. Efficient use of the system requires that at least one person, preferably an airport security professional, become exceptionally familiar with the menus and options. Comments received from TRI personnel describe the software as both functional and user-friendly.

[redacted]

[redacted]

DHS/TSA 2600.02.01.10-007	**Airport Perimeter Security (APS) Operational Testing & Evaluation (OT&E) Support – Tri-Cities Regional Tennessee/Virginia Airport (TRI) Test Report** COPYRIGHT © 2010 National Safe Skies Alliance, Inc. ALL RIGHTS RESERVED	
	Project Performed by: National Safe Skies Alliance 110 McGhee Tyson Boulevard Suite 201 Alcoa, TN 37701	Safe Skies Author(s) Scott Arnold Jeff Vanvactor
	Project Performed for and funded by: U.S. Dept. of Homeland Security Transportation Security Administration 601 S. 12th Street Mail Stop TSA-16 Arlington, VA 22209	TSA Technical Review Team Charles Kelley John Nestor David Taylor
	January 2010 Final Report	

[redacted]

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

COPYRIGHT © 2010 National Safe Skies Alliance, Inc.

ALL RIGHTS RESERVED. No part of this work may be reproduced, transcribed, or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution, or information storage and retrieval systems—without the prior written permission of the publisher.

For permission to use material from this text or program, submit a request to National Safe Skies Alliance by email at safeskies@sskies.org.

[redacted]

Technical Report Documentation Page

1. Report No. DHS/TSA—10-007	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Airport Perimeter Security Operational Testing and Evaluation Support – Tri-Cities Regional Airport		**5. Report Date** January 2010 **6. Performing Organization Code**
7. Author(s) Scott Arnold, Jeff Vanvactor		**8. Performing Organization Report No.** DHS/TSA—2600.02.01.10-007
9. TSA/TSL Reviewer(s) Charles Kelley, John Nestor, David Taylor		**10. Work Unit No. (TRAIS)**
11. Performing Organization Name and Address National Safe Skies Alliance 110 McGhee Tyson Center Suite 201 Alcoa, TN 37701		**12. Contract or Grant No.** 00-G-019 **13. Type of Report and Period Covered** Final Report, January 2010
14. Sponsoring Agency Name and Address U.S. Department of Homeland Security Transportation Security Administration 601 S. 12th Street Mail Stop TSA-16 Arlington, VA 22209		**15. Sponsoring Agency Code** TSA-16

16. Supplementary Notes
This plan was prepared by Scott Arnold of National Safe Skies Alliance.

17. Abstract

National Safe Skies Alliance was asked by the Transportation Security Administration to support the Airport Perimeter Security (APS) pilot program. The APS offers U.S. airports an opportunity to enhance security capabilities by applying commercial off-the-shelf technologies. Through this program, Tri-Cities Regional Tennessee/Virginia Airport has implemented the Videx CyberLock® access control solution.

Safe Skies served as an independent evaluator by conducting Operational Testing and Evaluation (OT&E) of the CyberLock system. This report presents the evaluation results and collective observations to reflect the operability of the CyberLock within an airport environment. Safe Skies conducted the assessment in November 2009.

18. Key Words
Access Control, CyberKey®, CyberLock, Electronic Lock, Perimeter, Tri-Cities, TRI, Videx

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
SSI/FOUO	Unclassified	57	

Reproduction of completed page authorized

[redacted]

[redacted]

DOCUMENT CHANGE HISTORY

Version	Description/Author	Date(s)	TSA Approval
.1	Initial Draft/Charles Kelley	December 2009	
1.0	Final Draft/Charles Kelley	January 2010	

[redacted]

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	vi
ACRONYMS	xii
1. INTRODUCTION	1
1.1 Background	1
1.2 Purpose	1
2. SCOPE	1
2.1 Objective	1
2.2 Limitations/Risks/Assumptions	2
3. SYSTEM/PROCESS DESCRIPTION	2
3.1 Specifications	3
3.2 Operating Principles	3
3.3 Installation	6
4. METHODOLOGY	9
4.1 Sites/Schedule	9
4.2 Critical Operation Issues	9
5. RESULTS	10
5.1 Integration (COI: 1A and 1B)	10
5.2 Operational Success Rates (COI: 2A and B)	11
5.3 Scheduling and Access Event Recording (COI: 2B and 3A)	13
5.4 Process Times (COI: 2C)	16
5.5 Reprogramming Requirements and Cost Benefits (COI: 2D and 4A)	16
6. OBSERVATION/RECOMMENDATIONS	17
7. REFERENCES	18

APPENDIX A - TRI PERIMETER ZONE DESCRIPTION

APPENDIX B - PROJECT COSTS

APPENDIX C – TEST CORRELATION AND ATTEMPTS DATA

APPENDIX D – TEST KEY TIME AUDIT JOURNALS

APPENDIX E - AUDIT TRAIL EVENTS AND DEFINITIONS

LIST OF TABLES

Table 1. Pass/Fail Results – CyberKeys Programmed to Allow Access to Gates vii
Table 2. Pass/Fail Results – CyberKeys Programmed to Allow Access to Doors vii
Table 3. Pass/Fail Results – CyberKeys Programmed to Deny Access to Gates viii
Table 4. Pass/Fail Results – CyberKeys Programmed to Deny Access to Doors viii
Table 5. Time Audit Results – CyberLock Gates and Doors ix
Table 6. Hypothetical Comparison Between Traditional Lock and CyberLock Systems x
Table 7. Installation Cost Summary x
Table 8. Installation Cost Summary 6
Table 9. Critical Operational Issue, Measures, and Tasks 10
Table 10. Pass/Fail Results – CyberKeys Programmed to Allow Access to Gates 11
Table 11. Pass/Fail Results – CyberKeys Programmed to Allow Access to Doors 12
Table 12. Pass/Fail Results – CyberKeys Programmed to Deny Access to Gates 12
Table 13. Pass/Fail Results – CyberKeys Programmed to Deny Access to Doors 13
Table 14. Time Audit Results – CyberLock Gates and Doors 13
Table 15. Hypothetical Comparison Between Traditional Lock and CyberLock Systems 17
Table 16. Equipment and Installation Costs B-1
Table 17. Test Key and Serial Number Correlation C-1
Table 18. Gate and Lock Assignments C-2
Table 19. Total Attempts by Gate – CyberKeys Programmed to Allow Access C-3
Table 20. Total Attempts by Door – CyberKeys Programmed to Allow Access C-4
Table 21. Total Attempts by Gate – CyberKeys Programmed to Deny Access C-5
Table 22. Total Attempts by Door – CyberKeys Programmed to Deny Access C-6
Table 23. Total Mechanical Resists by Gate by CyberKeys C-7
Table 24. Total Mechanical Resists by Door Lock by CyberKeys C-8
Table 25. Time Audit Journal – November 16, 2009 D-1
Table 26. Time Audit Journal – November 17, 2009 D-2
Table 27. Time Audit Journal – November 18, 2009 D-3
Table 28. Time Audit Journal – November 19, 2009 D-4
Table 29. Audit Trail Events for CyberKey System E-1
Table 30. Audit Trail Events for CyberLocks E-4

LIST OF FIGURES

Figure 1. Examples of CyberLock Cylinders 2
Figure 2. CyberLock Padlock and CyberKey 3
Figure 3. CyberLock and CyberKey With Power Supply 4
Figure 4. Standard Mechanical Cylinder Replaced by CyberLock Cylinder 4
Figure 5. CyberLock Authenticator Unit 5
Figure 6. CyberKey Grand Master Key 6
Figure 7. Keyport Located Outside TRI Badge Office 7
Figure 8. CyberLock Keyport in Ready Mode 7

[redacted]

Figure 9. Perimeter Gate With Chain and CyberLock Installed 8
Figure 10. Perimeter Door With CyberLock Cylinder Installed 9
Figure 11. CyberAudit Report – Gate M 14
Figure 12. CyberAudit Report – Test Key #12 15
Figure 13. CyberLock Test Positions – TRI Project Layout Plan A-2
Figure 14. CyberLock Test Positions – TRI Aerial View A-3

[redacted]

[redacted]

EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) has established the Airport Perimeter Security Program (APS) in order to promote innovative applications of new technologies to the critical perimeter areas within airport facilities. This program provides direct funding to individual airports for the initial purchase and installation of commercial off-the-shelf technologies, as well as the operational testing and evaluation (OT&E) resources and other support services necessary to assess the effectiveness of the new perimeter protection systems.

The TSA has asked National Safe Skies Alliance (Safe Skies) to provide OT&E services for some of the APS projects. In addition to OT&E support, Safe Skies works with airport authorities to evaluate the suitability of technologies within an operational environment.

This pilot pertains to the evaluation of the CyberLock® electronic access control solution, which is a proprietary product of Videx, Incorporated of Corvallis, Oregon. This innovative lock system converts existing mechanical cylinder locks into an access control system. The combination of electronic lock cylinders, programmable CyberKeys®, and CyberAudit® software allegedly creates a solution capable of tracking and controlling access to every lock at the facility's perimeter. This solution is unique in that there is no need for additional power or communication resources, which normally are unavailable in remote perimeter areas without intensive infrastructure upgrades.

The CyberLock solution was installed, operated, and maintained at the Tri-Cities Regional Tennessee/Virginia Airport (TRI). It was deployed and evaluated as a security enhancement solution for outer-perimeter-gate access control and monitoring. Safe Skies collected data for a 5-day period at TRI (November 16-20, 2009).

This report presents the evaluation results and collective observations to reflect the operability of the CyberLock within an airport environment.

Tables 1 and 2 display the pass/fail results of CyberKeys programmed to allow access to 11 gates and 2 doors, respectively. [redacted]

[redacted]

[redacted]

Table 1. Pass/Fail Results – CyberKeys Programmed to Allow Access to Gates

Gate	Access Allowed (Pass)	Access Denied (Fail)
[redacted]		

Table 2. Pass/Fail Results – CyberKeys Programmed to Allow Access to Doors

Door	Activity	Access Allowed (Pass)	Access Denied (Fail)
Door 1	[redacted]		
Door 2			
Total			

Tables 3 and 4 display the pass/fail results of CyberKeys programmed to deny access to 12 gates and 2 doors, respectively. [redacted]

[redacted]

[redacted]

Table 3. Pass/Fail Results – CyberKeys Programmed to Deny Access to Gates

Gate	Access Denied (Pass)	Access Allowed (Fail)
[redacted]		

Table 4. Pass/Fail Results – CyberKeys Programmed to Deny Access to Doors

Door	Access Denied (Pass)	Access Allowed (Fail)
Door 1	[redacted]	
Door 2		
Total		

In order to evaluate the accuracy of system records, access events from each key were downloaded, and a sample of access events was audited. Data downloaded from the CyberKeys was assessed in conjunction with the actual times of the access attempts at each gate and door. A "pass" occurred when data from the CyberLock reporting system (e.g. lock ID, date and time of attempt, and event) matched the data recorded by testing personnel for the attempt.

Table 5 displays the results of a time audit conducted on gate access attempts. All locks and test keys were included in the time audit sampling evaluation. The system performed to a 100% success rate on scheduling and recording accuracy.

[redacted]

[redacted]

Table 5. Time Audit Results – CyberLock Gates and Doors

Date	Number Samples	Passed Time Audit
11/16/2009	21	100%
11/17/2009	30	100%
11/18/2009	29	100%
11/19/2009	24	100%
Total	104	100%

System maintenance and lost or stolen keys are issues of concern to airport security personnel. Under the CyberLock system, the loss of a master key would require one person to reprogram a single key, which would take approximately 15 min, and then reprogram the individual locks in the field. The total time required to reprogram the locks in the field is directly dependent on the number of locks and their locations. The estimated labor to reprogram all 18 locks at TRI is approximately 3 hrs. The CyberLock system can be electronically refreshed instead of being replaced, which eliminates the need for new hardware in the case of lost keys or the institution of service contracts for maintenance needs. Reprogramming the perimeter locks at TRI requires the labor of a single person to complete the task.

Table 6 shows a hypothetical scenario comparison between the CyberLock system and the traditional lock and key system at TRI. The estimates were developed by TRI and Safe Skies.

[redacted]

[redacted]

Table 6. Hypothetical Comparison Between Traditional Lock and CyberLock Systems

Hypothetical Scenario: *An airport security vehicle is vandalized and a master key is stolen. The key allows access to 18 locks in the facility; 90 employees hold keys to the facility.*		
	Traditional Lock & Key System	**CyberLock System**
Consequences	• Security operations is informed that a Master Key is stolen • Estimates are called in to purchase new cores for 13 gate and 5 door locks **$55 per core** • Purchase new keys for 90 people **$1.00 per key** • Assume contractor or union costs to perform labor **$27 per hr** • Assume 30 min time to re-core a lock and move to next location **9 hours** • Labor for one person to reissue new keys **9 hours**	• Security operations is informed that a master CyberKey is stolen • Security operations programs a new master key • The programmer key is updated with the newest security information • The security operations staff physically reprograms each lock with a Programmer Key • Assume comparable costs to perform labor **$27 per hr** • Total time to complete all events listed above **3 hours, 15 min**
Total Time	3-4 days	1 day
Total Cost	$1,566	$88

The installation cost incurred by TRI is summarized in Table 7.

Table 7. Installation Cost Summary

Items	Cost
CyberLock equipment, freight	$25,921
Computer, monitor, printer, cable	$2,185
Installation labor	$1,700
Total	**$29,806**

[redacted]

[redacted]

Reviews from daily users were positive, with the exception of the CyberKey being larger than a traditional key. No operational troubles were indicated by the officers or contract personnel who were interviewed.

Reviews of the system's administrative functions were also positive. The system allows administrative personnel to investigate key and lock activity through data filtering options. Complete audit reviews were possible within minutes and could be arranged according to individuals, groups, locks, dates, or specific time ranges. Comments received from TRI personnel describe the software as both functional and user-friendly.

[redacted]

[redacted]

ACRONYMS

APS	Airport Perimeter Security Program
COI	Critical Operational Issue
FAA	Federal Aviation Administration
OT&E	Operational Testing and Evaluation
TRI	Tri-Cities Regional Airport – FAA Designation
TSA	Transportation Security Administration

[redacted]

[redacted]

1. INTRODUCTION

As the air transportation industry expands, so, too, do the security threats against it. Screening, monitoring, biometrics, and explosive detection technologies have advanced quickly within the past 10 years to address the ever-increasing demand. The Transportation Security Administration (TSA) has established the Airport Perimeter Security (APS) pilot program, which offers U.S. airports an opportunity to enhance their perimeter security capabilities by employing new or innovative commercial off-the-shelf technologies. APS provides direct funding to individual airports for the initial purchase and installation of the technologies, as well as the operational testing and evaluation (OT&E) resources and other support services necessary to assess the operational effectiveness of new perimeter protection systems.

1.1 Background

Tri-Cities Regional Tennessee/Virginia Airport (TRI) located in Blountville, Tennessee was selected to participate in the APS program, and implemented a CyberLock® access control solution. Safe Skies provided support services on behalf of the TSA for the evaluation of the CyberLock solution at TRI. Operational testing of the CyberLock solution's integration, maintenance, and general performance was conducted by TRI and Safe Skies personnel.

1.2 Purpose

This report describes OT&E results for the deployment of the CyberLock access control within an operational airport. The conclusions drawn from this evaluation may be used by the TSA to assess the suitability of the CyberLock solution within an operational airport perimeter.

2. SCOPE

2.1 Objective

Safe Skies evaluated the effectiveness of the CyberLock system when installed in an operational airport perimeter-gate infrastructure at TRI. Test parameters included the following aspects:

- Critical performance features of CyberLock system
- Meeting airport security expectations for overall protection of the airport
- Associated cost benefit from the installation of the system

The operational test examined the basic functionality of the solution's more significant features, such as programming capabilities and locking mechanisms.

Any issues (e.g., time constraints, programming complications, etc.) that interfered with the integration process were recorded. End-user responses were also collected at the end of the evaluation.

[redacted]

[redacted]

2.2 Limitations/Risks/Assumptions

Safe Skies collected data from all affected gates and doors at TRI. Due to on-going construction activities, some positions were not available during the study. The final study sample sizes are based on the amount of data that was collected during the 5-day period. The CyberLock system was deployed at TRI with no modifications to the commercial off-the-shelf design by Videx, Inc.

Safe Skies performed an assessment of the CyberLock system in a previous project entitled *Pittsburgh International Airport: Videx, Inc. CyberLock® System Operational Evaluation Report* (DHS/TSA 2600.02.01.09-014). Tests were conducted to investigate operational weaknesses potentially caused by extreme temperatures and weather conditions. Therefore, these parameters were not re-evaluated during testing performed at TRI.

3. SYSTEM/PROCESS DESCRIPTION

The CyberLock, manufactured by Videx, Incorporated, of Corvallis, Oregon, is an electronic locking device that replaces mechanical locks or lock cylinders used in doors and padlocks. A CyberLock controls the access of an employee or subcontractor based on permissions programmed into a CyberKey® (see Figures 1 and 2). Access permission schedules are programmed into the keys using the CyberAudit® software. The access record information is stored within the CyberAudit software, where administrators can investigate all access activities.

The CyberLock solution was installed at normal access gateways throughout the TRI outer perimeter and integrated with the administrative system used to program assigned permissions.

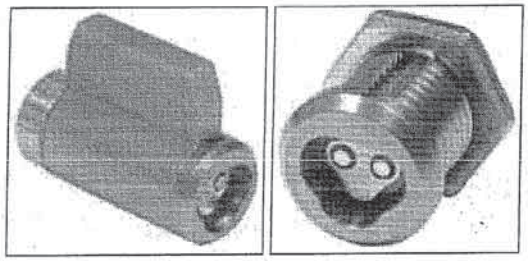

Figure 1. Examples of CyberLock Cylinders

[redacted]

[redacted]

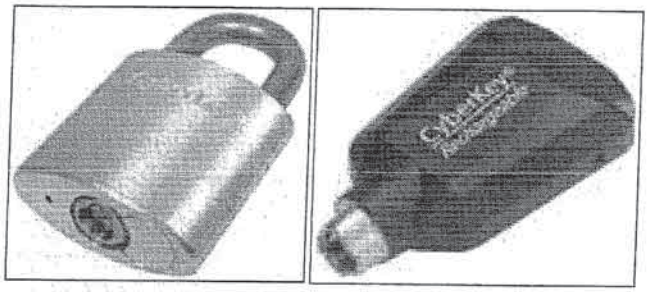

Figure 2. CyberLock Padlock and CyberKey

3.1 Specifications

The CyberLock System, manufactured by Videx, Inc. of Corvallis, Oregon, is an access control system that utilizes electronic locks and keys. It consists of five main components:

- CyberLocks
- CyberKeys
- Authorizers
- Programmers
- CyberAudit software

The CyberLock solution is proprietary equipment of Videx, Inc., and all subsequent equipment is standard for this type of installation. All end users of a facility perimeter would see a product configuration that is reasonably similar to the system installed at TRI.

3.2 Operating Principles

The CyberLock cylinder is an electronic version of a standard mechanical lock cylinder with several new features. Each unique lock does not require initial wiring or power, and does not contain any internal power source. The unique aspect of the CyberLock solution is that the power is found in the CyberKey and is transmitted to the CyberLock during an access attempt. Figure 3 displays the CyberLock and CyberKey with the power source. Upon successful contact with the CyberLock, a notification light on the CyberKey illuminates to indicate that the key is transmitting power.

[redacted]

[redacted]

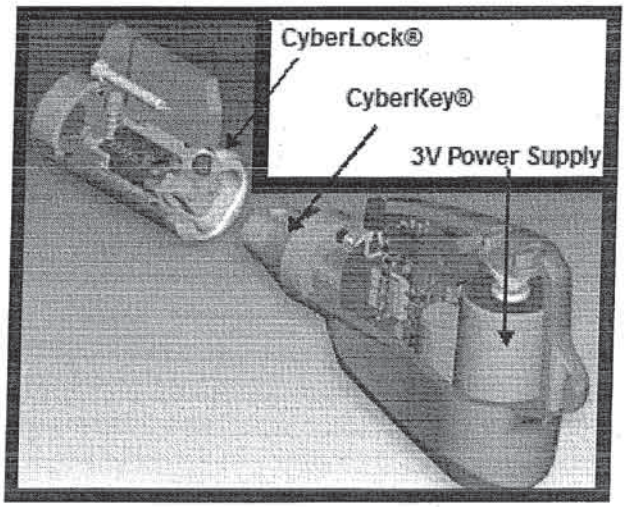

Figure 3. CyberLock and CyberKey With Power Supply

CyberLocks do not have a typical keyway, and cannot be picked like a typical mechanical lock. Purportedly, dirt and moisture will not interfere with the operation of the cylinder and the devices can resist forced rotation. Furthermore, the locks are designed to remain in the locked position in the event that tampering occurs. The conversion of a door lock by replacing a standard mechanical cylinder with a CyberLock cylinder is demonstrated in Figure 4.

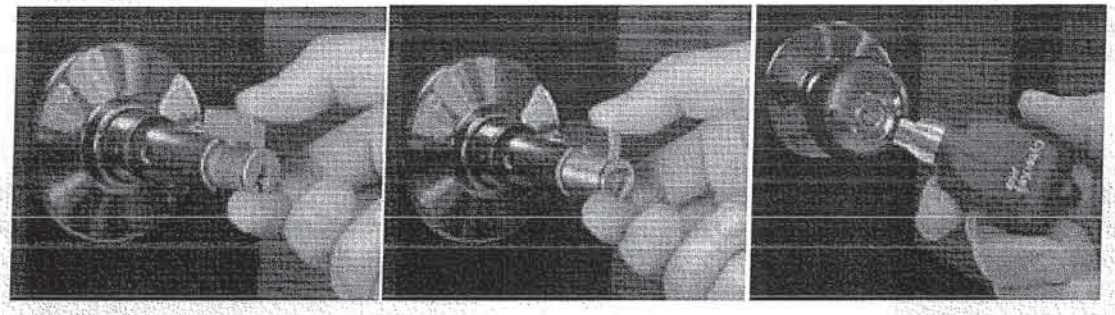

Figure 4. Standard Mechanical Cylinder Replaced by CyberLock Cylinder

Both the CyberKey and CyberLock are programmed with basic identification information, which is encrypted to the standards/passwords established by security administrators. Neither a lock nor key can be reproduced and then used to access other secured areas.

The CyberAudit Software is installed on a limited number of administrative terminals and connected to the authenticators via the local area network and fiber optic cable. Typically, Master Programming Key privileges are given to two administrative personnel who are

[redacted]

responsible for finalizing customized employee keys for access rights and programming all locks.

The CyberLocks are programmed with information specific to locations permitting easy reference identification. The CyberKey, however, is programmed with information pertinent to an individual user. Access rights and privileges for an individual key are selectively granted to specific locks for controlled periods of time. Once powered, the installed electronics of the devices relay identification and access permissions distinctive for that specific key and lock. The access event is digitally recorded and stored locally within both the lock and key regardless of admittance or rejection.

Locks do not necessarily require re-programming; however, keys may need refreshing periodically, or as established by facility security requirements. Individuals may need access to new areas, or access may be denied temporarily. Regardless of the need, the key can be reprogrammed or refreshed with new lock and schedule access privileges when it is inserted into an Authenticator unit (Figure 5). The Authenticator communicates with the key, downloads a history of access events, and refreshes the access rights.

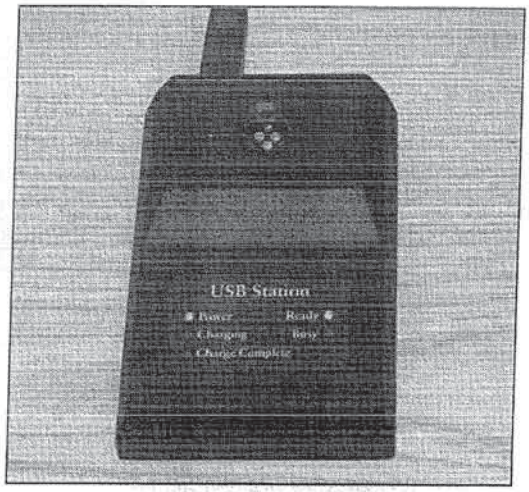

Figure 5. CyberLock Authenticator Unit

Each time a key is used at a lock, a record of the lock ID, date, and time is stored in the key, and a record of the key ID, date, and time is stored in the lock. Locks and keys also record all unauthorized attempts to open a lock with a CyberKey. The access history information is stored within the CyberAudit software, where administrators can investigate all access activities.

[redacted]

3.3 Installation

The CyberLock solution implemented at TRI consisted of the following major components:

- CyberLock – 13 gateways with padlocks, 5 doors
- CyberKey (model CK-IR7) – 160 Keys
- CyberAudit Software
- CyberKey Authorizer

The installation cost is summarized in Table 8.

Table 8. Installation Cost Summary

Items	Cost
CyberLock equipment, freight	$25,921
Computer, monitor, printer, cable	$2,185
Installation labor	$1,700
Total	**$29,806**

An itemized list of equipment and incurred cost for the CyberLock system is provided in Appendix B of this report.

The CyberAudit software was installed on a Dell Studio XPS 435T (6GB RAM) desktop computer, which operated as the system's programming terminal. The Grand Master CyberKey (Figure 6) was used to program locks and keys with a pre-programmed encrypted code. Both the [redacted]

Figure 6. CyberKey Grand Master Key

[redacted]

[redacted]

[redacted]

CyberLock padlocks were installed with new chains on perimeter gates as displayed in Figure 9.

[redacted]

[redacted]

[redacted]

Figure 9. Perimeter Gate With Chain and CyberLock Installed

Figure 10 displays a CyberLock cylinder installed on a perimeter door.

[redacted]

[redacted]

[redacted]

Figure 10. Perimeter Door With CyberLock Cylinder Installed

4. METHODOLOGY

4.1 Sites/Schedule

TRI, located in Northeast Tennessee, is designated as a CAT III airport by the Federal Aviation Administration (FAA). TRI has over 1,000 acres of property inside the perimeter fence with approximately 30 Air Operations Area access points. Safe Skies collected data for a 5-day period at TRI (November 16-20, 2009). The test followed a 1-week "burn-in" period so that airport personnel had become adept in using the CyberLock system.

4.2 Critical Operation Issues

Data collection addressed the following Critical Operational Issue (COI) presented in Table 9.

[redacted]

[redacted]

Table 9. Critical Operational Issue, Measures, and Tasks

COI: Does the CyberLock system provide an increased level of security that meets or exceeds the facility's current perimeter requirements?		
Measure	**Task**	
1 Integration	A	Document the CyberLock system requirements for integration
	B	Document operational or maintenance procedures
2 Operation	A	Document success rate of access/rejection rights feature
	B	Document success rate of scheduling feature
	C	Record process times required to program mechanisms
	D	Document reprogramming requirements in event of a compromised key or lock
3 Reporting	A	Document accuracy of the access event recording capability
4 Cost Benefit	A	Document any cost-benefits of the CyberLock solution

To evaluate the effectiveness of the access/rejection rights program, Safe Skies designated 21 CyberKeys as test keys on perimeter locks using a "pass/fail" approach. To assure that sufficient data was collected, 12 gates and 2 doors were programmed for each sample key. Multiple "rounds" to gain access with the test keys were conducted daily on available locks. Each test key was programmed to allow access 8:00 am – 12:00 pm and deny access all other occasions. A perimeter zone description identifying test gate/door locations is provided in Appendix A of this report.

In order to evaluate the accuracy of system records, events from each key were downloaded and audited (e.g. lock ID, date and time of attempt, event). The downloaded data was assessed in conjunction with the actual access attempt times at each gate and door.

5. RESULTS

The following data collection efforts devised to evaluate the COI and measure system performance and other characteristics were conducted at TRI.

5.1 Integration (COI: 1A and 1B)

Implementation and integration tasks identified in COI: 1A and 1B are addressed in Section 3 (System/Process Description) of this report. An itemized list of equipment and incurred cost is displayed in Appendix B. Locally, product installation was performed by airport employees.

[redacted]

[redacted]

5.2 Operational Success Rates (COI: 2A and B)

Tables 10 and 11 display the pass/fail results of CyberKeys programmed to allow access to 11 gates and 2 doors, respectively. [redacted]

Table 10. Pass/Fail Results – CyberKeys Programmed to Allow Access to Gates

Gate	Access Allowed (Pass)	Access Denied (Fail)	Percent Passed	95% Confidence Interval	Mech. Resist
[redacted]					

CIs for rate statistics, including those in Table 10 above, are calculated using the Clopper-Pearson method of calculating CIs (Fleiss, 2003, 26). The CIs can be considered a range of values with a stated percentage (in this case, 95%) representing the proportion of CIs that could be expected to contain the true value. For example, if the true passing percent for CyberKeys programmed to allow access on [redacted] was, in fact, [redacted] we would expect 95% of all CIs for samples of data taken under similar conditions to contain the true median value of [redacted] In the case of the median on [redacted] for example, the CI bounds indicate that, with 95% confidence, we can narrow our estimate's CI to a range of [91.6%, 100.0%], a width of 8.4%.

[redacted]

[redacted]

Table 11. Pass/Fail Results – CyberKeys Programmed to Allow Access to Doors

Door	Activity	Access Allowed (Pass)	Access Denied (Fail)	Percent Passed	95% Confidence Interval	Mech. Resist
Door 1	[redacted]					
Door 2						
Total						

A detailed account of total attempts by individual test key for each gate/door is presented in Appendix C. A detail account of mechanical resistance by test key for each gate/door is also provided.

Tables 12 and 13 display the pass/fail results of CyberKeys programmed to deny access to 12 gates and 2 doors, respectively. [redacted]

Table 12. Pass/Fail Results – CyberKeys Programmed to Deny Access to Gates

Gate	Access Denied (Pass)	Access Allowed (Fail)	Percent Passed	95% Confidence Interval
[redacted]				

[redacted]

[redacted]

Table 13. Pass/Fail Results – CyberKeys Programmed to Deny Access to Doors

Door	Access Denied (Pass)	Access Allowed (Fail)	Percent Passed	95% Confidence Interval
Door 1	[redacted]			
Door 2				
Total				

A detailed account of total access denied attempts by individual test key for each gate/door is provided in Appendix C.

5.3 Scheduling and Access Event Recording (COI: 2B and 3A)

In order to evaluate the accuracy of the system records, the access events from each key were downloaded and a sample of access events audited. Data downloaded from the CyberKeys was assessed in conjunction with the actual times of the access attempts at each gate and door. A "pass" occurred when data from the CyberLock reporting system (e.g. lock ID, date and time of attempt, and event) matched the data recorded by testing personnel for the attempt.

Table 14 displays the results of a time audit conducted on gate access attempts. All locks and test keys were included in the time audit sampling evaluation. The system performed to a 100% success rate on scheduling and recording accuracy.

Table 14. Time Audit Results – CyberLock Gates and Doors

Date	Number Samples	Passed Time Audit	95% Confidence Interval
11/16/2009	21	100%	[83.9%, 100.0%]
11/17/2009	30	100%	[88.4%, 100.0%]
11/18/2009	29	100%	[88.1%, 100.0%]
11/19/2009	24	100%	[85.8%, 100.0%]
Total	104	100%	[96.5%, 100.0%]

Appendix D contains daily time audit journals identifying gate, test key, time of attempt and audit result.

Figure 11 displays a CyberAudit report, which was developed for TRI[redacted]

[redacted]

[redacted]

Safe Skies Test Keys

11/20/09 7:35 AM

Eastern time (US+Canada)

10 Events

Person	Lock	Event	Date	Source	Download Date	
Test Key 12	[redacted]		10:32:46 AM	key	11/19/2009	2:59:55 PM
Test Key 17			10:30:50 AM	key	11/20/2009	7:03:37 AM
Test Key 12			7:43:08 AM	key	11/19/2009	2:59:55 PM
Test Key 17			7:40:30 AM	key	11/20/2009	7:03:37 AM
Test Key 17			7:51:06 AM	key	11/20/2009	7:03:37 AM
Test Key 12			7:47:24 AM	key	11/19/2009	2:59:55 PM
Test Key 17			2:41:06 PM	key	11/20/2009	7:03:37 AM
Test Key 12			2:38:00 PM	key	11/19/2009	2:59:55 PM
Test Key 17			11:39:02 AM	key	11/20/2009	7:03:37 AM
Test Key 12			11:37:12 AM	key	11/19/2009	2:59:55 PM

Figure 11. CyberAudit Report - [redacted]

Figure 12 displays a CyberAudit report developed for Test Key #12.

[redacted]

[redacted]

Safe Skies Test Keys

11/19/2009 14:59

Eastern time (US+Canada)

27 Events

Person	Lock	Event	Date	Source	Download Date	
Test Key 12	[redacted]		12:00:06 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:54:42 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:39:44 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:12:24 AM	key	11/19/2009	2:59:55 PM
Test Key 12			10:43:48 AM	key	11/19/2009	2:59:55 PM
Test Key 12			10:32:46 AM	key	11/19/2009	2:59:55 PM
Test Key 12			10:13:06 AM	key	11/19/2009	2:59:55 PM
Test Key 12			9:59:54 AM	key	11/19/2009	2:59:55 PM
Test Key 12			9:44:18 AM	key	11/19/2009	2:59:55 PM
Test Key 12			9:24:22 AM	key	11/19/2009	2:59:55 PM
Test Key 12			8:53:58 AM	key	11/19/2009	2:59:55 PM
Test Key 12			8:10:42 AM	key	11/19/2009	2:59:55 PM
Test Key 12			12:00:06 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:53:22 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:43:50 AM	key	11/19/2009	2:59:55 PM
Test Key 12			11:29:30 AM	key	11/19/2009	2:59:55 PM
Test Key 12			10:31:54 AM	key	11/19/2009	2:59:55 PM
Test Key 12			10:16:56 AM	key	11/19/2009	2:59:55 PM
Test Key 12			9:44:06 AM	key	11/19/2009	2:59:55 PM
Test Key 12			8:49:54 AM	key	11/19/2009	2:59:55 PM
Test Key 12			8:38:58 AM	key	11/19/2009	2:59:55 PM
Test Key 12			8:19:42 AM	key	11/19/2009	2:59:55 PM
Test Key 12			2:00:06 AM	key	11/19/2009	2:59:55 PM
Test Key 12			2:19:38 PM	key	11/19/2009	2:59:55 PM
Test Key 12			1:55:50 AM	key	11/19/2009	2:59:55 PM
Test Key 12			1:37:12 AM	key	11/19/2009	2:59:55 PM
Test Key 12			1:19:22 AM	key	11/19/2009	2:59:55 PM

Figure 12. CyberAudit Report – Test Key #12

Explanations of audit event nomenclature of the CyberLock reporting system are provided in Appendix E.

[redacted]

[redacted]

5.4 Process Times (COI: 2C)

The period to set up and program the test access schedule within the CyberLock system for 21 keys and 14 locks was observed to be approximately 8 min. The programming time for an individual key was collected for 11 of the 21 keys used in testing. The median time to program these keys was 1 min 35 sec, with observed times ranging from 1 min 7 sec to 4 min 4 sec. The time to refresh a key's programming was collected in 4 instances. The refresh time for these 4 keys ranged from 22 sec to 32 seconds.

5.5 Reprogramming Requirements and Cost Benefits (COI: 2D and 4A)

Under the CyberLock system, the loss of a master key would require one person to reprogram a single key, which would take approximately 15 min, and then reprogram the individual locks in the field. The total time required to reprogram the locks in the field is directly dependent on the number of locks and their locations. The estimated labor to reprogram all 18 locks at TRI is approximately 3 hrs. The CyberLock system can be electronically refreshed instead of being replaced, which eliminates the need for new hardware in the case of lost keys or the institution of service contracts for maintenance needs. Reprogramming the perimeter locks at TRI requires the labor of a single person to complete the task.

Table 15 shows a hypothetical scenario comparison between the CyberLock system and the traditional lock and key system at TRI. The estimates were developed by TRI and Safe Skies and are included to demonstrate possible cost benefits of the system.

[redacted]

[redacted]

Table 15. Hypothetical Comparison Between Traditional Lock and CyberLock Systems

Hypothetical Scenario: *An airport security vehicle is vandalized and a master key is stolen. The key allows access to 18 locks in the facility; 90 employees hold keys to the facility.*		
	Traditional Lock & Key System	**CyberLock System**
Consequences	• Security operations is informed that a Master Key is stolen • Estimates are called in to purchase new cores for 13 gate and 5 door locks **$55 per core** • Purchase new keys for 90 people **$1.00 per key** • Assume contractor or union costs to perform labor **$27 per hr** • Assume 30 min time to re-core a lock and move to next location **9 hours** • Labor for one person to reissue new keys **9 hours**	• Security operations is informed that a master CyberKey is stolen • Security operations programs a new master key • The programmer key is updated with the newest security information • The security operations staff physically reprograms each lock with a Programmer Key • Assume comparable costs to perform labor **$27 per hr** • Total time to complete all events listed above **3 hours, 15 min**
Total Time	3-4 days	1 day
Total Cost	$1,566	$88

6. OBSERVATION/RECOMMENDATIONS

From the data presented in this report, it is clear that the CyberLock system had a positive effect on the TRI perimeter security efforts [redacted] The system performed to a 100% success rate on scheduling and recording accuracy (time audits).

Reviews from daily users were positive, with the exception of the CyberKey being larger than traditional keys. No operational troubles were indicated by the officers or contract personal interviewed.

[redacted]

Reviews of the systems administrative functions were positive. The system allows administrative personnel to investigate key and lock activity through data filtering options. Complete audit reviews were possible within minutes and could be arranged according to individual people, groups, locks, dates, or specific time ranges. Efficient use of the system requires that at least one person, preferably an airport security professional, become exceptionally familiar with the menus and options. Comments received from TRI personnel describe the software as both functional and user-friendly.

7. REFERENCES

Fleiss, J.L. (2003). Statistical *Methods for Rates and Proportions* (3rd ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

[redacted]

APPENDIX A - TRI PERIMETER ZONE DESCRIPTION

[redacted]

[redacted]

Tri-Cities Regional Airport (TRI), located in Blountville, Tennessee, is designated as a CAT III airport by the FAA. TRI has over 1,000 acres of property inside the perimeter fence. There are approximately 30 Air Operations Area access points. TRI's property covers approximately 1,225 acres, including an 118,835 square-ft. terminal with 7 aircraft gates, an Air Cargo Logistics Center, and corporate hangars. There are 8 conventional hangars ranging in size from 8,000 to 28,000 sq. ft. The primary runway is 8,000 by 150 feet and contains both Category I and II Instrument Landing Systems.

TRI serves Northeast Tennessee, Southwest Virginia, Western North Carolina, and Eastern Kentucky.

CyberLock® test positions are displayed in Figures 13 and 14.

[redacted]

[redacted]

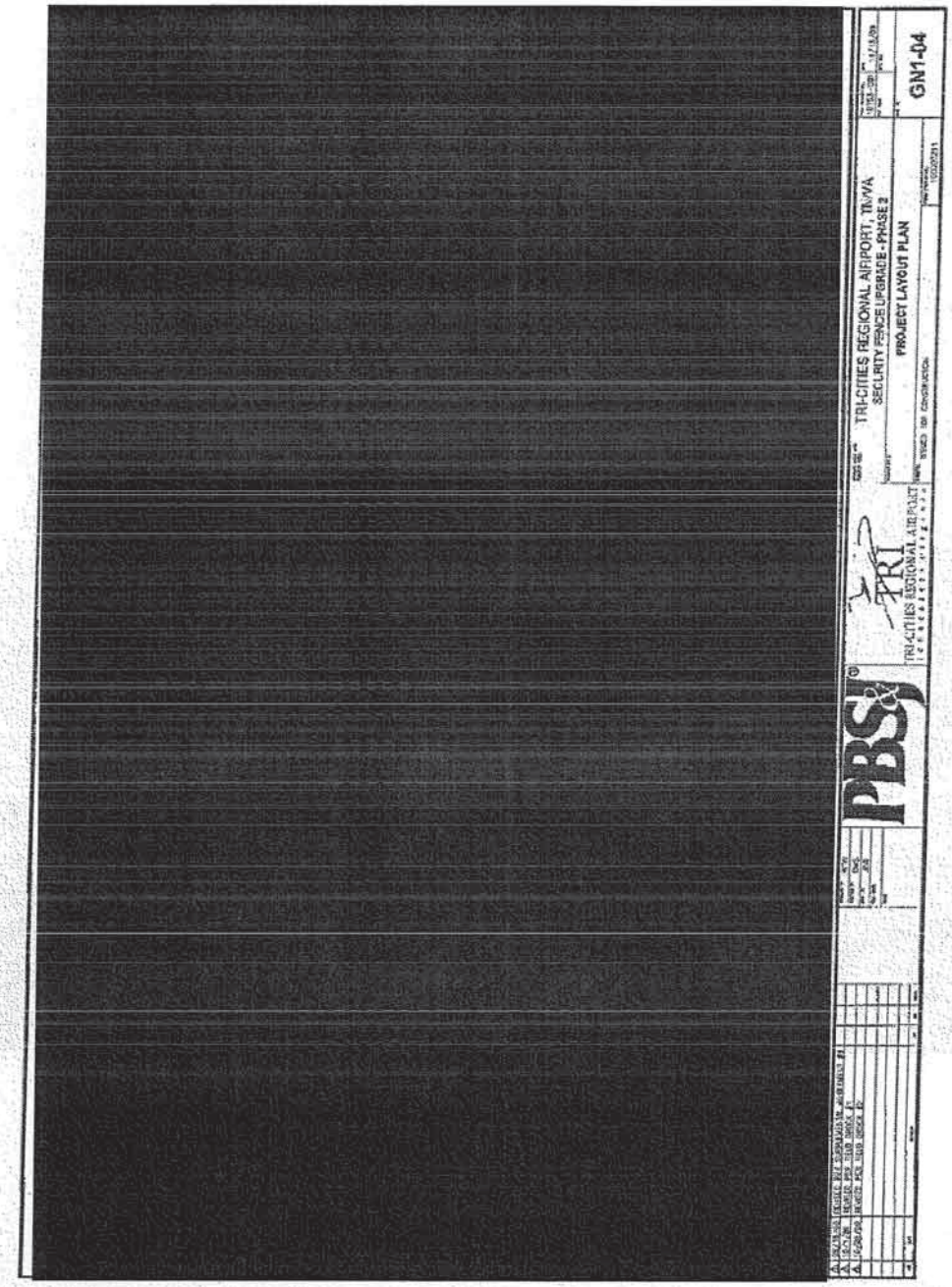

Figure 13. CyberLock Test Positions – TRI Project Layout Plan

[redacted]

[redacted]

Figure 14. CyberLock Test Positions – TRI Aerial View

[redacted]

[redacted]

APPENDIX B - PROJECT COSTS

[redacted]

[redacted]

Table 16 presents an itemized list of equipment and incurred cost for the CyberLock® system in TRI.

Table 16. Equipment and Installation Costs

Item	Quantity	Price Each	Total
PL-02 CyberLock Padlocks	25	$199.00	$4,975.00
CK-IR6 CyberKeys	160	$98.00	$15,680.00
BRUSH Lock & Key pin cleaning brushes for key ring	20	$5.00	$100.00
CyberAudit Web Pro Software Starter Kit	1	$1,237.00	$1,237.00
Double Keyed Deadbolts	3	$390.00	$1,170.00
Single Keyed Deadbolts	1	$225.00	$225.00
CyberLock CL-M2 (TCA Ramp Door) Ruswin keyed both sides	2	$187.00	$374.00
Grade 1 knob including CyberLock cylinder	1	$275.00	$275.00
Replacement tips TIP-001	20	$7.50	$150.00
Batteries	50	$5.00	$250.00
Freight	1	$45.00	$45.00
Interior door cylinder	1	$200.00	$200.00
Dell Computer and monitor	1	$1,950.00	$1,950.00
Misc. Hardware for Lock Replacements	1	$250.00	$250.00
Installation by Airport Personnel (days)	5	$240.00	$1,200.00
Locksmith fees	1	$500.00	$500.00
Canon Printer Pixma MX 850	1	$205.00	$205.00
Printer Cable	1	$30.00	$30.00
CyberKey® Web Authorizer Hub	1	$595.00	$595.00
CyberKey Authorizer Keyport	1	$595.00	$595.00
Total			**$29,806.00**

[redacted]

[redacted]

APPENDIX C – TEST CORRELATION AND ATTEMPTS DATA

[redacted]

[redacted]

Table 17 displays the CyberKey® serial numbers for each test key.

Table 17. Test Key and Serial Number Correlation

Test Key Number	CyberKey Serial Number
1	K60003F38
2	K60003F24
3	K60003F56
4	K60003FC4
5	K60003F47
6	K60003FCE
7	K60003F3D
8	K60003F52
9	K60003FD4
10	K60004109
11	K60003FD3
12	K60003FC3
13	K60003FD6
14	K60003FC4
15	K60003FCF
16	K60003FCC
17	K60003F57
18	K60003F34
19	K60003F1B
20	K60003F23
21	K60003F5F

Table 18 displays the lock assigned to each gate.

[redacted]

[redacted]

Table 18. Gate and Lock Assignments

Gate	CyberLock Serial Number
[redacted]	L49F616C7
	L49F616BC
	-
	-
	L49F61671
	-
	L49F616F9
	-
	L49F616FE
	L49F616EF
	L49F6167B
	L49F616E0

Safe Skies recorded the CyberLock serial numbers from stickers located on the actual locks. In some cases, the stickers were missing due to weather or deterioration from user activities. No identification stickers were available on the doors.

Tables 19 – 22 display additional data results referenced in the report. These tables do not include instances of mechanical resistance. A count of mechanical resistance occurrences for all locks/keys can be seen in Tables 23-24. Each instance of mechanical resistance was followed by a successful attempt.

[redacted]

Table 19. Total Attempts by Gate – CyberKeys Programmed to Allow Access

Table 20. Total Attempts by Door – CyberKeys Programmed to Allow Access

Table 21. Total Attempts by Gate – CyberKeys Programmed to Deny Access

[redacted]

[redacted]

Tables 23-24 present the total mechanical resists by gate by each CyberKey. The percentage of resist as compared to total successful attempts is also displayed.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Table 24. Total Mechanical Resists by Door Lock by CyberKeys

[redacted]

[redacted]

[redacted]

APPENDIX D – TEST KEY TIME AUDIT JOURNALS

[redacted]

[redacted]

Tables 25 – 28 display a chronicle and results of the time audit.

Table 25. Time Audit Journal – November 16, 2009

Time Start	Time Finish	Gate	Prog. Status	Test Key Number	Audit Result
11:10	11:20	[redacted]			Passed
11:30	11:45				Passed
11:50	12:00				Passed
12:00	12:21				Passed
12:40	12:47				Passed
12:50	13:00				Passed
13:04	13:08				Passed
13:20	13:30				Passed
14:15	14:20				Passed
14:35	14:44				Passed
14:47	14:54				Passed
15:00	15:05				Passed
15:09	15:14				Passed
15:20	15:25				Passed

[redacted]

[redacted]

Table 26. Time Audit Journal – November 17, 2009

Time Start	Time Finish	Gate	Prog Status	Test Key Number	Audit Result
8:10	8:20	[redacted]			Passed
8:30	8:41				Passed
8:50	8:58				Passed
9:07	9:15				Passed
9:23	9:30				Passed
9:38	9:51				Passed
9:56	10:05				Passed
10:11	10:20				Passed
10:29	10:35				Passed
11:25	11:34				Passed
11:37	11:45				Passed
11:49	11:58				Passed
7:47	7:53				Passed
12:05	12:13				Passed
12:20	12:25				Passed
12:38	12:45				Passed
12:50	13:00				Passed
13:10	13:15				Passed
13:30	13:36				Passed
13:50	13:57				Passed
14:05	14:11				Passed
14:15	14:23				Passed
14:30	14:35				Passed

[redacted]

[redacted]

Table 27. Time Audit Journal – November 18, 2009

Time Start	Time Finish	Gate	Prog Status	Test Key Number	Audit Result
8:06	8:13	[redacted]			Passed
8:17	8:25				Passed
8:35	8:41				Passed
8:50	8:58				Passed
9:08	9:15				Passed
9:20	9:28				Passed
9:30	9:39				Passed
9:44	9:50				Passed
9:55	10:02				Passed
10:11	10:18				Passed
10:28	10:36				Passed
10:42	10:50				Passed
11:07	11:14				Passed
11:25	11:32				Passed
11:40	11:47				Passed
11:50	11:57				Passed
7:40	7:46				Passed
7:50	7:56				Passed
12:05	12:11				Passed
14:05	14:15				Passed
14:25	14:31				Passed
14:40	14:46				Passed
14:55	15:01				Passed
15:05	15:12				Passed
15:16	15:24				Passed
15:30	15:35				Passed
15:50	15:56				Passed

[redacted]

[redacted]

Table 28. Time Audit Journal – November 19, 2009

Time Start	Time Finish	Door	Prog Status	Test Key Number	Audit Result
9:00	9:05	[redacted]			Passed
9:06	9:15				Passed
9:32	9:39				Passed
9:48	9:55				Passed
9:57	10:06				Passed
10:10	10:17				Passed
10:20	10:28				Passed
10:30	10:36				Passed
10:40	10:49				Passed
10:51	10:58				Passed
11:10	11:19				Passed
11:22	11:40				Passed
12:55	1:07				Passed
12:55	1:07				Passed
13:09	13:18				Passed
13:09	13:18				Passed
13:20	13:30				Passed
13:20	13:30				Passed
13:35	13:44				Passed
13:35	13:44				Passed
13:50	13:59				Passed
13:50	13:59				Passed
14:10	14:19				Passed
14:10	14:19				Passed

It should be noted that in Table 28, the programmed to reject data for Doors 1 and 2 was collected within the same assigned 9-to 10-minute blocks of time.

[redacted]

APPENDIX E - AUDIT TRAIL EVENTS AND DEFINITIONS

Tables 29 – 30 display the audit trail events and definitions within the CyberAudit system. The events and definitions apply to CyberKeys® and CyberLocks® manufactured after October 2008.

Table 29. Audit Trail Events for CyberKey System

Audit Trail Events from CyberKeys (Applies to CyberKeys manufactured after October 2008)	
CyberPoint Contact	Contact with a CyberPoint or contact with a lock using a CyberPoint schedule.
Software reset	A reset of the key at the factory during manufacture or service. Lock column contains voltage data from battery and capacitor.
Low Battery	The key discovered its battery was below threshold during one of its periodic reads or during a lock opening, the key emitted a low tone beep once every eight seconds for one minute. Lock column contains voltage data from battery and capacitor.
Dead Battery	The battery voltage dropped below operation voltage during one of its periodic reads or during a lock opening. If the read was during a lock opening, the key emitted a single high tone beep followed by a low tone beep once every eight seconds for one minute. Lock column contains voltage data from battery and capacitor.
E2 Access	Failure to read memory.
Scheduled Battery Reading	The key reads and records its battery level daily, after midnight local time Lock column contains voltage data from battery and capacitor.
Write Event Failed	Failure to write to memory.
Power restored	When the key comes up from low or no voltage, the processor starts and triggers this event.
Reset	For keys manufactured after October 2008 this is a non-power related CPU reset. For keys manufactured before that time it is a general reset that applies to all the categories shown above.
Multi-key access key 1	The first key for multi-key access was accepted by the lock.
Multi-key access key 2	The second key for multi-key access was accepted by the lock.
Multi-key access key 3	The third key for multi-key access was accepted by the lock.
Multi-key access key 4	The fourth key for multi-key access was accepted by the lock.
Authorized to open	*
Master key authorized	*
Authorized to open (bypass multikey)	Lock has a multi-key setting bypassed from instruction in schedule.
Authorized to open (bypass delay)	Lock has a delay setting bypassed from instruction in schedule.

Authorized to open (b)	Lock had no multi-key or delay setting when key was configured. Key was configured to bypass multi-key or delay for this lock.
Programmer or CyberPoint contact	Programmer contact or contact with lock using a CyberPoint schedule. Key beeped 3 times.
Lock reset attempted	Reset keys only
Unprogrammed lock - authorized	If a key is operating within its key schedule (i.e. not expired) and if the key is not disabled, it is automatically authorized to open a lock that is not programmed.
No lock ID-authorized	This event should never occur. It indicates that the lock was not set up with an ID. It cannot be programmed and will not function in a CyberAudit system.
Key in lock more than 1 minute or removed from lock	Keys in a subsystem may be configured to report all "removed from lock" events. The message text will depend on this setting.
Access code failed	This message will occur if: • A lock contains different access codes than expected by the database because it has been moved to or from a different database. • The lock has been updated with new access codes but the key has not. • The lock does not contain the access code that a master key is programmed to use.
Key disabled	The key has been disabled either by: 1. The lock because the key was designated as "lost" and the lock was designated as a disabling point or 2. Disabled when updating and removed from the communicator before updating was complete.
Hardware mismatch – access denied	This event should never occur. it indicates manufacturing difference between lock and key.
Out of schedule for lock	The key found the lock ID in its lock list but the time of contact with the lick was not during the scheduled operating time. • The time frame did not match the current time • The day did not match the current day • It is before the schedule is to begin • The schedule has expired
Key expired or out of schedule	If it is a master key, it could generate this event if: * The key schedule time frame did not match the current day * The key schedule day did not match the current day * It is before the key is to begin operating * The key has expired

[redacted]

Access Denied – No Permissions	*
Clock stopped	This is a special "out of schedule" condition. All keys except system reset keys and unscheduled system master keys will stop working if their clock stops.
Access count expended	Applies to one-time access and fixed-used countdown schedules.

* This symbol was produced by the software in certain cells—the meaning is unknown.

[redacted]

[redacted]

Table 30. Audit Trail Events for CyberLocks

Audit Trail Events from CyberLocks	
Multi-key access key 1	The first key for multi-key access was accepted by the lock.
Multi-key access key 2	The second key for multi-key access was accepted by the lock.
Multi-key access key 3	The third key for multi-key access was accepted by the lock.
Multi-key access key 4	The fourth key for multi-key access was accepted by the lock.
Authorized to open/td	*
Authorized to open (b)	The key was granted access and no multi-key or delay lock setting was found.
Authorized to open (bypass multikey)	Lock had a multi-key setting which the key bypassed from an instruction in the schedule corresponding to the lock
Authorized to open (bypass delay)	Lock had a delay setting which the key bypassed from an instruction in the schedule corresponding to the lock
Master key authorized	*
Programmer or CyberPoint contact	Programmer contact or contact with lock using a CyberPoint schedule. Key beeped 3 times.
Lock reset successful	System reset keys only – if a reset key gains access but does not successfully reset the lock, the lock will record a "Master key authorized" event.
Unprogrammed lock – authorized	*
No lock ID – authorized	This event should never occur. It indicates that the lock was not set up with an ID. It cannot be programmed and will not function in a CyberAudit-Wed system.
Access denied	The lock reports this event when it receives a "bad access code." Keys in a subsystem may be set to generate "no access" events in locks they are not permitted to open. In those cases where access is denied, they send a "bad access code" to the lock to generate this event.
Key disabled	The key has been disabled by the lock because the key was designated as "lost" and the lock was designated as a disabling point.
Hardware mismatch – access denied	This event should never occur. It indicates manufacturing difference between lock and key.

[redacted]