



**Transportation
Security
Administration**

Office of Security Technology

Airport Perimeter Security Projects for FY06

FINAL REPORT

Pittsburgh International Airport (PIT)

Videx, Inc. CyberLock System

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

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

[REDACTED] the airport installed the CyberLock System, a series of electronic locks that require specific programmable keys to allow access. PIT's expectations were that the system had the capacity to work in remote areas where power and communication infrastructure do not exist, exhibit durability and easy operation, allow flexible programming for key assignments, provide access history activity, and be maintainable and usable by airport personnel.

[REDACTED]

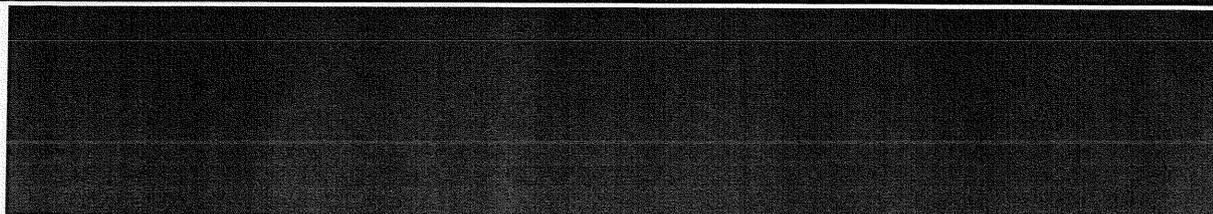
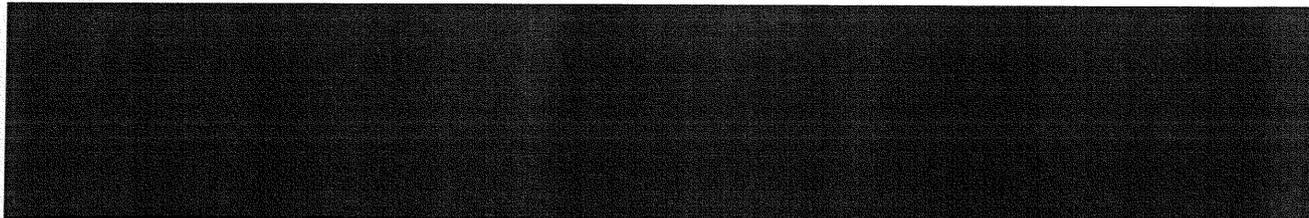
This project pertained to the evaluation of the CyberLock electronic access control solution, which is a proprietary product of Videx, Incorporated of Corvallis, Oregon. This innovative locking system converts existing mechanical cylinder locks into an access control system. The combination of electronic 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 security enhancement solution for outer-perimeter vehicle and pedestrian gates for access control.

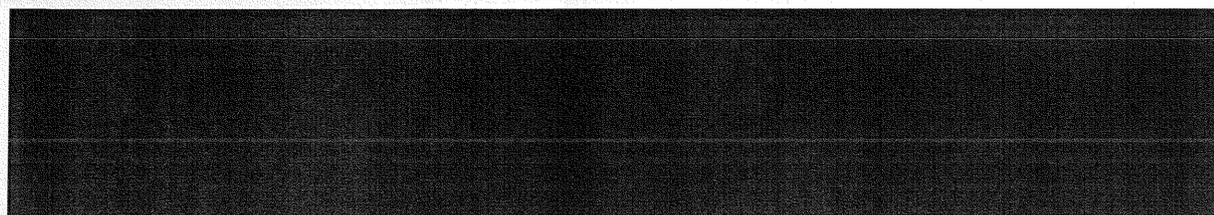
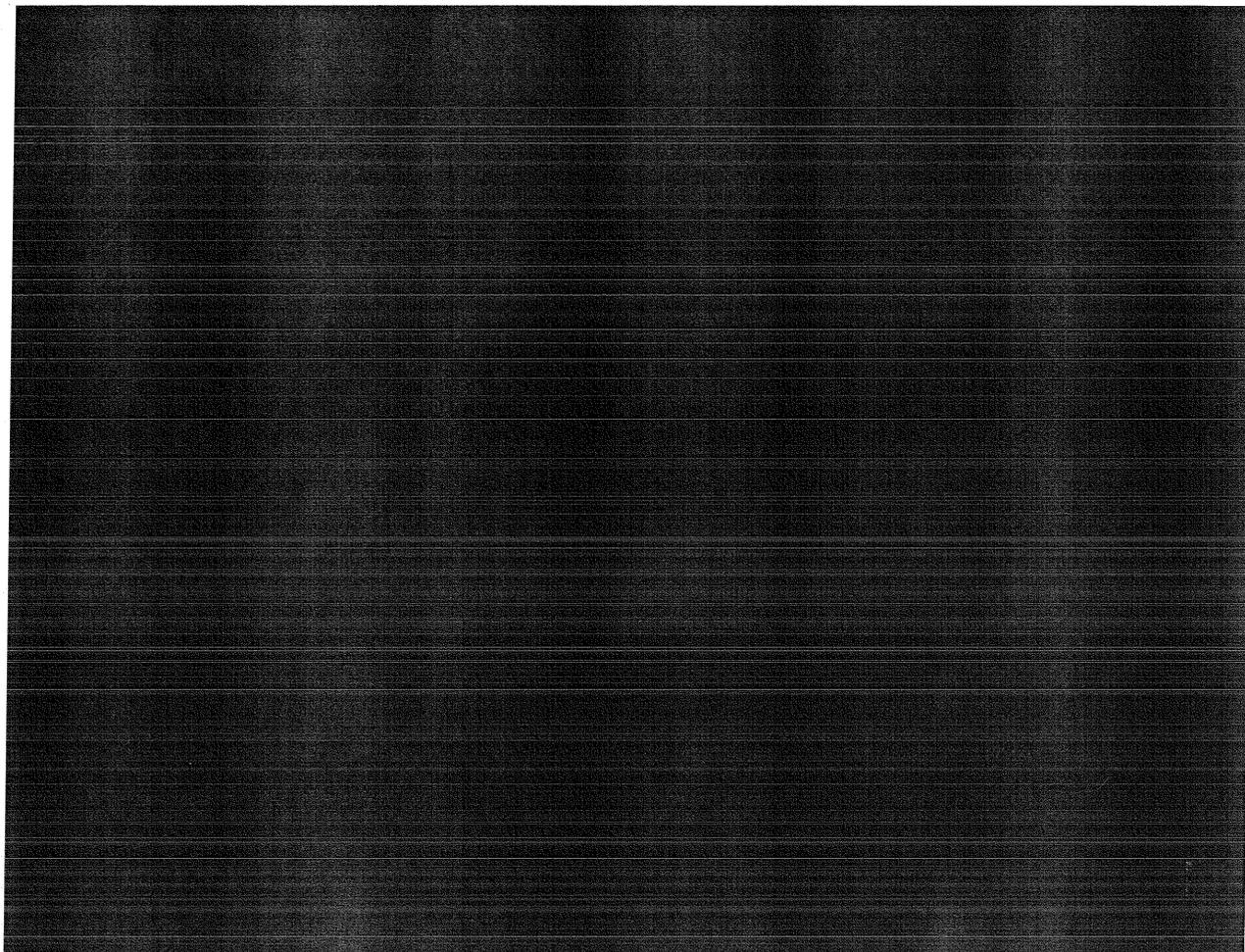
National Safe Skies Alliance (Safe Skies) provided independent verification and validation (IV&V) services and operated along with airport authorities to verify that the CyberLock system enhancements met the airport's security expectations. The IV&V was concluded December 10, 2008.

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 (approximately 5 minutes). 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 150 locks at PIT is approximately 16 hours for one person. 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 PIT 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.

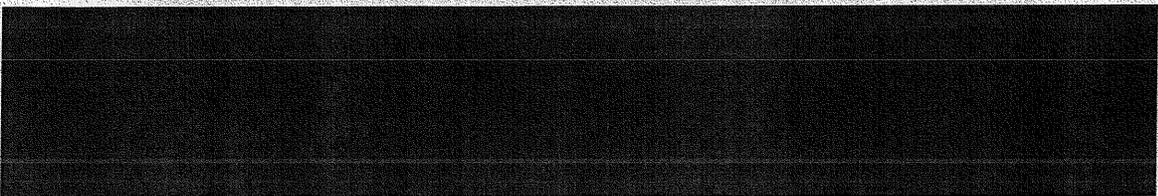
SUMMARY







<p>DHS/TSA 2600.02.01.09-014</p>	<h2>Pittsburgh International Airport: Videx, Inc. CyberLock[®] System Operational Evaluation Report</h2> <p>COPYRIGHT © 2009 National Safe Skies Alliance, Inc. ALL RIGHTS RESERVED</p>	
	<p><u>Project Performed by:</u> National Safe Skies Alliance 110 McGhee Tyson Boulevard Suite 201 Alcoa, TN 37701</p>	<p><u>Safe Skies Author(s)</u> John Hunsucker Jeff Vanvactor</p>
	<p><u>Project Performed for and Funded by:</u> U.S. Dept. of Homeland Security Transportation Security Administration 601 S. 12th Street Mail Stop TSA-16 Arlington, VA 22209</p>	<p><u>TSA Technical Review Team</u> Charles Kelley John Nestor</p>
<p>January 2009</p> <p>Final Report</p>		





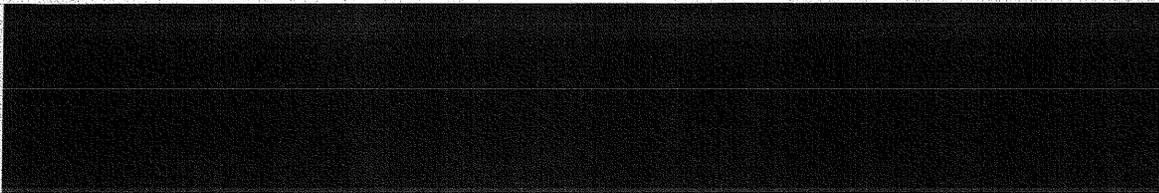
NOTICE

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 © 2009 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.



Technical Report Documentation Page

1. Report No. DHS/TSA—09-014		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Pittsburgh International Airport: Videx, Inc. CyberLock® System Operational Evaluation				5. Report Date January 2009	
				6. Performing Organization Code	
7. Author(s) John Hunsucker, Jeff Vanvactor				8. Performing Organization Report No. DHS/TSA—2600.02.01.09-014	
9. TSA Reviewer(s) Charles Kelley, John Nestor				10. Work Unit No. (TRAIS)	
11. Performing Organization Name and Address National Safe Skies Alliance 110 McGhee Tyson Blvd Suite 201 Alcoa, TN 37701				12. Contract or Grant No. 00-G-019	
				13. Type of Report and Period Covered Final Report, January – December 2008	
14. Sponsoring Agency Name and Address U.S. Department of Homeland Security Transportation Security Administration 601 S. 12 th Street Mail Stop TSA-16 Arlington, VA 22209				15. Sponsoring Agency Code TSA-16	
16. Supplementary Notes This report was prepared by John Hunsucker of National Safe Skies Alliance					
17. Abstract This report documents the results of lab and field testing of the CyberLock System, produced by Videx, Inc., and its functionality as a tool to enhance the perimeter security at PIT. National Safe Skies Alliance performed testing January 21 – February 25, 2008 and December 8 -10, 2008. Testing of this system was made possible through funding and resources allotted from the TSA Airport Perimeter Security program. The statements included in this document are in reference to the Critical Issues that were approved in the project's Final Test Plan (DHS/TSA 2600.02.01.07-206, November 2007).					
18. Key Words Access Control CyberKey, CyberLock, Enhancement, Gate, Infrastructure, Perimeter, PIT, Remote, Security,					
19. Security Classif. (of this report) SSI/FOUO		20. Security Classif. (of this page) Unclassified		21. No. of Pages 27	
				22. Price	

Reproduction of completed page authorized



DOCUMENT CHANGE HISTORY

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

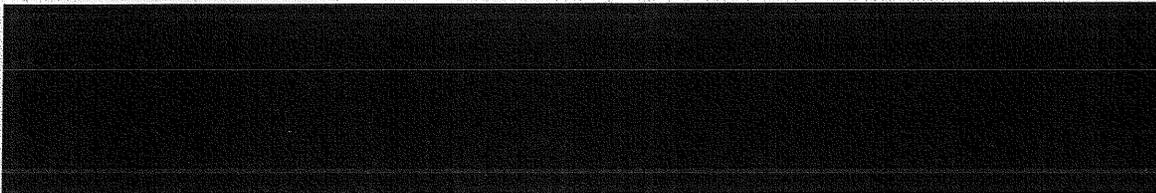




TABLE OF CONTENTS

	Page
1. INTRODUCTION	2
1.1 Background	2
1.2 Purpose of Document	2
2. SCOPE	2
2.1 Objective	2
3. SYSTEM DESCRIPTION	2
3.1 System Overview	2
3.2 Installation	3
4. METHODOLOGY	4
4.1 Sites and Schedule	4
4.2 Equipment	4
4.3 Critical Issues	4
5. RESULTS	5
5.1 Measure 1: Integration Effectiveness	5
5.2 Measure 2: Impact on Existing Access Control Operations	8
5.3 Measure 3: Programming Verification	11
5.4 Measure 4: CyberLock and CyberKey Susceptibilities	13
5.5 Summary	16
6. REFERENCES	17

LIST OF TABLES

Table 1. Installation and Use Issues	7
Table 2. Estimated Time to Program Devices	8
Table 3. Audit Report Functionality Results	12
	14
	16

LIST OF FIGURES

Figure 1. 	3
Figure 2. 	4
Figure 3. CyberLock® System	A-1



[REDACTED]

EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) established the Airport Perimeter Security Program (APS) to support the expansion and implementation of security technology at the perimeters of United States airports. Through this program, commercial off the shelf (COTS) technologies are incorporated into an airport's security network to enhance the overall perimeter security infrastructure. Pittsburgh International Airport (PIT) determined that the most

[REDACTED]

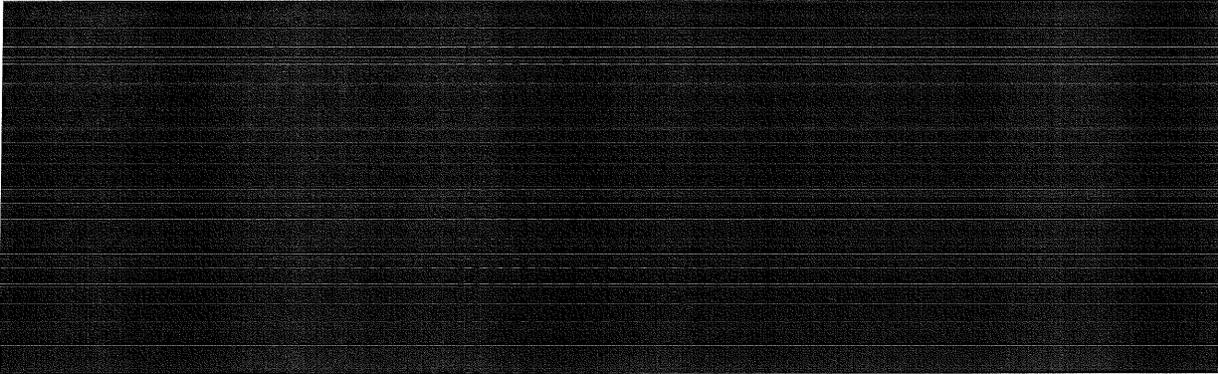
Airport expectations were that the CyberLock system:

- Have the capacity to operate in remote areas absent of power and communication infrastructure
- Exhibit durability and easy operation
- Allow flexible programming for key assignments
- Provide access history activity and activity updates
- Remain maintainable, usable, and economical by airport personnel

As part of the APS program requirements, National Safe Skies Alliance (Safe Skies) conducted third-party evaluations of the system, both in-house laboratory and operationally in the field at PIT. The data collected for this assessment was generated at the Safe Skies testing facility from January 21 – February 25, 2008, and operationally at PIT December 8 – 10, 2008. The in-house laboratory test procedures were designed to determine the responsiveness of the system's programming, overall functionality, and potential susceptibilities to extreme hot and cold conditions. The field tests were designed to determine whether the system features were easily implemented by PIT personnel, and whether the system enhanced the existing perimeter access control infrastructure.

[REDACTED]

¹ The CyberLock system, a product of Videx, Inc., utilizes electronic locks and battery powered keys to create an access control system that can be implemented in a wide range of security applications.

Installation of the CyberLock system could prove to be cost-effective over traditional lock systems². Under the traditional system, PIT security estimates that 100% hardware replacement and processing could cost \$350,000 to \$500,000 plus hundreds of man-hours. Instances where 100% of the hardware must be replaced could occur if a master key were lost, stolen, or not returned due to employee termination; or, replacing or switching the locks every 2-3 years may be part of the airport security program. Additionally, replacing a traditional lock system could result in downtime throughout the airport. If the system initially cost \$350,000 for hardware, installation, keys, and man-hours it would cost approximately \$350,000 *per instance* to replace the system. This assumes that the hardware costs and labor contract costs do not increase, and does not take into account lost productivity.

Under the CyberLock system, the loss of a master key would require one person to reprogram a single key, which would take approximately 5 min, and then manually reprogramming the locks in the field. The time associated with reprogramming the locks in the field is directly dependent on the number of locks and their locations. With the current limited configuration at PIT, the estimated time to reprogram the locks is approximately 3-4 hrs. The CyberLock system, at an initial cost of \$60,000, can be electronically refreshed instead of being replaced. New hardware need not be installed or distributed and service contracts are not necessary. Reprogramming the locks requires the time of a single person to handle the task and the cost of one new CyberKey, if it is needed.

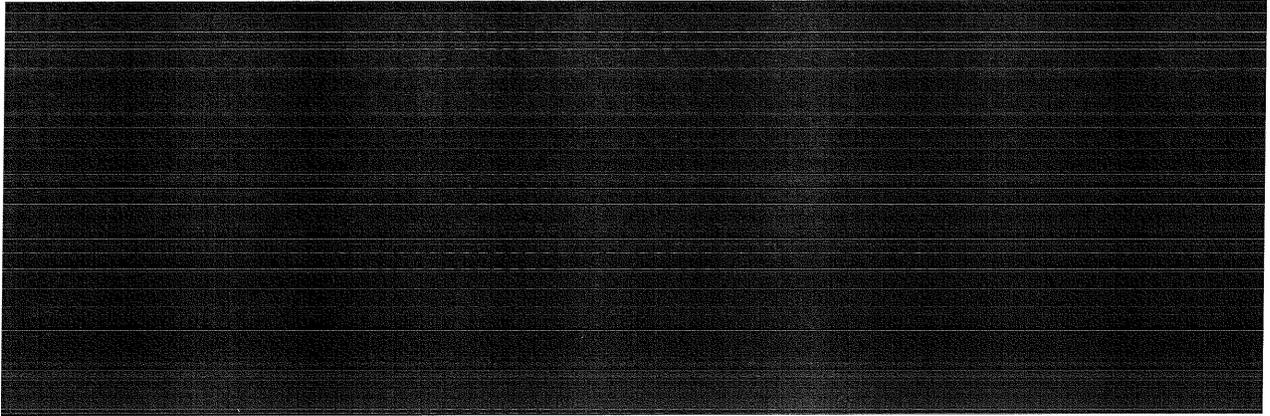
The following table shows a hypothetical comparison between the CyberLock system and the previous method at PIT. The numbers used are estimates provided by PIT. The initial cost of the PIT lock network is not immediately known, but is estimated at \$500,000. The initial cost of the CyberLock throughout the PIT lock network would be approximately \$900,000 – \$1,200,000 without any bulk discount.

² A “traditional” lock and key system uses a metallic key and lock with a mechanical tumbler that relies on the exact cut pattern on the key to allow or deny entry. The cost of the traditional key system comes from hardware and service contracts with certified locksmiths or security professionals.

Table 1. Hypothetical Comparison between Traditional Lock System and CyberLock System

Hypothetical Scenario: <i>The airport security director's vehicle is vandalized and the master key is stolen. The key allows access to 7,000 doors in the facility; 1,000 employees hold keys to the facility.</i>		
	Traditional Lock & Key System	CyberLock System
Consequences	<ul style="list-style-type: none"> • Director informs security operations that a Master Key is stolen • Estimates are called in to purchase new cores for approximately 7,000 locks \$55 per core • Estimates are called in to purchase new keys for 1,000 people \$1.40 per key • Assume contractor or union costs to perform labor \$25 per hr • Assume estimated time to re-core a lock and move to next location. 30 min • Assume 8-man team working 16 hrs a day 	<ul style="list-style-type: none"> • Director informs security operations that a master CyberKey is stolen • Security operations programs a new master key for the Director \$150 • The programmer keys 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 \$25 per hr • Assume estimated time to reprogram a lock and move to next location. 5 min • Assume 8-man team working 16 hrs a day
Total Time	26-29 days	4-5 days
Total Cost	\$450,000 – 500,000	\$10,000 – 20,000

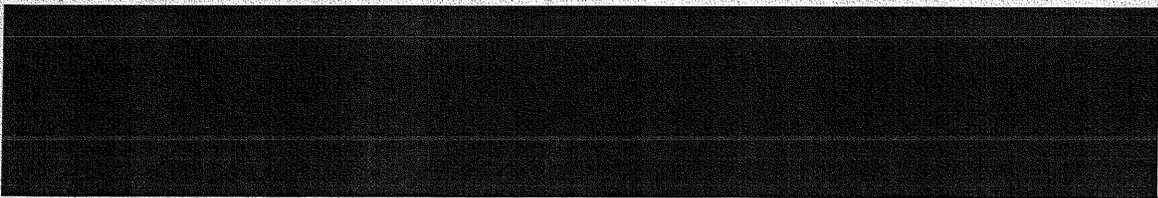
The initial cost of the CyberLock system is roughly twice that of the original system. In the event of a lost master key however, the value of the system becomes more apparent. The CyberLock System would require a fraction of the time and resources to have the entire facility secured. If this same event were to occur more than once in the lifetime of the traditional lock network, it would pay for the cost of the CyberLock system. Furthermore, the recurring maintenance cost of the traditional lock network would never approach the initial cost of the CyberLock system.





ACRONYMS

ACB&P	Access Control, Biometrics, and Perimeter
AOA	Air Operations Area
APS	Airport Perimeter Security
CI	Critical Issue
FAA	Federal Aviation Administration
LTE	Lead Test Engineer
MOE	Measure of Effectiveness
MOP	Measure of Performance
OT&E	Operational Testing and Evaluation
PIT	Pittsburgh International Airport – FAA designation
SIDA	Security Identification Display Area
TSA	Transportation Security Administration

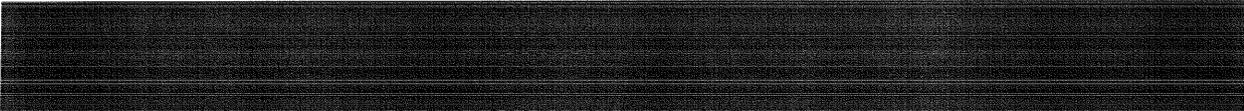




1. INTRODUCTION

The Transportation Security Administration (TSA) established the Airport Perimeter Security Program (APS) to support the expansion and implementation of security technology at the perimeters of United States airports. Through this program, commercial off the shelf (COTS) technologies are incorporated into an airport's security network to enhance the overall perimeter security infrastructure. As a requirement of the program, participating airports are required to submit the security technology improvement for operational testing and evaluation (OT&E) by an independent evaluator. At the request of the TSA, National Safe Skies Alliance (Safe Skies) provides OT&E services and operates along with airport authorities to verify that the response of the security technology improvement meets the airport's security expectations.

1.1 Background



installed the CyberLock[®] System, a series of electronic locks that require specific programmable keys to allow access. PIT's expectations were that the system: have capacity to work in remote areas where power and communication infrastructure do not exist, exhibit durability and easy operation, allow flexible programming for key assignments, provide access history activity, and, moreover, be maintainable and usable by airport personnel.

1.2 Purpose of Document

This Operational Evaluation Report illustrates the implementation of the CyberLock system and general user feedback provided by PIT personnel. The results reference Critical Issues that were approved in the project's Final Test Plan (DHS/TSA 2600.02.01.07-206, November 2007).

2. SCOPE

2.1 Objective

Safe Skies' operational evaluation was conducted according to the Critical Issues outlined in Section 4.3 of this report, which were approved in the Final Test Plan (DHS/TSA 2600.02.01.07-206) prior to data collection.

3. SYSTEM DESCRIPTION

3.1 System Overview

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

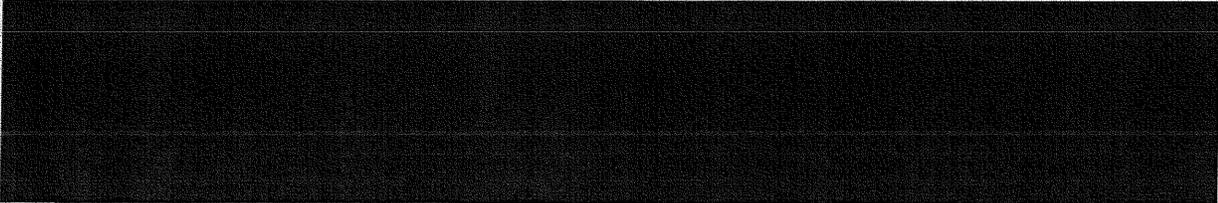
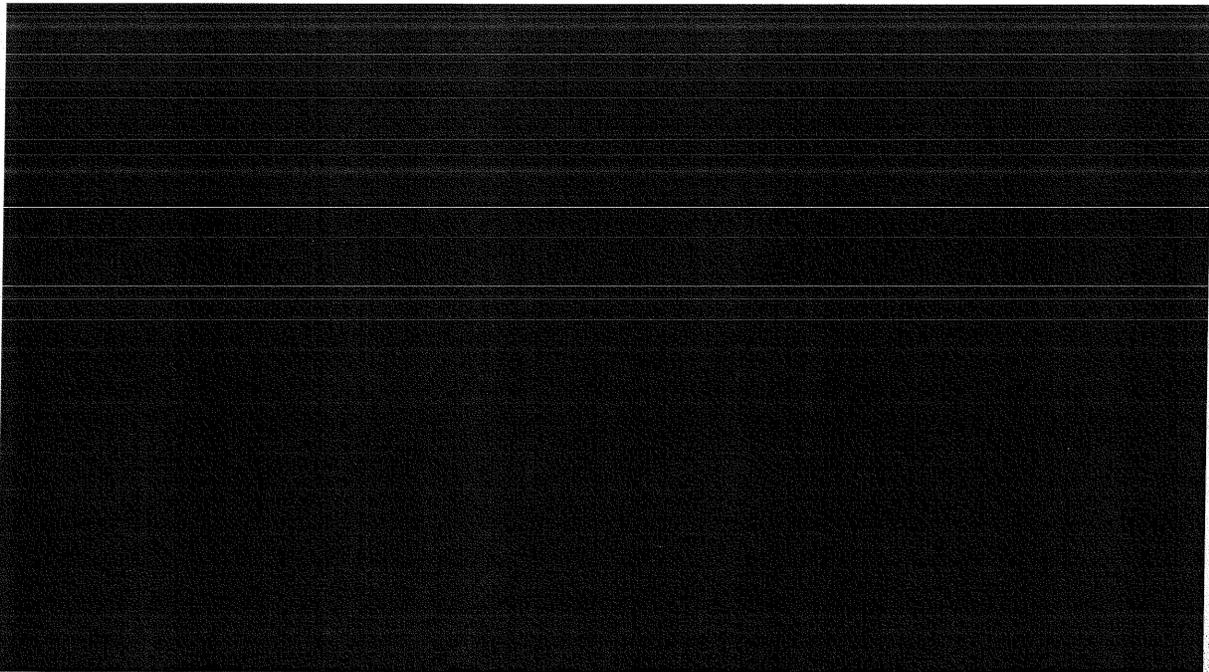
A more in depth description of the system is provided in Appendix A.

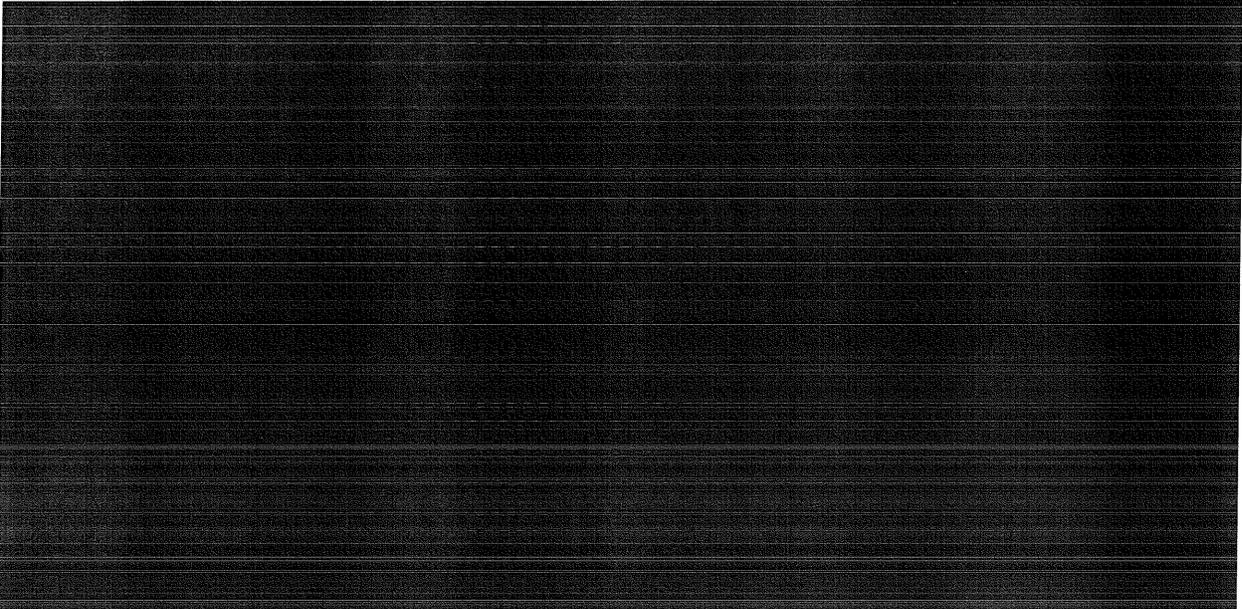
3.2 Installation

The CyberLock installation at PIT consisted of the following major components:

- 150 CyberLocks
- 200 CyberKeys
- CyberAudit Software
- 2 CyberKey Authorizers

The CyberAudit software was installed on a typical PC workstation that operated as the system's main programming terminal. The PC is located within a locked area inside PIT Badge Office, to which access is highly controlled. The main programming terminal was connected to the PIT secured LAN and communicated to the Authorizers and Keyports, which were located in the field and connected via Ethernet/fiber connections.



4. METHODOLOGY

4.1 Sites and Schedule

Testing took place at two locations: Safe Skies Headquarters (HQ) and PIT. Testing at Safe Skies HQ was conducted January 21 – February 25, 2008. The PIT installation, networking, and programming took place between November 2007 and June 2008. The distribution of the CyberLocks and Keys effectively ended December 1, 2008.

4.2 Equipment

The HQ testing operations required the following equipment:

- Thermal chamber capable of maintaining approximate temperatures of 125°F and -40°F
- Stop watch
- Infrared temperature gauge

No additional equipment was required at PIT.

4.3 Critical Issues

The CIs are the primary objectives of this evaluation. The procedures and data collection processes are designed, using Measures of Effectiveness (MOE) and Measure of Performance (MOP), to generate qualitative and quantitative data that can be used to address the identified

CI's. Measures and Tasks are used to develop methods for collecting quantitative and/or qualitative information that does not lend itself to statistical analysis.

- **CI 1: Does the system meet or exceed the facility's perimeter security expectations?**

CI 1: Does the system meet or exceed the facility's perimeter security expectations?	
Measure	Task
1 Integration effectiveness with existing network and operations infrastructure.	A CyberAudit integration with local security network
	B Integration requirements
	C Operational or maintenance issue related to integration process
2 Impact on existing access control operations	A Required time to program a CyberKey or CyberLock
	B Required time to reprogram all CyberKeys and CyberLocks in the event of a lost or stolen CyberKey
	C Required time to access a CyberLock with a CyberKey
	D Time required to provide emergency privileges
3 Programming Verification	A Schedule program feature functionality
	B Access privilege feature functionality
	C Audit report functionality
4 CyberLock and CyberKey Susceptibilities	A Hot and cold susceptibilities
	B Weather-related susceptibilities
	C Operational-usage related susceptibilities
	D Power-related susceptibilities
	E Obstruction-related susceptibilities

5. RESULTS

5.1 Measure 1: Integration Effectiveness

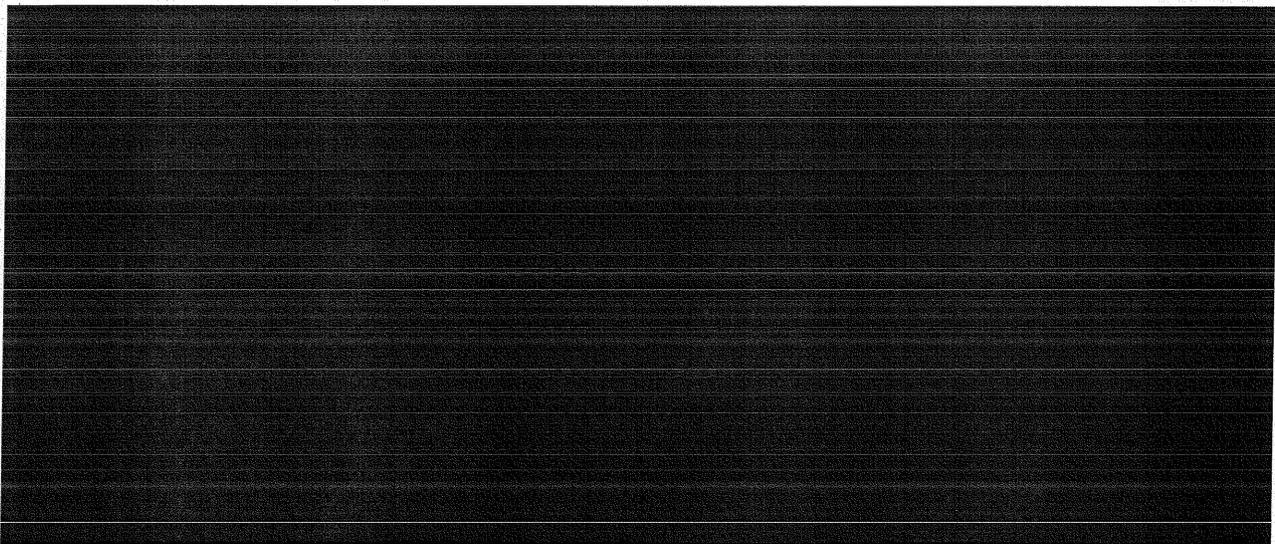
TASKS A & B

Measure 1 was evaluated by observing and recording the process by which the system was installed on the network at PIT. A survey was issued to those involved in the system installation to describe the process in broad terms and to describe the major hurdles of integration. Personnel involved in the integration included several members of the Security Department and the Information Technology (IT) Group. PIT maintenance personnel performed the physical installation.



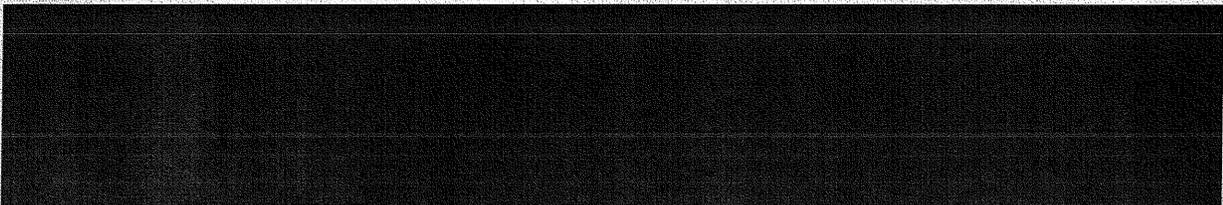
Integration requirements may change from location to location, but for the PIT site, the network requirements were as follows:

- The CyberAudit Software installed on a secured PC workstation/laptop that is network-ready
- The CyberAudit PC must be located in a secured area of the airport. (Badge Office)
- Any security data relating to airport personnel information or access controls must be stored on a secured server controlled by the airport information technology group.
- Network IP assignments must be performed by the PIT IT Group
- All passwords associated with the CyberAudit software must be generated by the PIT IT Group
- The communication between the CyberAudit/workstation and Authorizers must be secured



TASK C

The completed installation and final configuration of the hardware and software took place in July 2008. Between July and December 2008, there were no additional hardware or software issues that rendered the system non-functional. Keys and locks have been programmed, updated, and distributed to perimeter gate locations and various personnel.



[REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

[Redacted]

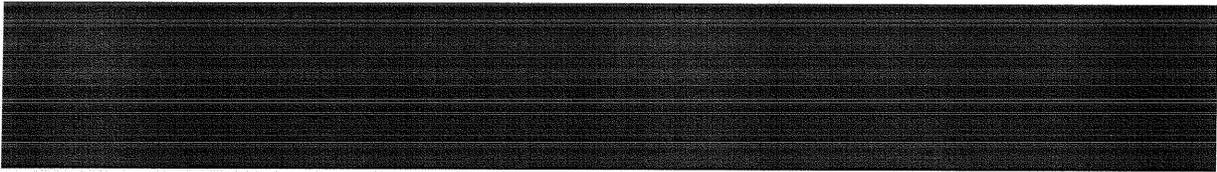
[Redacted]



TASK B

This task is based on the scenario of a user losing a master key that has full access to all locks at all time. Under a traditional lock/key system, this would compromise the security of the entire airport until such time as the locks are replaced.

The programming capabilities of the CyberAudit software allow changes to occur within the system that essentially neutralize access to the gates without having to reprogram any of the other keys. The programmer key is used to change the status of the locks so that each lock is "aware" that one particular key is missing. After updating the locks with the programmer key, the master key that was lost or stolen is now ineffective, and cannot open any locks on the premises. The time required to update the locks depends on the number of locks that are integrated into the security infrastructure and the physical distance between gates.



According to PIT security personnel, if a master key of the traditional type were lost or stolen, it would require all locks to be collected and re-cored; every key that was issued to airport personnel would have to be collected and destroyed; a set of replacement locks, latches, and keys would be issued to key personnel on a temporary basis; new keys would have to be made and distributed; and all the necessary paperwork would have to be filled out for each key. The following table shows a hypothetical comparison between the CyberLock system and the previous method at PIT. The numbers used are estimates provided by PIT. The initial cost of the PIT lock network is not immediately known, but is estimated at \$500,000. The initial cost of the CyberLock throughout the PIT lock network would be approximately \$900,000 – \$1,200,000 without any bulk discount.



Table 4. Hypothetical Comparison between Traditional Lock System and CyberLock System

Hypothetical Scenario: <i>The airport security director's vehicle is vandalized and the master key is stolen. The key allows access to 7,000 doors in the facility; 1,000 employees hold keys to the facility.</i>		
	Traditional Lock & Key System	CyberLock System
Consequences	<ul style="list-style-type: none"> • Director informs security operations that a Master Key is stolen • Estimates are called in to purchase new cores for approximately 7,000 locks \$55 per core • Estimates are called in to purchase new keys for 1,000 people \$1.40 per key • Assume contractor or union costs to perform labor \$25 per hr • Assume estimated time to re-core a lock and move to next location. 30 min • Assume 8-man team working 16 hrs a day 	<ul style="list-style-type: none"> • Director informs security operations that a master CyberKey is stolen • Security operations programs a new master key for the Director \$150 • The programmer keys 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 \$25 per hr • Assume estimated time to reprogram a lock and move to next location. 5 min • Assume 8-man team working 16 hrs a day
Total Time	26 – 29 days	4 – 5 days
Total Cost	\$450,000 – \$500,000	\$10,000 – \$20,000

A similar lost key scenario was performed in the lab while the system was being studied at Safe Skies. In the scenarios performed at the Safe Skies facility, 20 locks and 6 keys were utilized. Each key was programmed for full access to every lock. The tester then accessed the key privileges in the CyberAudit software and changed the status to "Lost." The programmer key was updated with the lost key information and transmitted to each of the 20 locks. In every instance, the lock would not grant access to the lost key. This was repeated on all 20 locks with each of the 6 keys, and all 120 attempts successfully denied access with the lost key.



TASK D

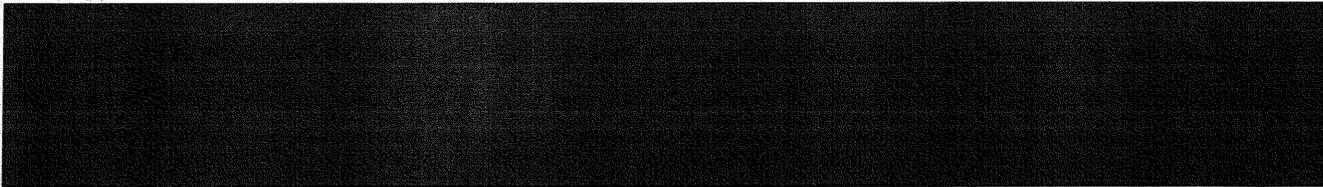
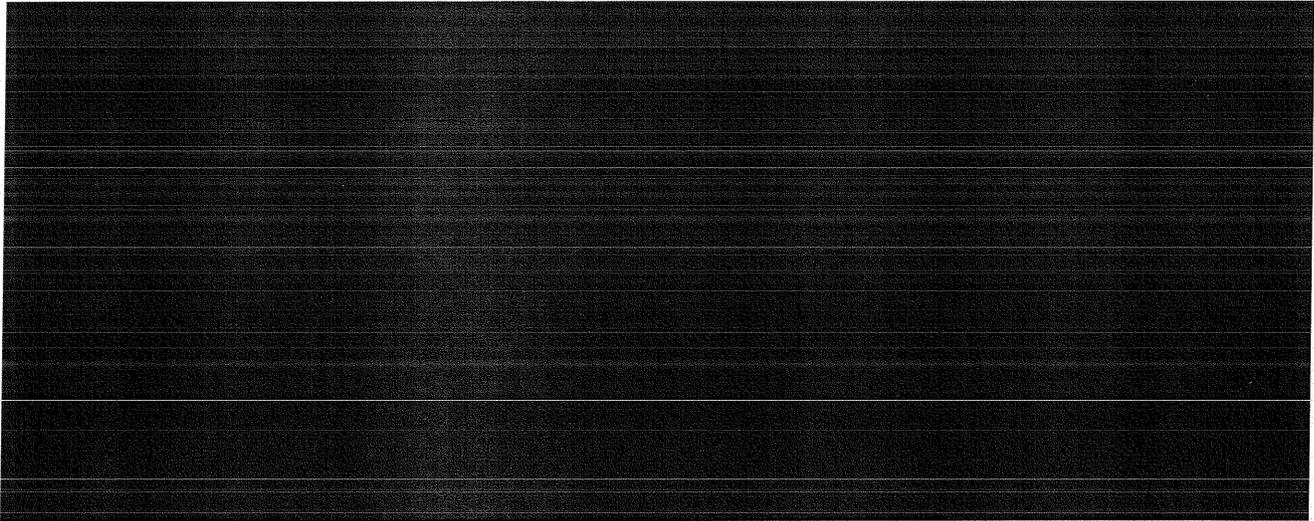
This task pertains to the time required to provide emergency privileges in the case of a crisis situation. This scenario was not physically implemented. PIT personnel decided that it would serve better to allow first responders and specific staff complete access 100% of the time, thus eliminating any need for an emergency privilege update.

5.3 Measure 3: Programming Verification

TASK A

This measure involves the functionality of the CyberLock and CyberKey programming. More than 400 programming functions were performed on both the CyberKeys and CyberLocks at Safe Skies HQ, but only 400 were recorded for testing purposes.

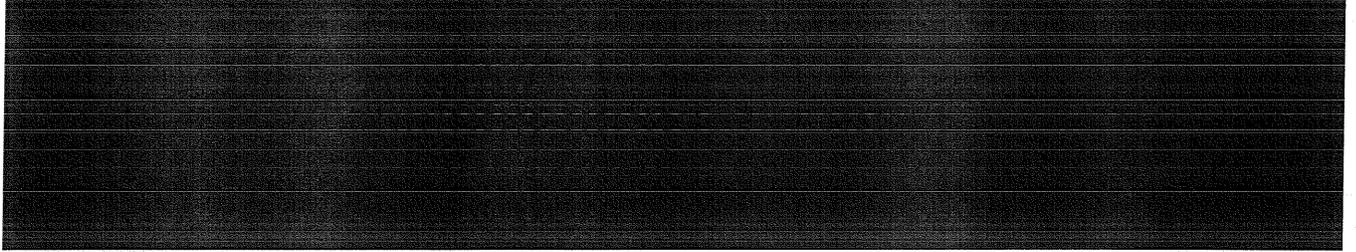
The following list describes the range of programming complexity that was performed to test the programming functions of the key:





TASK B

The scenarios to test the CyberLocks did not range in complexity to the same extent as the CyberKeys:

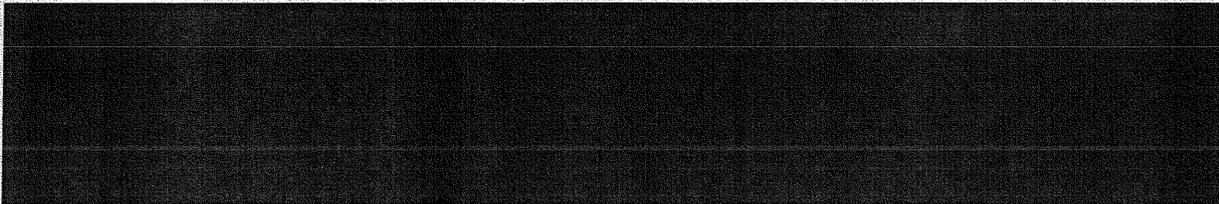


TASK C



Table 5. Audit Report Functionality Results

	Gate
Key	



[Redacted]

[Redacted]

[Redacted]

[Redacted]

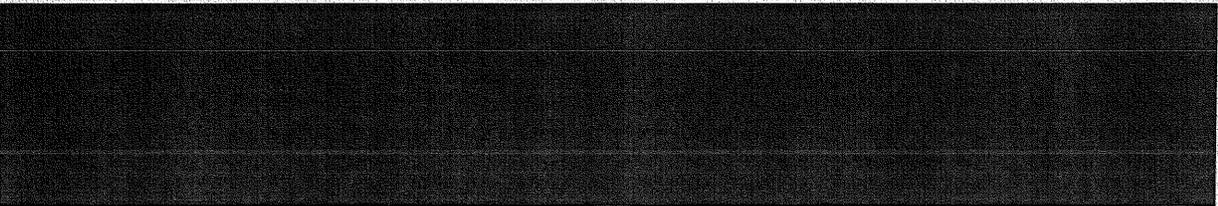
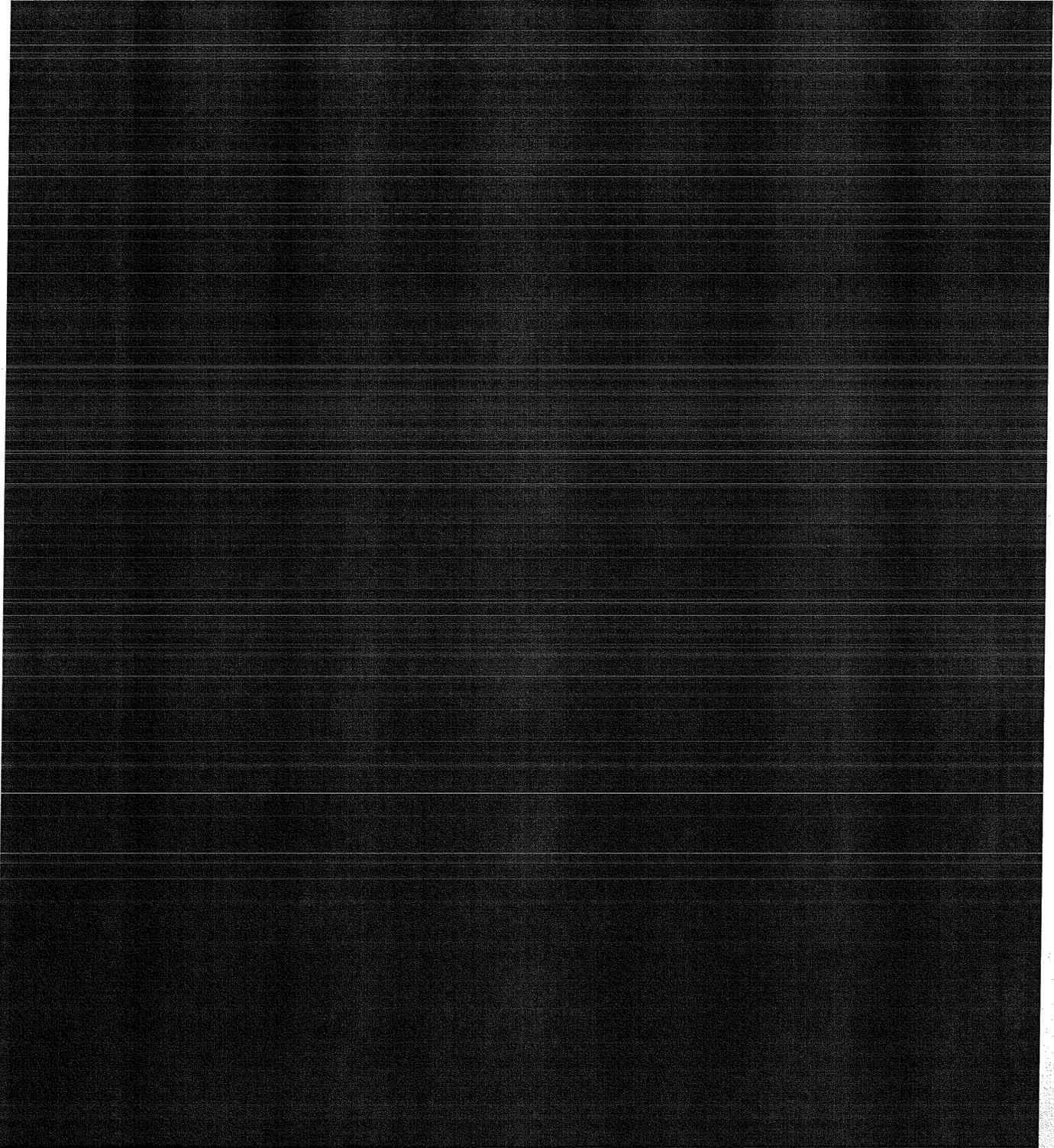
[Redacted]

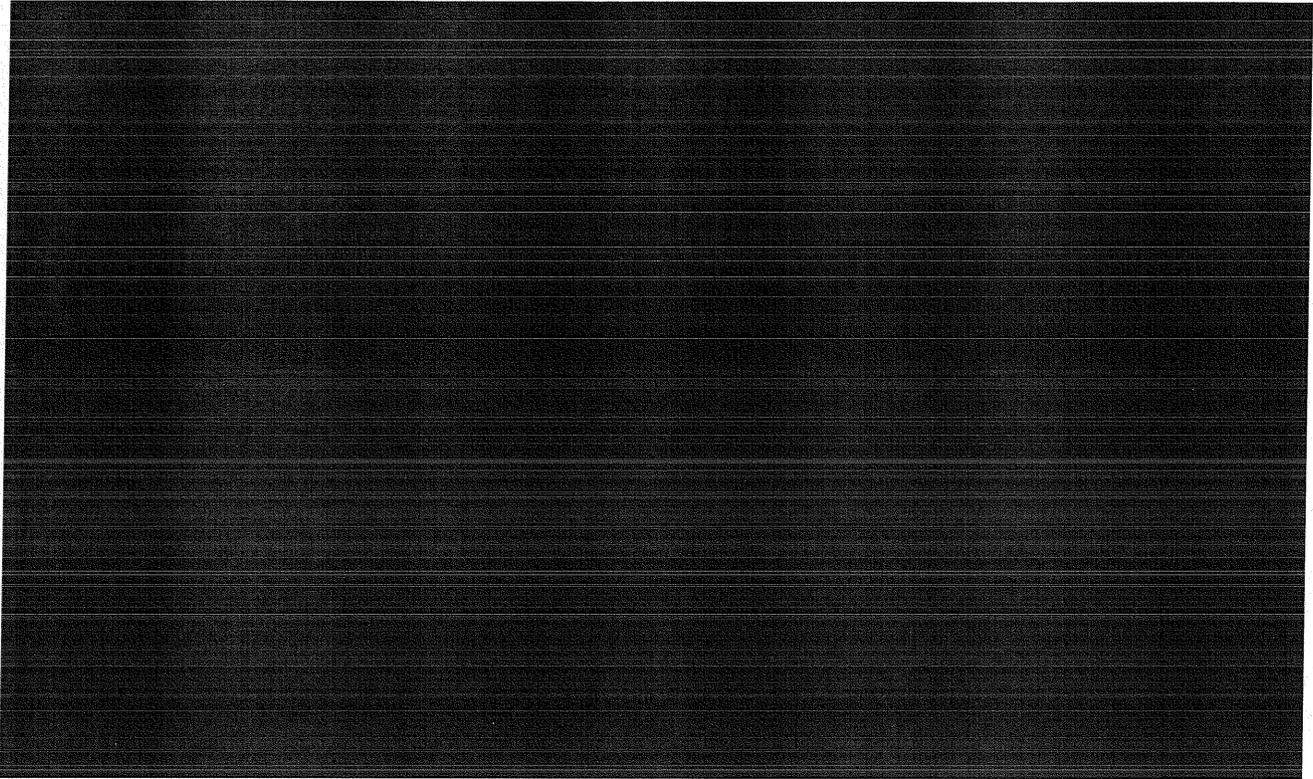
[Redacted]

[Redacted]

[Redacted]

[Redacted]





6. REFERENCES

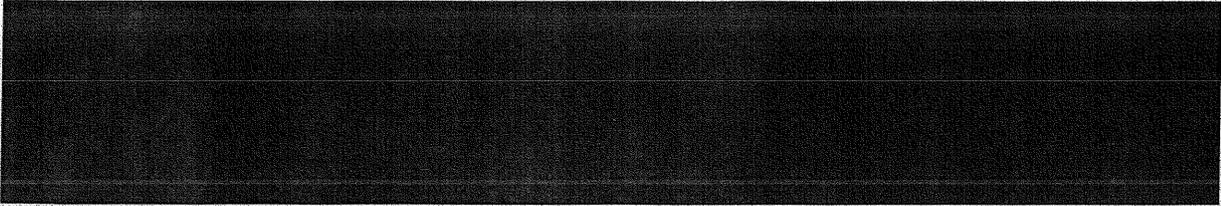
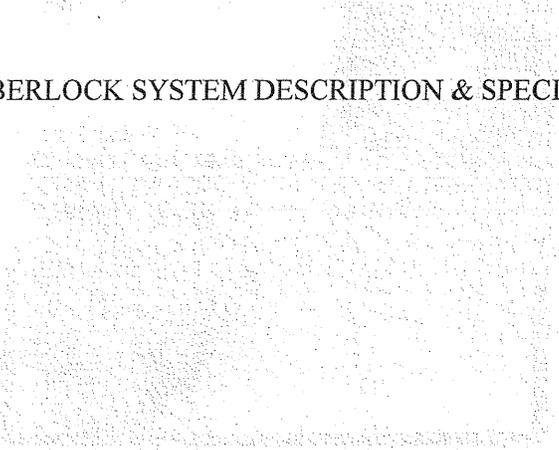
NIST (2006). *NIST/SEMATECH e-Handbook of Statistical Methods*,
<http://www.itl.nist.gov/div898/handbook/>, January 7, 2009.

SAS Institute, Inc. (2008). *Documentation for SAS® 9.2 Products*.
<http://support.sas.com/cdlsearch?ct=80000>, January 7, 2009.





APPENDIX A – CYBERLOCK SYSTEM DESCRIPTION & SPECIFICATION SHEETS



[REDACTED]

The CyberLock® System is a proprietary access control security solution manufactured by Videx, Inc. of Corvallis, Oregon. The system is designed to provide:

- Flexible programming of assigned locks and keys
- Decreased lost time associated with a turn-around caused by a lost or stolen key
- Reliable operation in various temperatures and operational conditions
- Access control monitoring capabilities
- Flexible low cost installation and maintenance

The CyberLock® utilizes electronic locks and keys instead of normal mechanical locks. It consists of five main components:

- CyberLocks
- CyberKeys (Figure 1)
- Authorizers
- Programmers
- CyberAudit software

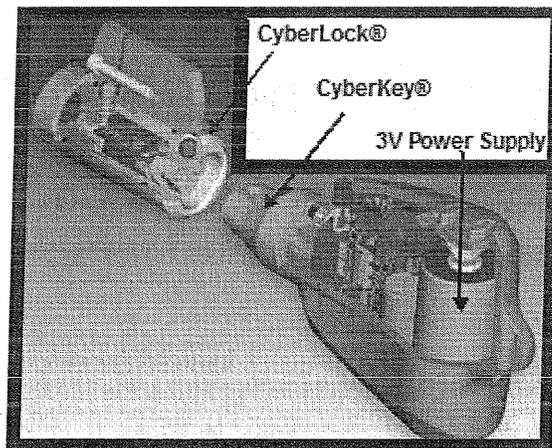


Figure 3. CyberLock® System

In this pilot application, the CyberLocks appear as standard locks designed for outdoor fence security. The core and tumbler mechanism inside the lock, however, is electronic and does not accept standard keys, only CyberKeys.



CYBERLOCK

A CyberLock stores its identity⁹ in an encrypted format in non-volatile memory inside the lock. In addition to maintaining identity information, the CyberLock is capable of storing thousands of access-attempt history records that include key identities, dates, times, and failure records. It should be stressed that there is not power supply inside the lock itself. All power required for access control purposes is transmitted via the CyberKey.

CYBERKEY

The CyberKey is equipped with a 3V lithium ion battery, and does not require a constant power supply in order to maintain operation or retain information. A CyberKey is assigned to a single person, and that person's identity information—which includes name, rank, position, access rights, and/or access schedule—are encrypted and stored in the onboard memory of the key. The encryption, which is established by the main programming terminal, is the same as that of the lock, thus allowing for secure information transmission when attempting access to a lock. Additionally, the CyberKey documents the access-attempt history of the key, reporting the lock identities, dates, times, and failure records. When a key is refreshed at an Authorizer, it instantly downloads the access history to the main programming terminal for auditing purposes.

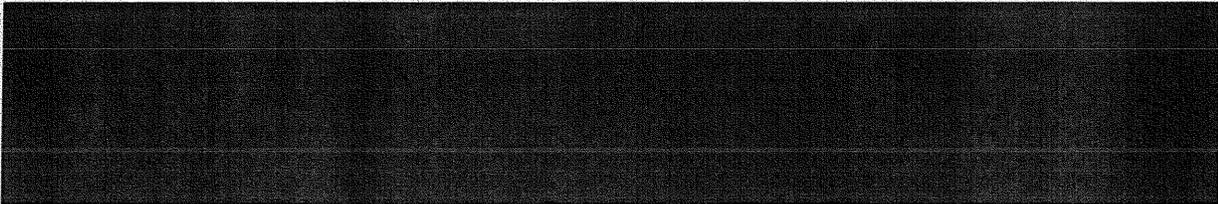
AUTHORIZER

Key privileges can only be changed through the main programming terminal, but the information can be transmitted via the Authorizer. Authorizers are remote stations that communicate back to the main programming terminal where the CyberAudit software is housed. These Authorizers are strategically positioned in remote locations to allow users expedited CyberKey updates. Typically, they would be placed near time punch-card locations or main entryways through which employees typically traverse. As an additional security feature, each Authorizer is equipped with a numerical key pad, where a user may enter their PIN before any information is transmitted over the network.

PROGRAMMER KEY

Information can only be transmitted to or from the CyberLock via the Programmer Key. The primary purpose of the Programmer Key is to transmit encrypted identity information between the locks and the CyberAudit software. However, the Programmer Key and Programmer USB attachments can be used to perform manual audits of the locks themselves. For example, if someone with a CyberKey attempted to gain access to a remote area under suspicious circumstances a manual audit would be able to record the details of the attempt from the lock without the suspect being aware. Only one Programmer Key is issued per system. CyberLocks cannot have information deleted or reprogrammed simply by using another Programming Key from Videx; and new Programmer Keys must be ordered through Videx and reprogrammed at the main programming terminal. The encryption on the Programming Key is unique to the

⁹ Identity: The lock's identity is the information that is programmed onto it by the user/administrator. It is typically named after the location in which it is placed.





software passwords on the main programming terminal and cannot be replicated on another system.

CYBERAUDIT SOFTWARE

Finally, the CyberAudit software is front end software at the main programming terminal where all of the data entry and audit tools are located. Typically, CyberLock and CyberKey identities are encrypted and stored on secured servers at a facility. The database is referenced by the main programming terminal and the Authorizers in the field. Any data that passes through the main programming terminal or Authorizer is stored in this database. The CyberAudit software is useful in searching for potentially malicious or suspicious activity, namely people trying to use their keys where they do not belong. That information is transmitted to the database whenever a user presents their CyberKey to an Authorizer, main programming terminal, or when access history is physically pulled from a lock by the Programming Key.

The company specification sheets follow:

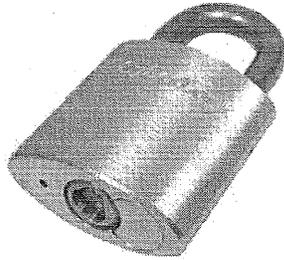
- Padlocks A-4
- CyberKey Authorizer Keyport A-6
- CyberKey, Infrared, with Replaceable Tip A-8
- CyberKey Web Authorizer Hub A-10
- CyberKey Station and Connection Cable A-12
- CyberLock Programmer A-14

Padlocks

Part number:

PL-01	1" shackle
PL-01KR	1" shackle, key-retaining
PL-02	2" shackle
PL-02KR	2" shackle, key-retaining
PL-03	3" shackle
PL-03KR	3" shackle, key-retaining

Standard Cylinder Custom Cylinder

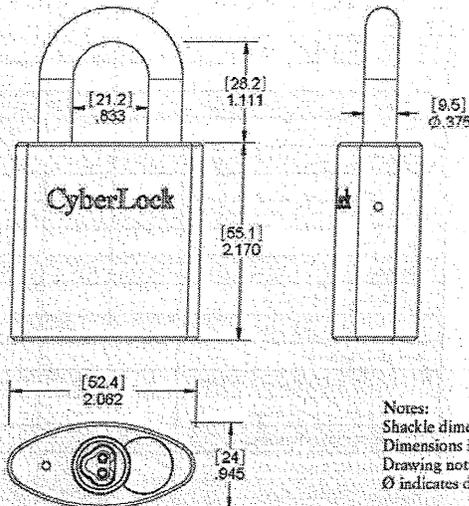


Shown: PL-01

The CyberLock padlock is a Wilson Bohannon 8900 series padlock with the CyberLock weather resistant 6-pin Schlage format cylinder pre-installed. It has a solid brass body and a stainless steel shackle. The retainer, ball bearings, and shackle pin are also stainless steel. Three shackle lengths are available as indicated by the part numbers above. On key-retaining padlocks, the shackle must be returned to the closed position before the key can be removed.

The CL-6P3WR cylinder is specifically designed for use in exposed applications such as an outdoor padlock. The weather resistant 6-pin cylinder sealed design prevents dirt and water from entering into the back of a cylinder.

Applications include storefronts, gates, construction sites, equipment, or any padlock location needing access control.



Notes:
 Shackle dimensions for PL-01
 Dimensions in inches (mm)
 Drawing not to scale
 Ø indicates diameter

602022

Common Hardware Specifications

Keys

- A key cannot be duplicated
- A key remembers up to 3900 events with date and time
- A standard user key can access up to 3300 locks
- A key contains the scheduled access days & times
- A key holds the battery power source
- Operating temperature: 32° to 122° F; 0° to 50° C

Locks

- Locks have no keyway to pick
- Locks store the last 1100 events with date and time
- No limit to the number of keys that a lock can support
- Locks are torque and electrical charge resistant
- Operating temperature: -40° to 160° F; -40° to 70° C

CyberLock System Specifications

EntryPoint™ is a hardware-only system; no software is required. All keys have 24/7 access to all locks. A complete system requires locks, keys, and a Grand Master.

CyberAudit®-Web Lite is a PC or Macintosh software program with basic access control features. A complete system requires locks, keys, a Grand Master, an IR Encoder, and Lite software. Intended for systems up to 50 locks and 50 keys.

CyberAudit Professional is a Windows program that installs on a local PC. A complete system requires locks, keys, a CyberKey station and/or Authorizer®, a CyberLock Programmer and/or USB Programmer, and the Professional software (NOTE: Professional software includes one CyberLock Programmer). Intended for systems up to 500 locks and 500 keys.

CyberAudit-Web Enterprise is web-based software installed on an application server. A complete system requires locks, keys, the Enterprise server, and one or more communicator devices. Intended for large or geographically widespread installations.

CyberLock System Features Chart

- Rekeying a system is done via the software; no need to install new locks and issue new keys
- Programmed schedules provide control over specific days and times that a key will operate
- Holidays may be set as exceptions to the schedules

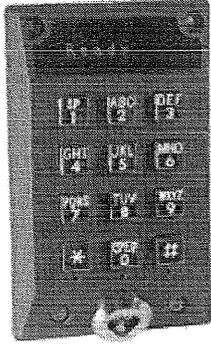
	EntryPoint	Lite	Professional	Enterprise
CyberLocks	*	*	*	*
CyberKeys	*	*	*	*
Grand Master Keys	*	*	*	*
IR Encoder		*	*	*
CyberKey Base Station			*	*
Authorizer			*	*
Cell Phone/PDA				*
USB Programmer			*	*
Audit Trail		*	*	*
Schedule Keys		*	*	*
Master Keys		*	*	*
Expire Keys		*	*	*
Lost Keys		*	*	*
Multiple Key Mode and Delay			*	*
Email Notification of Events			*	*
Web-based Software		*	*	*
Hierarchy of Administrators			*	*
Grouping of Locks and People			*	*
Grouping of Access Permissions			*	*
User Keys Download Locks		*	*	*
User Keys Program Locks		*	*	*



CyberLock® System

CyberKey Authorizer Keyport

Part number: AK-01



The CyberKey Authorizer keyport is part of the CyberKey Authorizer system. It requires an Authorizer hub to function. Please see the appropriate data sheet.

The CyberKey Authorizer is a remote interface that allows a computer and a key to exchange information via either a network or modem connection. This allows a CyberLock system spread out over a large geographical area to be controlled from one location.

The keyport includes mounting hardware for a single outlet electrical box. It can be placed up to 100 feet away from the hub, outside of the first lock (entryway) of the local CyberLock system. A second keyport can be added at any time. For increased security, the Authorizer can be set to require a personal identification number (PIN) before updating a key.

About Key Control:

For high-security areas, a key that is valid for only a short period of time is best. A key can be set to expire as little as 5 minutes after its validation. If keys are expired daily, a user would need to insert his or her key into the keyport and optionally enter a PIN to update the key with that day's access privileges before use. The CyberAudit software automatically manages key expirations either individually or in groups.

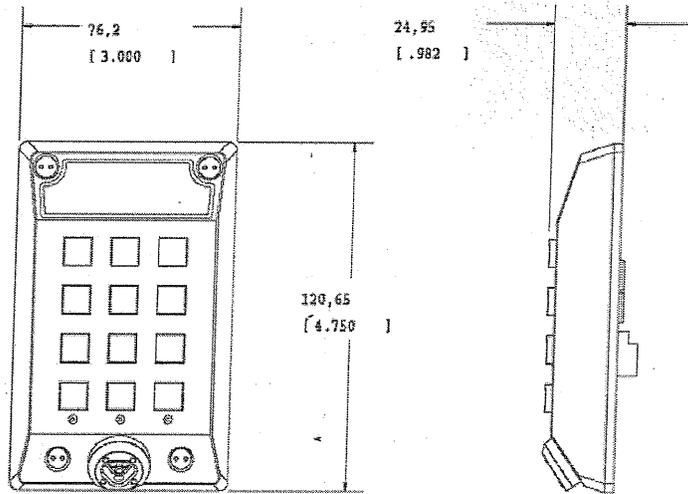
The Authorizer also downloads a key's event log when a key is inserted. A short key expiration cycle results in an up-to-date audit trail of a user's actions within the CyberLock system.



CyberKey Authorizer Keyport

Part number: AK-01

Notes:
 Dimensions in mm (inches)
 Drawing not to scale



Specifications

- Physical**
 - Black powder-coated cast aluminum with standard metal numeric keypad
 - Port for inserting CyberKey; connects to single-gang electrical box
 - Weather-resistant
- Operating Temperatures**
 - 2° to 140° F; -17° to 60° C
 - Indoor and outdoor installation
- Dimensions**
 - 0.98" H x 3.00" W x 4.75" L (2.49cm H x 7.62cm W x 12.07cm L)
- Weight**
 - 6.6 ounces (187.1g)
- Keypad**
 - Standard 12-key numeric keypad
- Power**
 - Supplied by hub
- Connection**
 - Connector: RJ-45
 - Length: 100 feet (30.48m) maximum Cat 5 Ethernet patch cable
- Display**
 - LED, 8 characters
- Additional Feature**
 - Optional PIN: 4 to 8 numbers; configured and assigned with the CyberAudit software

CyberKey, Infrared, with Replaceable Tip

Part number: CK-IR6



CyberKey is an electronic key that is used to operate CyberLocks. The CK-IR6 CyberKey is made of durable nylon-based plastic and has a replaceable brass tip. An indicator light shows battery power and key activation. A speaker makes tones indicating access, no access, and communication.

The CyberKey has memory that contains an encrypted access code, a list of locks it may access, schedules of dates and times for accessing locks, and a begin/end date range during which the key will operate. A CyberKey also contains an audit trail of up to 3,900 access events. Each time the key touches a CyberLock, it records the lock ID, date, time, and authorization status.

The CK-IR6 key communicates to the software either through the tip when placed in a CyberKey station or Authorizer Keypoint, or by making an infrared connection to an IR device. Infrared devices include cell phones, Pocket PC PDA's, and PCs with an infrared port or infrared adapter. Please contact Videx for a complete list of supported devices.

The type of communication possible depends on which of the two software systems are used to manage the CyberLock installation.

- CyberAudit 2.0 supports communication with the CyberKey station and the CyberKey Authorizer.
- CyberAudit-Web supports communication with the CyberKey Authorizer, cell phones, Pocket PC PDA's, infrared ports, and infrared adapters.

Communicator	CyberAudit 2.0	CyberAudit-Web
Key tip		
CyberKey base station	✓	
CyberKey Authorizer	✓	✓
Infrared port		
Cellular phone		✓
Pocket PC PDA		✓
IR port/adapter		✓

Additional Features:

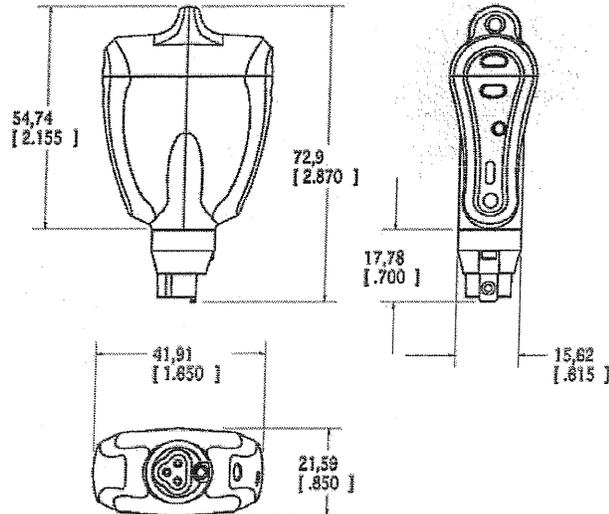
- Keys can generate a denied event in both the key memory and lock memory.
- A key can record when it was removed from a lock.
- A key's beeper can be disabled.

Additional Features with CyberAudit-Web:

- A key can use multiple schedules per lock.
- Schedules can expire independently.

CyberKey, Infrared, with Replaceable Tip

Part number: CK-IR6



Notes:
Dimensions in mm (inches)
Drawing not to scale

Specifications

- Finish** • Black plastic with a replaceable brass tip
- Operating Temperature** • 32° to 122° F; 0° to 50° C
- Operating Conditions** • Keep key dry. If exposed to water, remove battery and allow key to dry completely before use.
- Battery** • 1 CR-2 3v lithium battery
- Battery Life** • 2000 to 5000 openings, depending on settings and battery.
- Infrared Requirements** • CyberAudit-Web, CyberAgent
 - Remote IR devices must have an internet connection
- Number of Locks per Key** • Up to 3300 locks can be accessed with a standard user key.
 - A Master key has no limit to the number of locks it can access.
 - A database has no limit to the number of locks or keys it can manage.
- Access Schedules** • Schedules programmed into the CyberKey provide complete control over specific days and times that a key will operate. A key can use up to 49 different schedules to access locks.
 - A database has no limit to the number of schedules it can manage.
 - Holidays may be set as exceptions to the schedules.
- Audit Capacities** • A key remembers up to 3900 events with date and time. It can be set to keep only the most recent set of events or to stop operating when its audit trail is full.
 - The lock remembers the last 1100 events with date and time.
- Electronic Security Features** • Key Expiration – a begin/end date range can be set during which the key will work.
 - A key retains its audit trail if the power is interrupted.
- Electronic Rekeying** • Rekeying a system is done via the software; no need to install new locks and issue new keys.

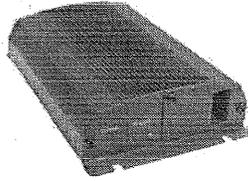
Videx, Inc., 1105 NE Circle Blvd., Corvallis, OR 97330 • 541-758-0521 • Fax 541-752-5285 • www.videx.com • sales@videx.com

CyberKey Web Authorizer Hub

Part numbers:

AH-W1 120v, 60Hz Station
 AH-W2 220v, 50Hz Station

Lite Professional Enterprise

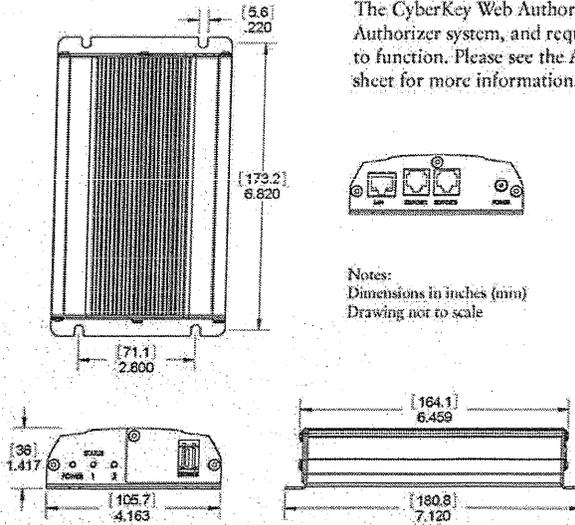


The CyberKey Web Authorizer Hub is one of three Authorizer hubs that allow programming and downloading keys from a remote location. The Web version of the hub works with Enterprise version 1.4 or higher and allows remote key communication either via LAN or over the internet. The Web Hub functions as a web client using HTTP with 128-bit SSL. It offers options of DHCP or static IP address selection.

In addition to being a remote CyberKey communicator, the Web Authorizer Hub stores key configurations in memory. This allows the hub to program a key even if it does not have a current connection to the CyberAudit database. It also stores the data downloaded from keys until the connection with the database is re-established.

The Web Authorizer Hub is made of black powder-coated aluminum, and has dual LED lights to indicate power and status. The hub has 2 USB connections and 3 RJ-45 connections, one for 100baseT Ethernet, and two for Keypoint connections. Either a 120v, 60Hz or 220v, 50Hz power supply is included, as indicated by the part numbers above.

The CyberKey Web Authorizer Hub is part of an Authorizer system, and requires an Authorizer Keypoint to function. Please see the Authorizer Keypoint data sheet for more information.



5002241

CyberKey Web Authorizer Hub Specifications

- Physical
 - Finish: Black powder-coated extruded aluminum
 - Dimensions: 1.42" H x 4.15" W x 7.12" L (3.60cm H x 10.54cm W x 18.08cm L)
 - Weight: 15.3 ounces (433.7g)
 - Operating Temperatures: 32° to 122° F; 0° to 50° C; indoor installation
- Power
 - Input: 12VDC, 500MA
 - AH-W1 has a 120V, 60Hz transformer
 - AH-W2 has a 220V, 50Hz transformer
- Connections
 - RJ-45 for 100baseT Ethernet
 - 2 RJ-45 for keyports; keyports connect to hub using CAT5 patch cable
 - USB for flash drives used to configure the Web Authorizer
- Indicator Lights
 - Power and (2) Status
- Ethernet
 - 100BaseT; 100Mbps, RJ-45
 - Length: 250 feet maximum using CAT5 patch cable
- Clock
 - Real time clock with 24-hour backup
- Regulatory Compliance
 - FCC
- Memory
 - 128MB NAND Flash, 64MB NOR

Connection to CyberAudit-Web server:

The Web Authorizer behaves as a web client that periodically checks in to its server using 128-bit https. A CyberAudit-Web server only responds if the Web-Authorizer's unique ID is found in its database.



CyberKey Station and Connection Cable

Part numbers:

CKB-002	120v, 60Hz Station
CKB-F02	220v, 50Hz Station
TWC-008	9-pin PC serial cable
TWC-001	25-pin PC serial cable

The CyberKey Station is one of two electronic interfaces that allow a computer and a key to exchange information. The other is the CyberKey Authorizer; please see the appropriate data sheet for information.

The CyberKey Station is finished in black metal and has a slot for a single key. Three separate lights indicate power, status, and communication. It ships with an external transformer to provide power. Videx offers transformers for two different input power requirements as indicated by the part numbers above.

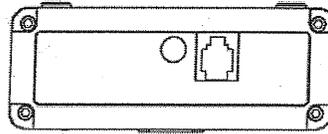
Two different PC connection cables are available, a 9-pin and a 25-pin. Both cables use phone connectors (RJ-11) to connect to the base station. Most PCs accept the 9-pin serial cable. Some older PCs will need the 25-pin serial cable. A cable pin-out diagram is available from Videx technical support upon request.

CyberLock® System

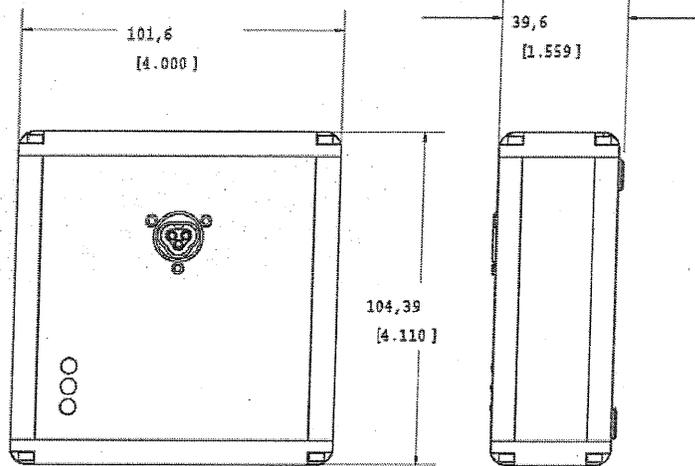
CyberKey Station and Connection Cable

Part numbers:

CKB-002	120v, 60Hz Station
CKB-F02	220v, 50Hz Station
TWC-008	9-pin PC serial cable
TWC-001	25-pin PC serial cable



Notes:
Dimensions in mm (inches)
Drawing not to scale



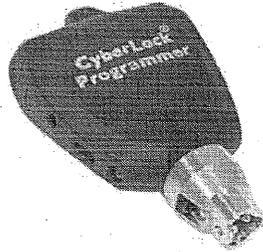
CyberKey Station Specifications

Finish	Black powder coated metal
Operating Temperature	32° to 122° F: 0° to 50° C
Communication Speed	9600 bps
Station Power Requirements	12 volts DC, 300 milliamps, center post positive
Transformer for CKB-002	In: 120VAC, 60Hz: Out: 12 volts DC, 300 milliamps
Transformer for CKB-F02	In: 220VAC, 50Hz: Out: 12 volts DC, 300 milliamps
Regulatory Compliance	FCC, CE

Videx, Inc., 1105 NE Circle Blvd., Corvallis, OR 97330 • 541-758-0521 • Fax 541-752-5285 • www.videx.com • sales@videx.com • www.videx.com

CyberLock Programmer

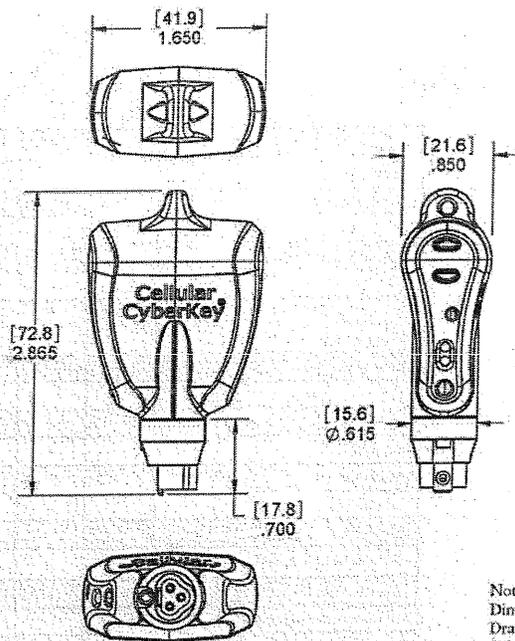
Part number: CK-P4



The Videx CyberLock Programmer is a device that is used to program and download CyberLocks in conjunction with the Professional and Enterprise software solutions. The CK-P4 case is made of a durable nylon-based plastic. An indicator light shows battery power and activation. A speaker makes tones indicating communication and programming status. Although the Programmer resembles a key, it will not open a CyberLock.

The Programmer's memory contains an encrypted access code, a list of locks to program, and the programming instructions for those locks.

The CyberLock Programmer is also used to download the audit trail from a lock.



Notes:
 Dimensions in inches (mm).
 Drawing not to scale
 Ø indicates diameter

0202121

Common Hardware Specifications

Keys

- A key cannot be duplicated
- A key remembers up to 3900 events with date and time
- A standard user key can access up to 3300 locks
- A key contains the scheduled access days & times
- A key holds the battery power source
- Operating temperature: 32° to 122° F; 0° to 50° C

Locks

- Locks have no keyway to pick
- Locks store the last 1100 events with date and time
- No limit to the number of keys that a lock can support
- Locks are resistant to electrical charge, magnetic force, and torque
- Operating temperature: -40° to 160° F; -40° to 70° C

CyberLock System Specifications

EntryPoint™ is a hardware-only system; no software is required. All keys have 24/7 access to all locks. A complete system requires locks, keys, and a Grand Master.

CyberAudit®-Web Lite is a PC or Macintosh software program with basic access control features. A complete system requires locks, keys, a Grand Master, an IR Encoder, and Lite software. Intended for systems up to 50 locks and 50 keys.

CyberAudit Professional is a Windows program that installs on a local PC. A complete system requires locks, keys, a CyberKey station and/or Authorizer®, a CyberLock Programmer and/or USB Programmer, and the Professional software (NOTE: Professional software includes one CyberLock Programmer). Intended for systems up to 500 locks and 500 keys.

CyberAudit-Web Enterprise is web-based software installed on an application server. A complete system requires locks, keys, the Enterprise server, and one or more communicator devices. Intended for large or geographically widespread installations.

CyberLock System Features Chart

- Rekeying a system is done via the software; no need to install new locks and issue new keys
- Programmed schedules provide control over specific days and times that a key will operate
- Holidays may be set as exceptions to the schedules

	EntryPoint	Lite	Professional	Enterprise
CyberLocks	*	*	*	*
CyberKeys	*	*	*	*
Grand Master Keys	*	*	*	*
IR Encoder		*	*	*
CyberKey Base Station			*	*
USB Station		*	*	*
Web Authorizer			*	*
Network/Modem Authorizer			*	*
Cell Phone/PDA			*	*
USB Programmer			*	*
Audit Trail		*	*	*
Schedule Keys		*	*	*
Master Keys			*	*
Expire Keys		*	*	*
Lost Keys			*	*
Multiple Key Mode and Delay			*	*
Email Notification of Events			*	*
Hierarchy of Administrators			*	*
Grouping of Locks and People			*	*
Grouping of Access Permissions			*	*
User Keys Download Locks		*	*	*
User Keys Program Locks			*	*