[redacted]

Transportation Security Administration

Office of Security Technology

Airport Perimeter Security Projects for FY06

FINAL REPORT

Newport News – Williamsburg International Airport (PHF)

Fixed Camera Tower Remote Monitoring 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

[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

The Newport News – Williamsburg International Airport (PHF) has purchased and implemented a surveillance-based perimeter protection system. The core technologies for this project are additional video surveillance via Pan-Tilt-Zoom (PTZ) cameras, day/night thermal cameras, video analytics, and a wireless communication network. Towers were erected at key locations and equipped with the core technologies. Additional power and wireless communication infrastructure was installed to channel the information into the security dispatch and command center. The airport's expectation of the perimeter protection system is to provide a [redacted]

National Safe Skies Alliance (Safe Skies) provided independent verification and validation (IV&V) services and operated along with airport authorities to verify that the fixed perimeter tower enhancements met the airport's security expectations. The IV&V was concluded November 7, 2008.

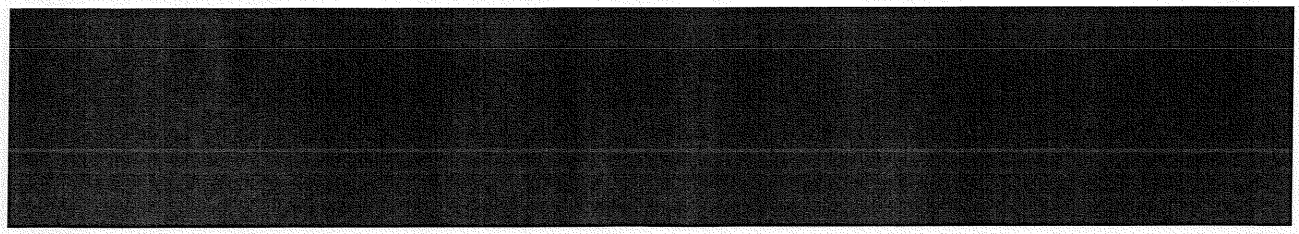
The enhanced security monitoring system combines remote towers, video surveillance equipment, wireless communication support, and video analytics with the security infrastructure. Five towers were erected at various points within the AOA, and equipment was mounted to the top of the air traffic control tower.

Vicon (SVFT-M35) PTZ cameras and FLIR (Patrol IR) thermal cameras comprise the video surveillance components of the enhancement. The thermal cameras are fixed cameras that observe heat signatures that animals, people, or objects emit at all times. They are designed so that even in complete darkness, they retain the ability to identify objects within a targeted protection area.

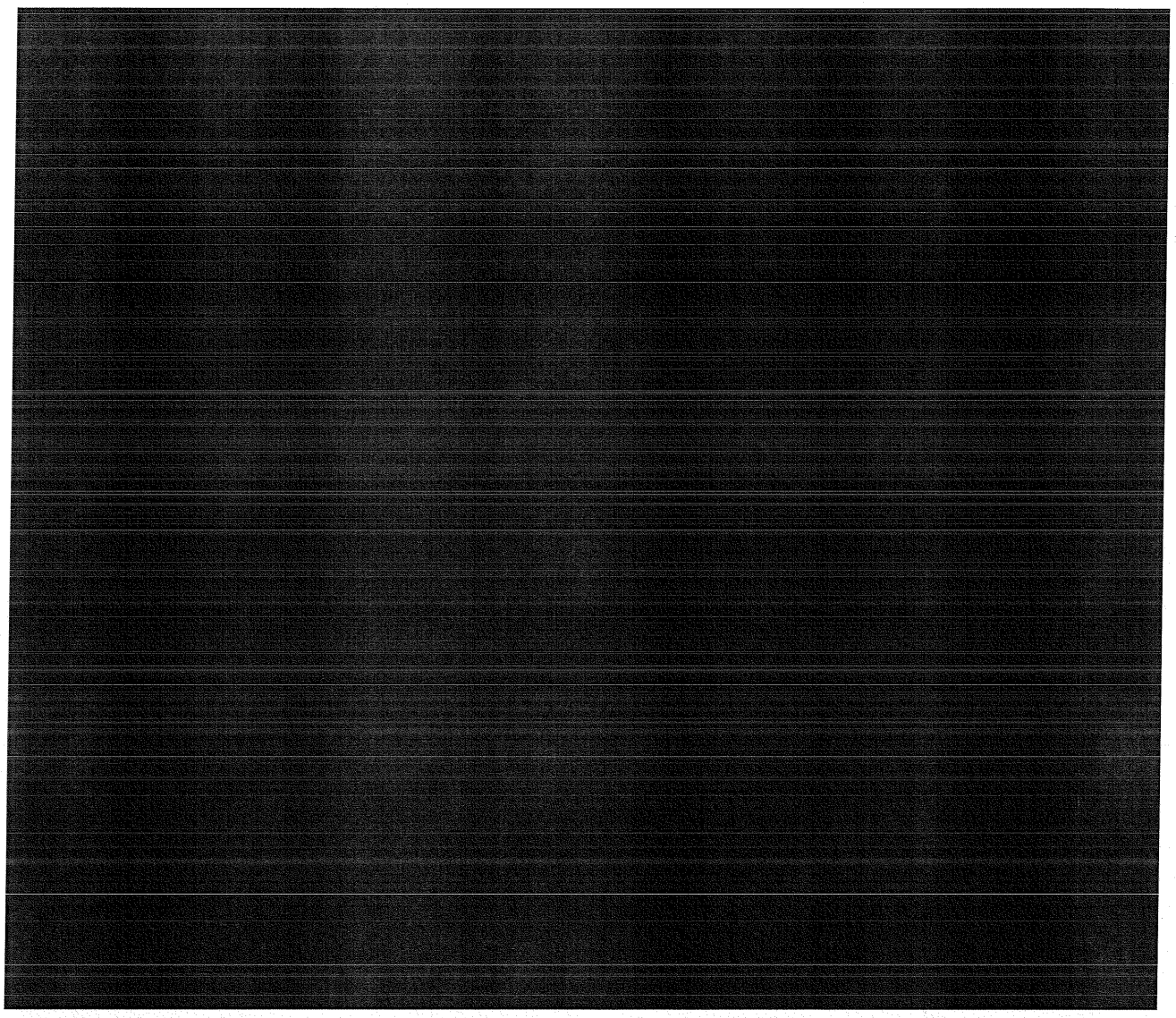
The video streams are transmitted wirelessly, through the utilization of directional antennas. The information is then relayed to the video servers at the Security Operations Center (SOC). The dispatch coordinator can review alarm information, which is relayed to dedicated video server screens, at the SOC Monitoring Station. The video analytic software handles all the unattended surveillance, which is stored on the GE video servers. The analytics software can be modified by the dispatch coordinator or security director as required to meet the unique needs of the airport.

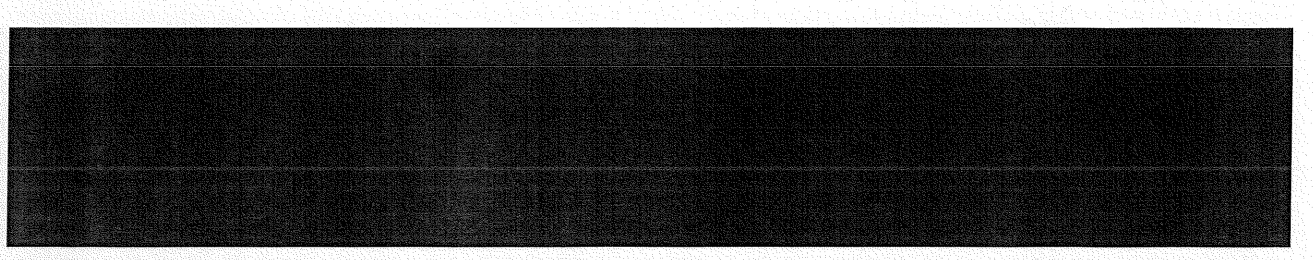
The tower PTZ cameras and thermal cameras were arranged and calibrated to cover specific areas of the AOA. These coverage areas and calibration settings can be changed as PHF personnel become accustomed to the normal operation and capabilities of the equipment and software.

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 PHF airport authorities. Representatives of TSA, Safe Skies, and PHF 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





[redacted]

DHS/TSA 2600.02.01.09-051	**Newport News – Williamsburg International Airport: Operational Evaluation Report** 	
	Project Performed by: National Safe Skies Alliance 110 McGhee Tyson Boulevard Suite 201 Alcoa, TN 37701	Safe Skies Author(s) John Hunsucker 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
	March 2009 Final Report	

[redacted]

[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.

[redacted]

[redacted]

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DHS/TSA—09-051		

4. Title and Subtitle	5. Report Date
Newport News – Williamsburg International Airport: IV&V Operational Evaluation Report	March 2009
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
John Hunsucker, Jeff Vanvactor	DHS/TSA—2600.02.01.09-051
9. TSA Reviewer(s)	10. Work Unit No. (TRAIS)
Charles Kelley, John Nestor	
11. Performing Organization Name and Address	12. Contract or Grant No.
National Safe Skies Alliance 110 McGhee Tyson Boulevard Suite 201 Alcoa, TN 37701	00-G-019
	13. Type of Report and Period Covered
	Final Report, November 2008
14. Sponsoring Agency Name and Address	15. Sponsoring Agency Code
U.S. Department of Homeland Security Transportation Security Administration 601 S. 12th Street Mail Stop TSA-16 Arlington, VA 22209	TSA-16

16. Supplementary Notes

This report was prepared by John Hunsucker of National Safe Skies Alliance

17. Abstract

This report illustrates the operational elements of the independent verification and validation as it pertains to the newly installed perimeter security enhancements at PHF. The statements included in this document are in reference to the Critical Issues that were approved in the project's Final Test Plan.

Information includes descriptions of the perimeter security enhancements, descriptions of secured areas, and results of simulated intrusions that were performed November 3 – 7, 2008.

18. Key Words

Baseline, Infrastructure, Newport News, Perimeter, PHF, Security, Site Survey, Williamsburg

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
SSI/FOUO	Unclassified	51	

[redacted]

[redacted]

DOCUMENT CHANGE HISTORY

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

[redacted]

[redacted]

TABLE OF CONTENTS

[redacted]

[redacted]

LIST OF TABLES

LIST OF FIGURES

[redacted]

[redacted]

EXECUTIVE SUMMARY

Newport News – Williamsburg International Airport (PHF) determined that there were some [redacted] PHF, through the Transportation Security Administration's Airport Perimeter Security (APS) program, installed a network of wireless observation towers, Pan Tilt Zoom (PTZ) cameras, and thermal cameras through which video analytics were used to provide automated surveillance of critical airport zones during all hours of operation.

Airport expectations were that the monitoring system:

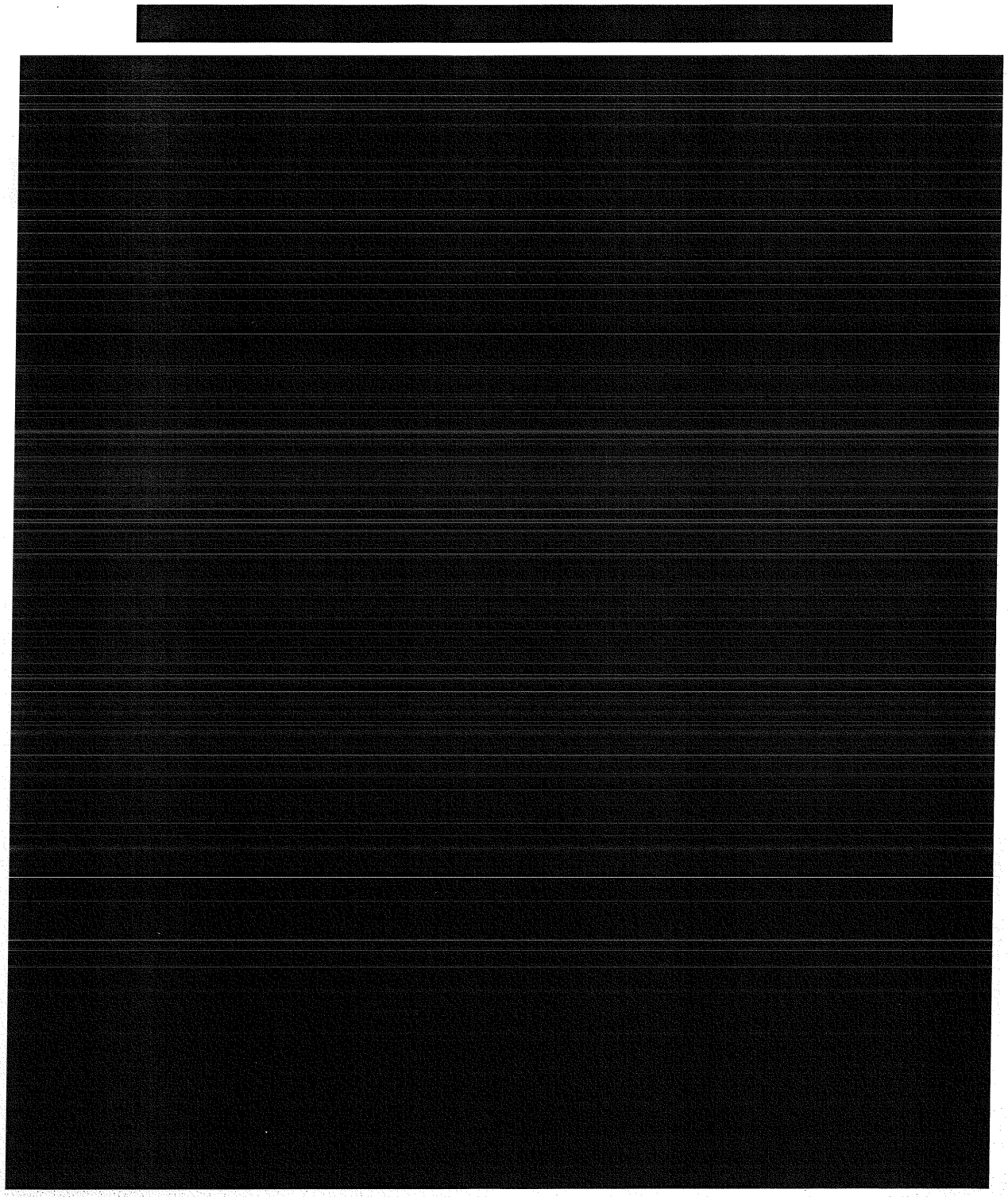
- Have the capacity to operate in remote areas and maintain stable communication
- Tower components exhibit durability and easy operation
- Allow flexible programming of assigned protected zones
- Alarm and record on suspicious activity or other events
- Provide quick reference to video archives
- Remain maintainable, usable, and economical for the airport

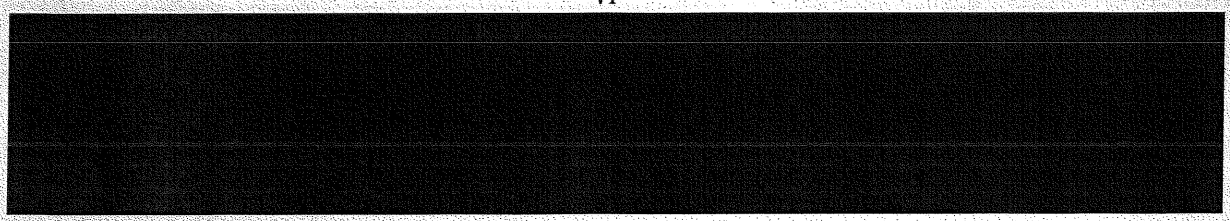
As part of the APS program requirements, National Safe Skies Alliance (Safe Skies) conducted both a baseline and an operational evaluation of the system. The data collected for the operational assessment was generated by Safe Skies personnel at PHF November 3 – 7, 2008. The field tests[1] were designed to verify that the system was capable of detecting and alarming on intruders moving through protected areas, and to provide PHF security personnel with information that can be used to further enhance the usefulness of the system in daily activities.

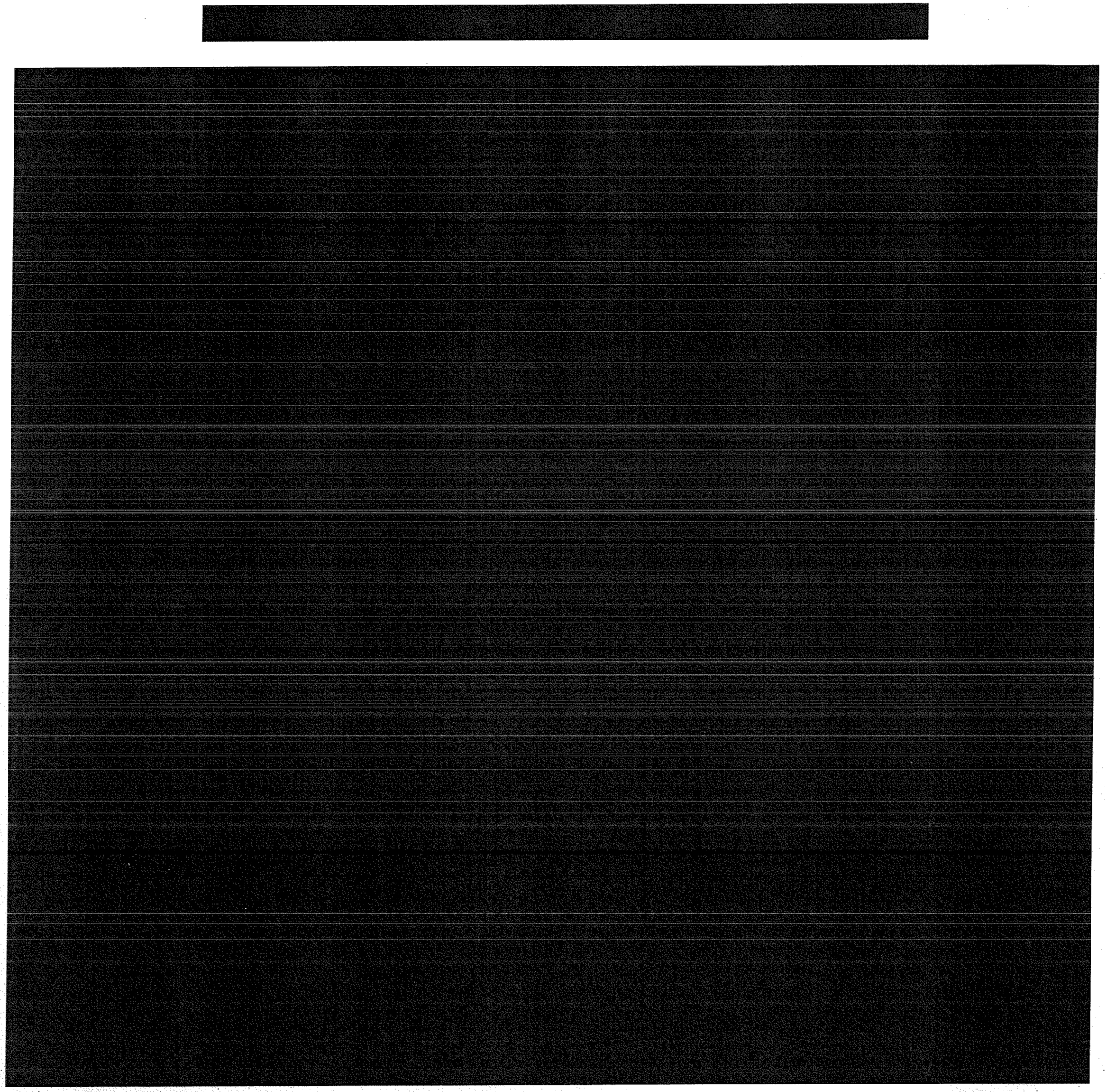
[redacted]

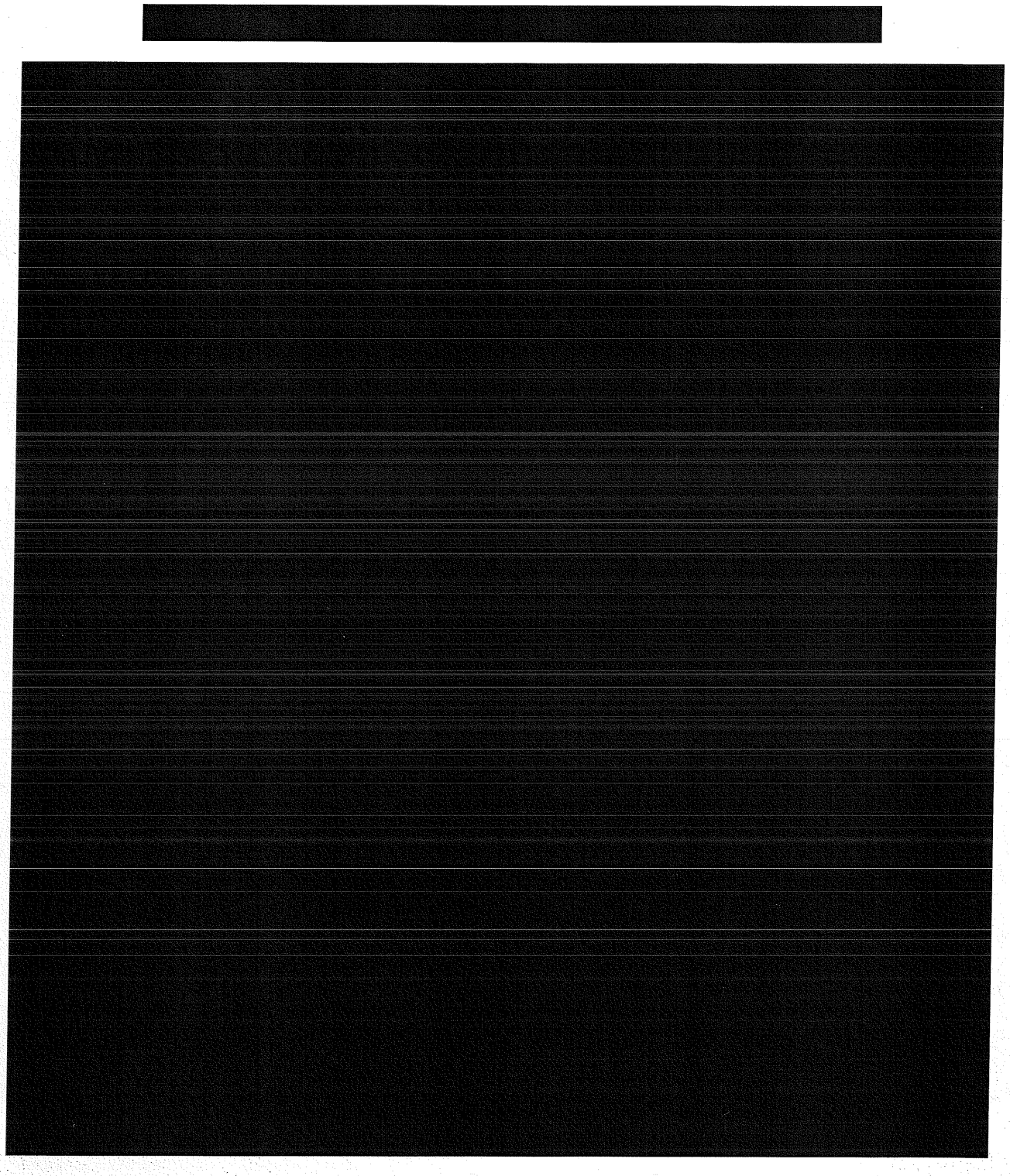
[1] Field tests are scenarios that were implemented in order to collect data that would verify that the system detects intruders and/or suspicious behavior.

[redacted]









[redacted]

ACRONYMS

ACB&P	Access Control, Biometrics, and Perimeter
AOA	Air Operations Area
APS	Airport Perimeter Security
BZ	Boundary Zone
CI	Confidence Interval
COI	Critical Operational Issue
FAA	Federal Aviation Administration
LTE	Lead Test Engineer
MOE	Measure of Effectiveness
MOP	Measure of Performance
OT&E	Operational Testing and Evaluation
OZ	Outer Zone
PHF	Newport News – Williamsburg International Airport – FAA designation
PTZ	Pan-Tilt-Zoom
RZ	Restricted Zone
SZ	Secure Zone
SIDA	Security Identification Display Area
SOC	Security Operations Center
TARZ	Taxi and Runway Zone
TSA	Transportation Security Administration

[redacted]

[redacted]

1. INTRODUCTION

The Transportation Security Administration (TSA) established the Airport Perimeter Security Program (APS) to support the expansion and implementation of security enhancements at the perimeters of United States airports. Through this program, commercial-off-the-shelf 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 enhancement for operational testing and evaluation (OT&E) by an independent evaluator. At the request of the TSA, National Safe Skies Alliance (Safe Skies) has provided the OT&E services and operated along with Airport Authorities to verify the operational effectiveness of security technology enhancements at several airports.

1.1 Background

Through the APS program, the Newport News – Williamsburg International Airport (PHF) has purchased and implemented a surveillance-based perimeter protection system. The core technologies for this project are additional video surveillance via Pan-Tilt-Zoom (PTZ) cameras, day/night thermal cameras video analytics, and a wireless communication network. Towers were erected at key locations[2] and equipped with the core technologies. Additional power and wireless communication infrastructure was installed to channel the information into the security dispatch and command center. The airport's expectation of the perimeter protection system is to provide a

[redacted]

1.2 Purpose of Document

This report documents the physical detection elements of the PHF enhancements, performance of the enhancements with respect to operational testing and evaluation methodologies listed in Section 3.1 – Critical Operational Issues of the Final Test Plan[3], and any outstanding issues concerning operability or maintenance requirements.

2. SCOPE

2.1 Objective

Safe Skies' operational evaluation of the surveillance and monitoring enhancements at PHF verify the operational capabilities of the technology. The results will serve as a source of information to compare against future or past evaluation efforts, and provide security personnel with information that can be used to further enhance the usefulness of the system in daily activities.

[2] A ***key location*** is a physical site within the facility area that is projected to have the greatest visibility and coverage of the perimeter.
[3] DHS/TSA 2600.02.01.08-206, November 2008

[redacted]

[redacted]

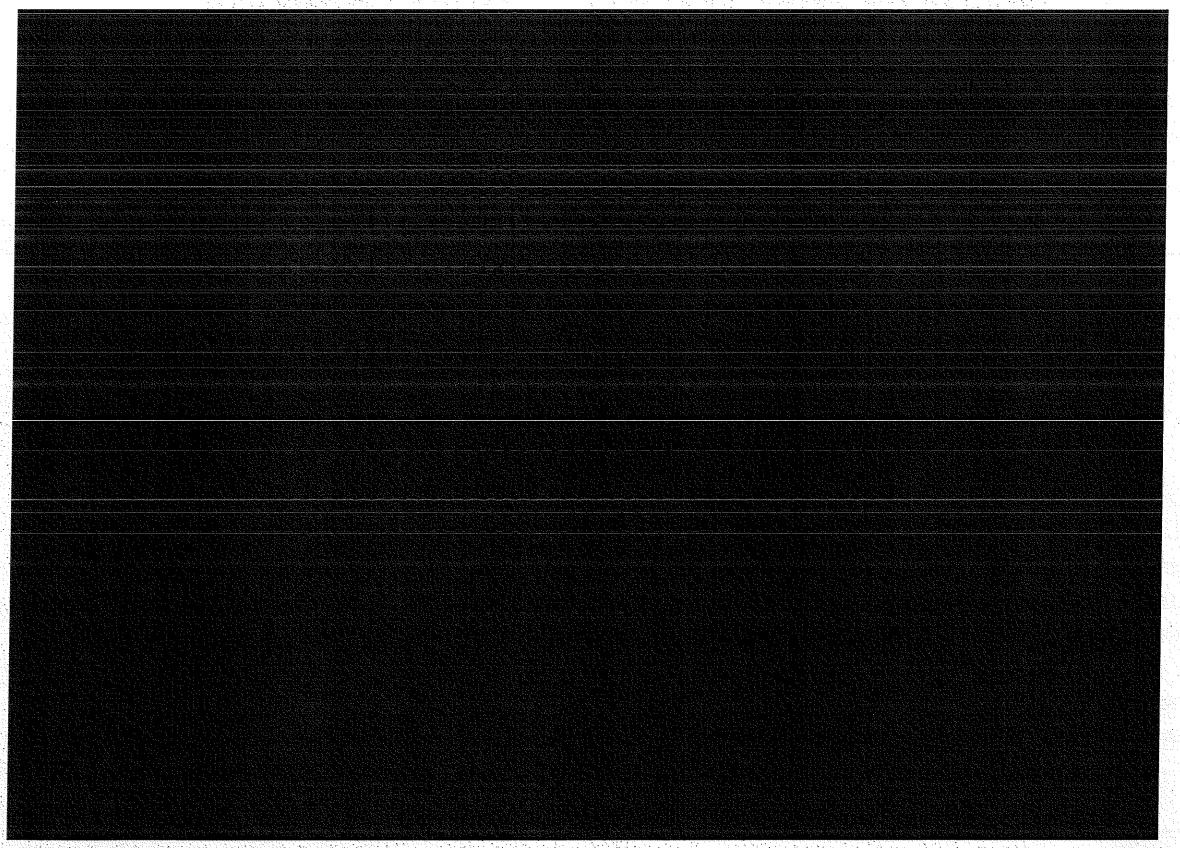
2.2 Limitations

Operational data was collected on the current calibration of the enhancement as established by PHF security personnel in conjunction with consultants from iComm, Inc., the primary integrator. Calibration settings were made prior to the arrival of the Safe Skies test team in November 2008. As such, any detection/coverage areas that are not included in the evaluation were intentionally excluded due to the operational settings in use by PHF security personnel.

3. SYSTEM/PROCESS DESCRIPTION

3.1 System Description

The enhanced security monitoring system combines remote towers, video surveillance equipment, wireless communication support, and video analytics with the security infrastructure. Five towers were erected at various points within the AOA, and equipment was mounted to the top of the FAA tower. Figure 1 shows the approximate location of each tower and its associated equipment.


[redacted]

[redacted]

[redacted]

Vicon (SVFT-M35) PTZ cameras (Appendix B) and FLIR (Patrol IR) thermal cameras (Appendix C) comprise the video surveillance components of the enhancement. The thermal cameras are fixed cameras that observe heat signatures that creatures, people, or objects emit at all times. They are designed so that even in complete darkness they retain the ability to identify objects within a targeted protection area.

The video streams are transmitted wirelessly, through the utilization of directional antennas. The information is then relayed to the video servers at the Security Operations Center (SOC), shown in Figure 2 below

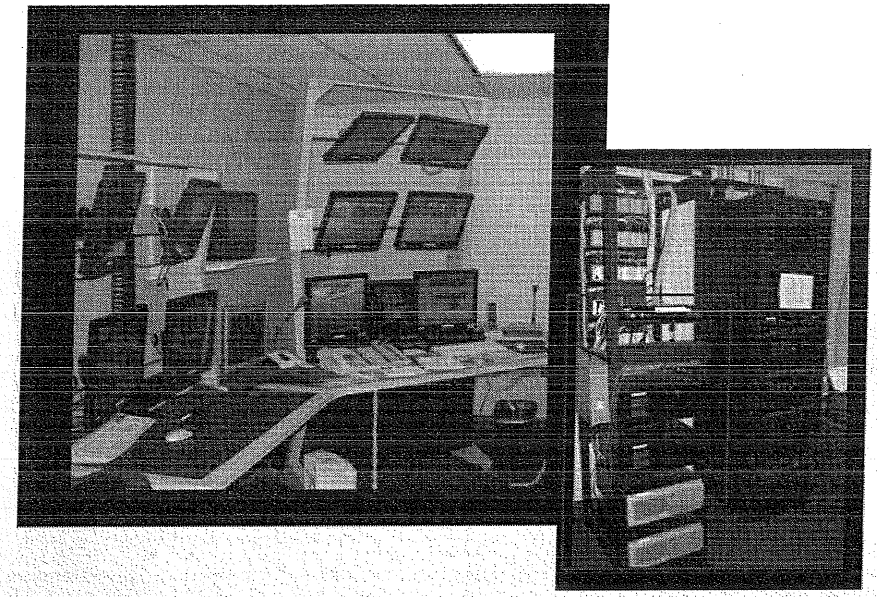


Figure 2. SOC Monitoring Station and Video Servers (Highlighted in Red)

Within the SOC, the dispatch coordinator can view and control all the cameras, and review alarm information, which is relayed to dedicated video server screens. The video analytic software handles all the unattended surveillance, which is stored on the GE video servers[4]. The analytics software can be modified by the dispatch coordinator or security director as required to meet the unique needs of the airport.

The tower PTZ cameras and thermal cameras were arranged and calibrated to cover specific areas of the AOA. These coverage areas and calibration settings can be changed as PHF

[4] Technical specifications for the GE Video servers and the Vicon DVR system can be found in Appendices D and E. Specifications for the wireless components are attached as Appendices F – H.

[redacted]

[redacted]

personnel become accustomed to the normal operation and capabilities of the equipment and software. Details of the current coverage of the towers are shown in Figures 3, 4 and 5 below.

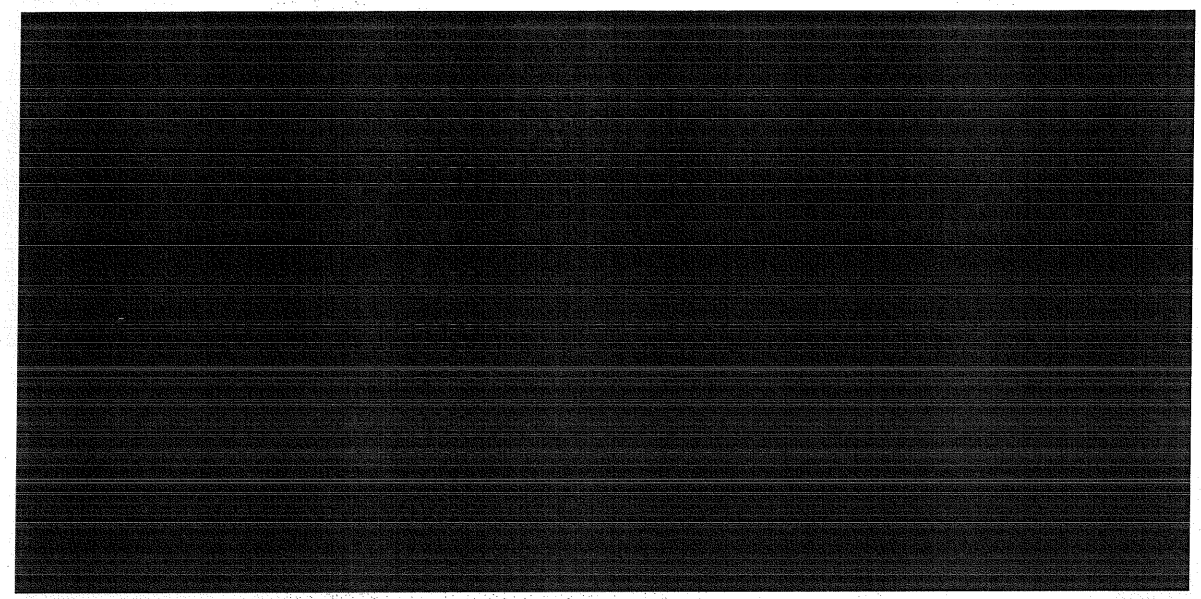


Figure 3. Tower Locations With PTZ Coverage Areas (Solid White Circle) and Thermal Imager Coverage Areas (Black and White Lines)

The areas enclosed by the black and white dashed lines illustrate the current thermal camera coverage. These are the approximate areas where the video analytics can detect and alarm on intruders, creatures, or objects. The solid white lines show the PTZ coverage of the towers. The PTZ coverage areas in this report are conservative estimates based on the orientation of the cameras, height of the towers, and the visible image at the front end in the SOC.

[redacted]

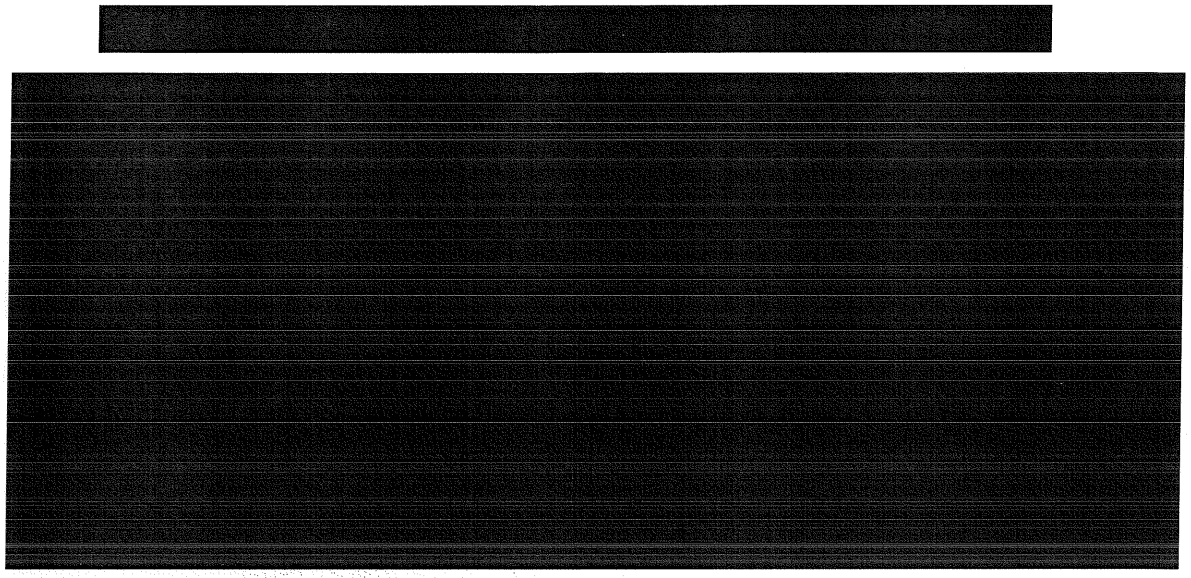


Figure 4. Thermal and PTZ Camera Coverage for Towers 1 and 2

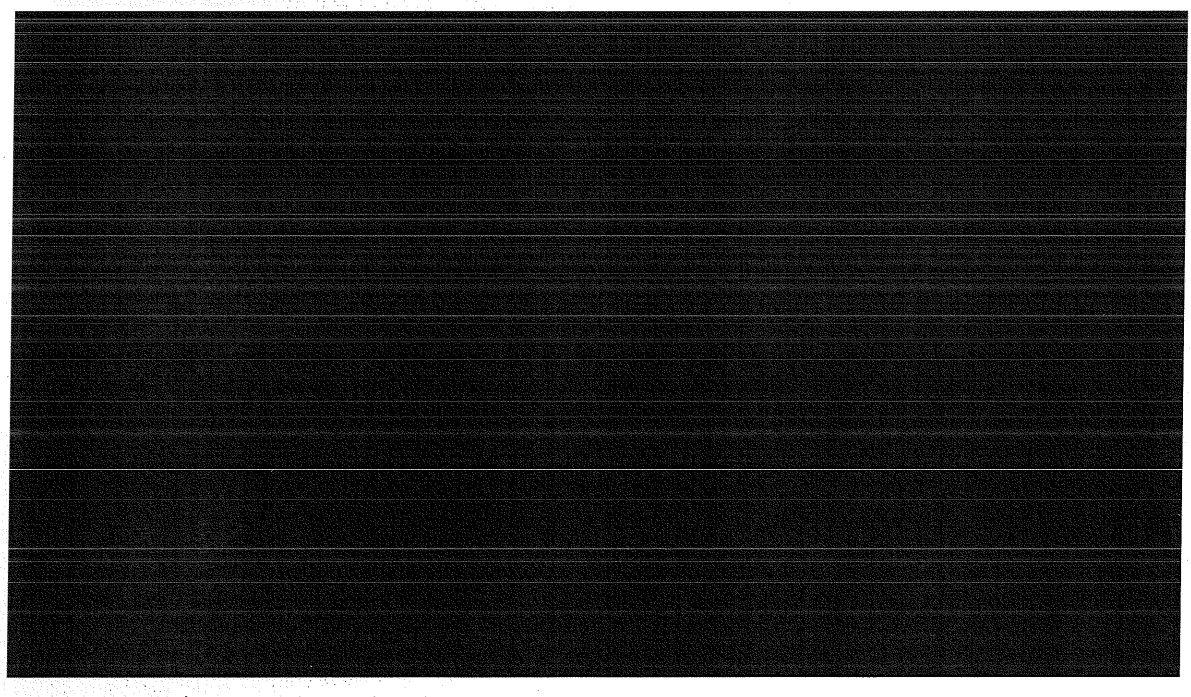


Figure 5. Thermal and PTZ Camera Coverage for Towers 3, 4, and 5

The full zoom enhancements of the PTZ cameras can extend further, but with a higher rate of image loss as the zoom increases. Figures 3, 4, and 5 illustrate how some areas have multiple angles of view and overlapping coverage. This configuration allows PHF to utilize other cameras to temporarily cover an unprotected zone in the event of a transmission/communication failure, power failure, or a damaged camera.

[redacted]

Currently, there are six thermal and one PTZ camera that are tied into the video analytics system. The PTZ is located on Tower 4 and remains fixed looking directly at [redacted] Figure 6.

[redacted]

4. METHODOLOGY

4.1 Test Sites

The test areas within the perimeter boundary were categorized according to the Perimeter Zone Classification Method (see Appendix A). In this method, classifications are based on a combination of factors, including:

- Potential security liabilities and perceived threat levels
- Boundaries, terrain, and artificial structures
- Existing regulations and/or definitions
- Airport operations (general and commercial aviation)

4.2 Test Subjects

The Safe Skies Lead Test Engineer (LTE) performed intrusion scenarios in the field. A second Safe Skies data collector in the SOC documented system status as testing was being performed.

4.3 Test Equipment

[redacted]

[redacted]

[redacted]

4.4 Test Schedule

The operational evaluation of the PHF system was conducted November 3 – 7, 2008.

4.5 Critical Operational Issues (COI)

The COIs are the primary objectives of this evaluation. The LTE and test team created procedures and data collection processes in order to generate qualitative and/or quantitative data that can be used to address the identified COIs. Measures of Effectiveness (MOE) and Measures of Performance (MOP) were used to develop methods for gathering statistically valid quantitative data.

- **COI 1: Does the perimeter protection system effectively monitor the key locations of the AOA?**
- **COI 2: Does the perimeter protection system incorporate efficiently into PHF security operations?**

COI 1: Does the perimeter protection system effectively monitor the key locations of the AOA?	
MOE	**MOP**
1 Does the system effectively identify targets loitering or moving within detection areas?	[redacted]

[5] Suspicious Behavior in this case is classified as an event taking place outside the AOA and within close proximity to key locations. An example of suspicious behavior is people or objects loitering near the fence around the fuel farm.

[redacted]

[redacted]

COI 2: Does the perimeter protection system incorporate efficiently into PHF security operations?		
MOE	**MOP**	
1 Is the system effective in meeting the functional demands of the security operations center?	**A**	Does the system generate nuisance alarms? If so, attempt to identify the rate and conditions of the alarm.
	B	Does the system generate false alarms? If so, attempt to identify the rate and conditions of the alarm.
	C	Determine the security personnel's opinions about the features of the system?
2 Does the system possess any maintenance or use issues?	**A**	Does the exterior equipment require routine maintenance?
	B	Does the interior equipment require routine maintenance?
	C	Are there any issues related to network integration?

5. RESULTS

5.1 COI 1

This COI addresses the effectiveness of the system to automatically monitor locations for targets/threats or suspicious activities.

[redacted]

[redacted]

[redacted]

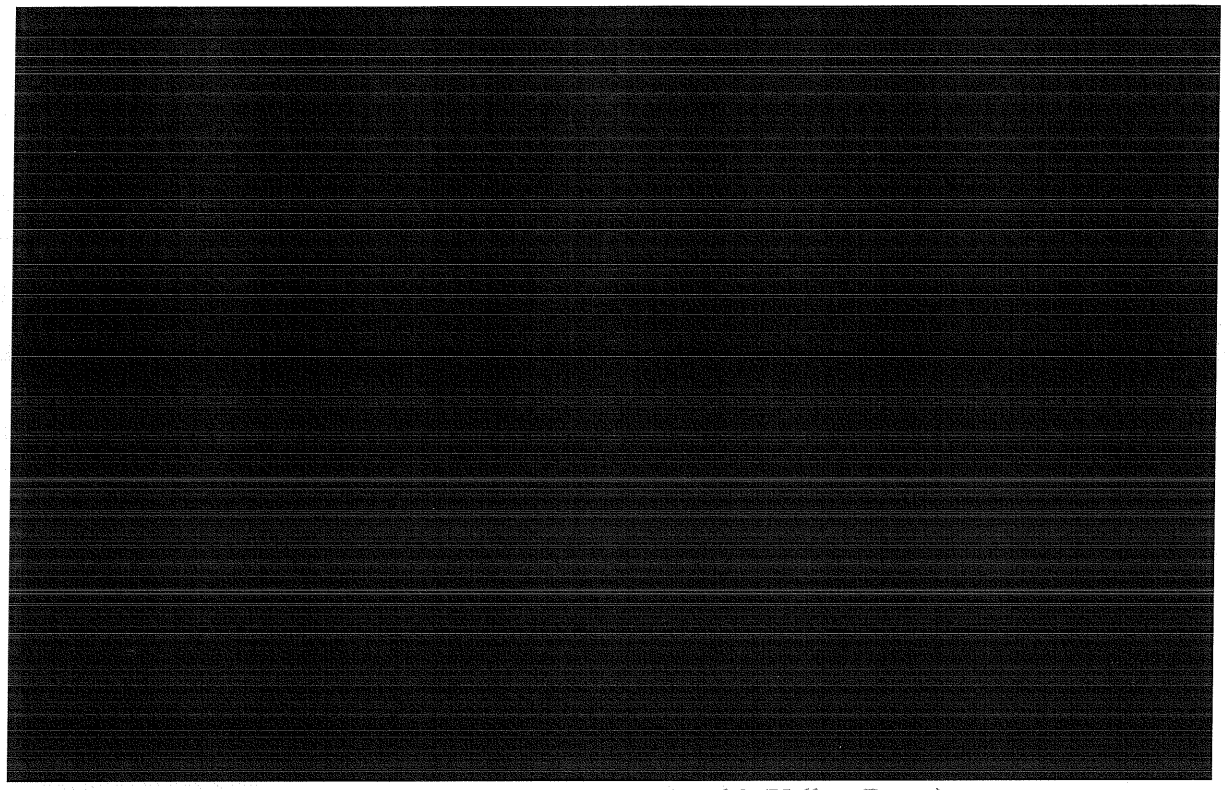


Figure 7. Tactical Paths at Towers 1 and 2 (Yellow Boxes)

[redacted]

[redacted]

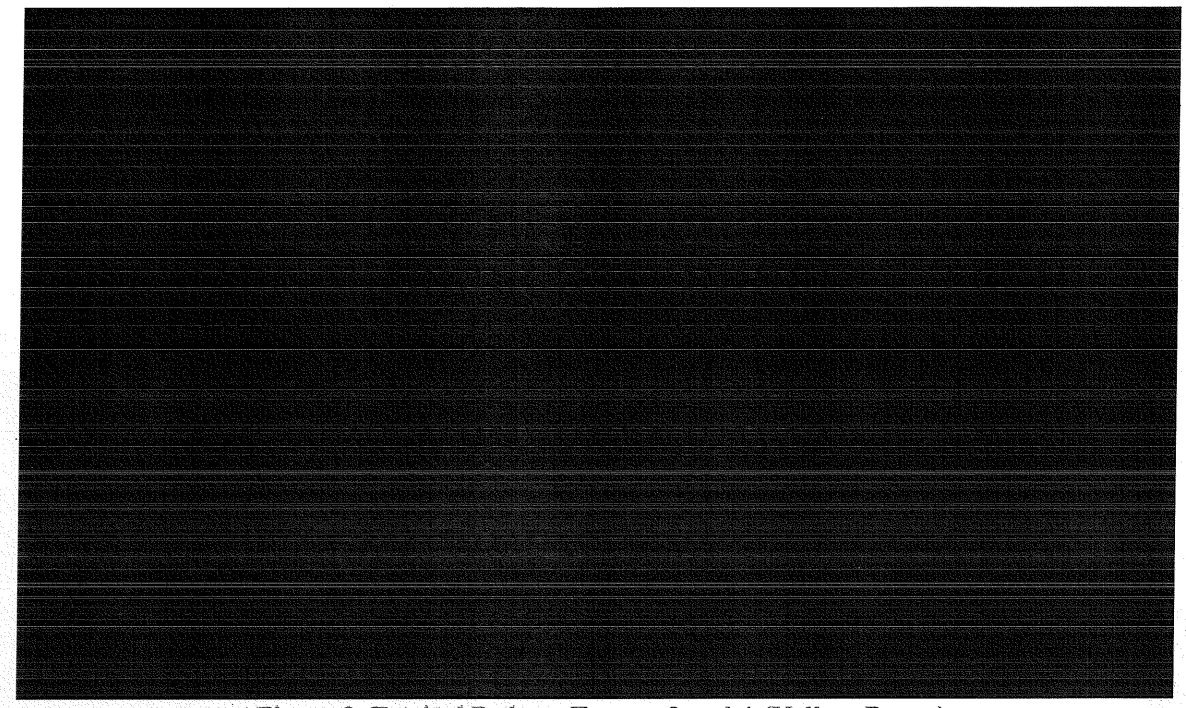
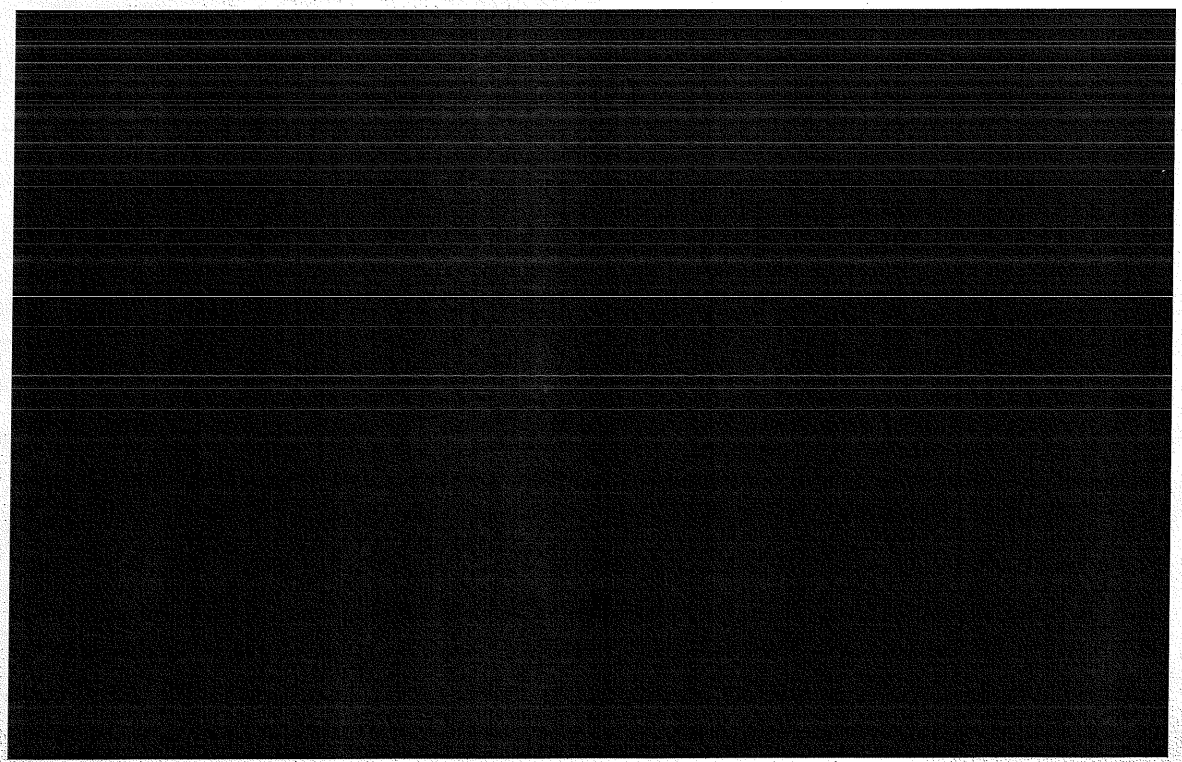


Figure 8. Tactical Paths at Towers 3 and 4 (Yellow Boxes)



[redacted]

[redacted]

5.1.1 MOE 1.1

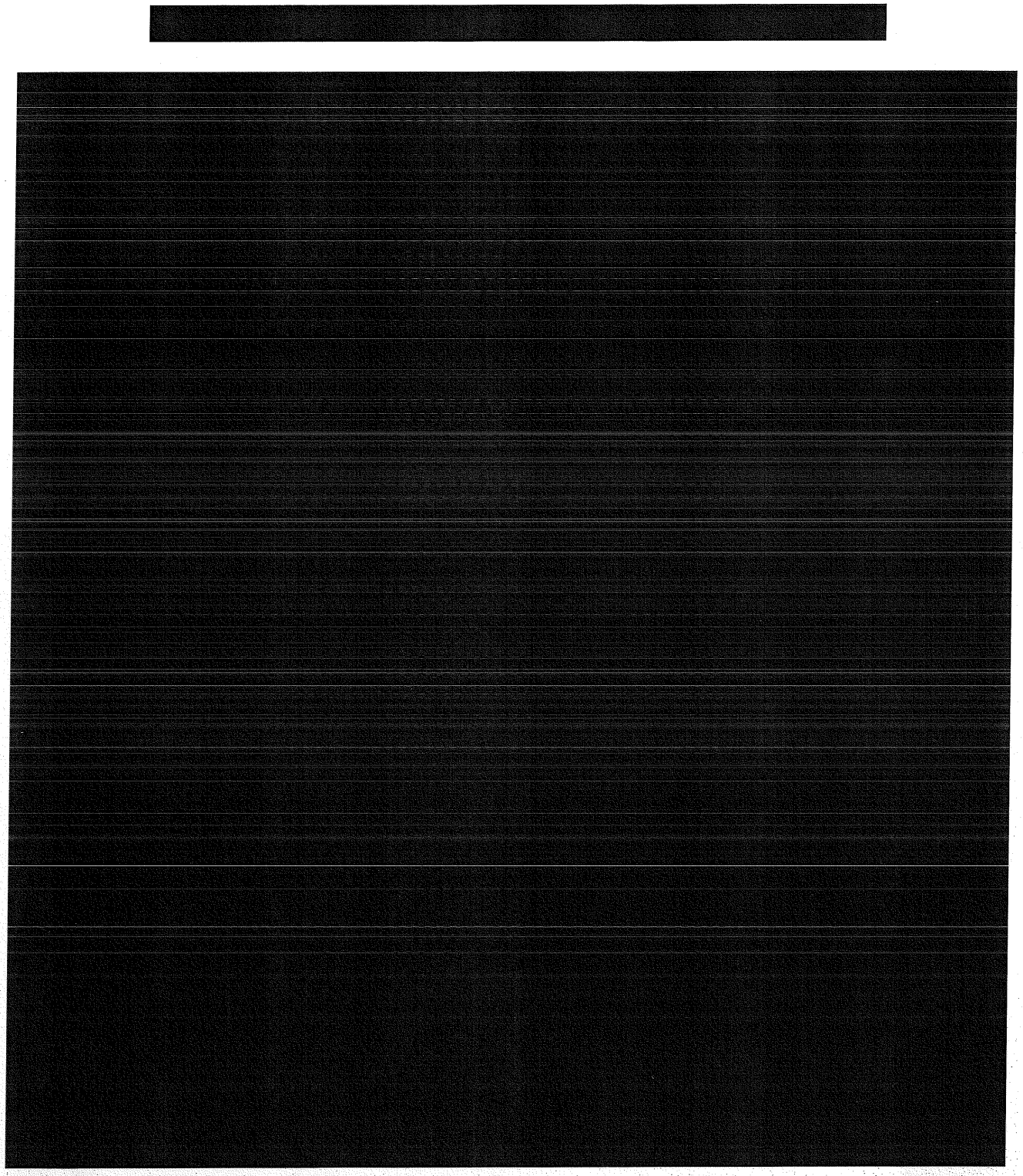
This measure is designed to determine the system's effectiveness in identifying targets within the detection areas. Test subjects were used to determine whether the system could correctly identify

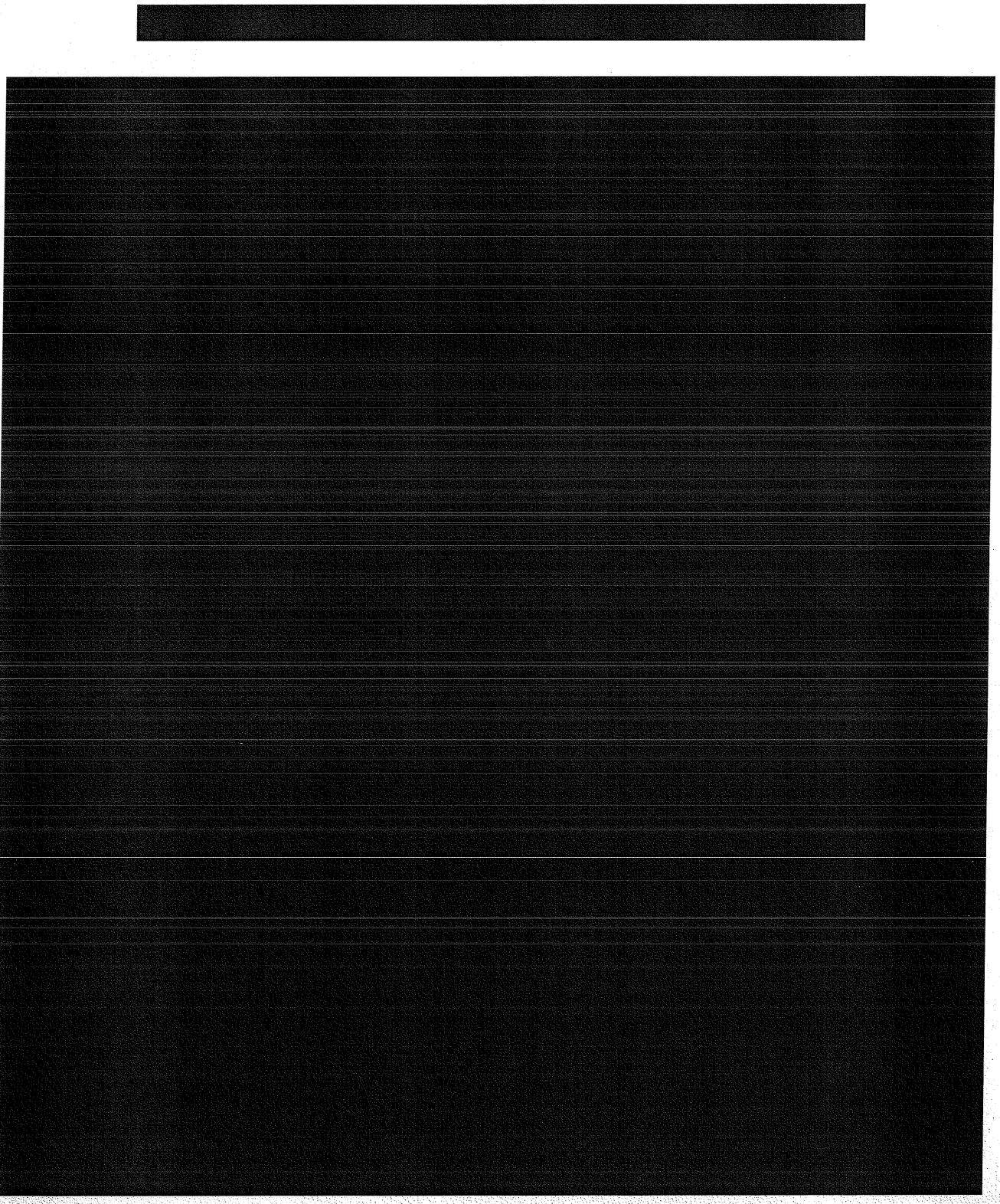
[redacted]

5.1.1.1 MOP 1.1A

[redacted]

[redacted]





[redacted]

[redacted]

5.2 COI 2

This COI addresses the functionality of the system as it pertains to the efficiency of the PHF SOC.

5.2.1 MOE 2.1

This MOE was designed to determine the effectiveness of the system in meeting the functional demands of the PHF SOC. The SOC is typically staffed by a single person during a regular shift; the system should be set up to minimize nuisance or false alarms that may cause a strain on personnel resources.

[redacted]

[redacted]

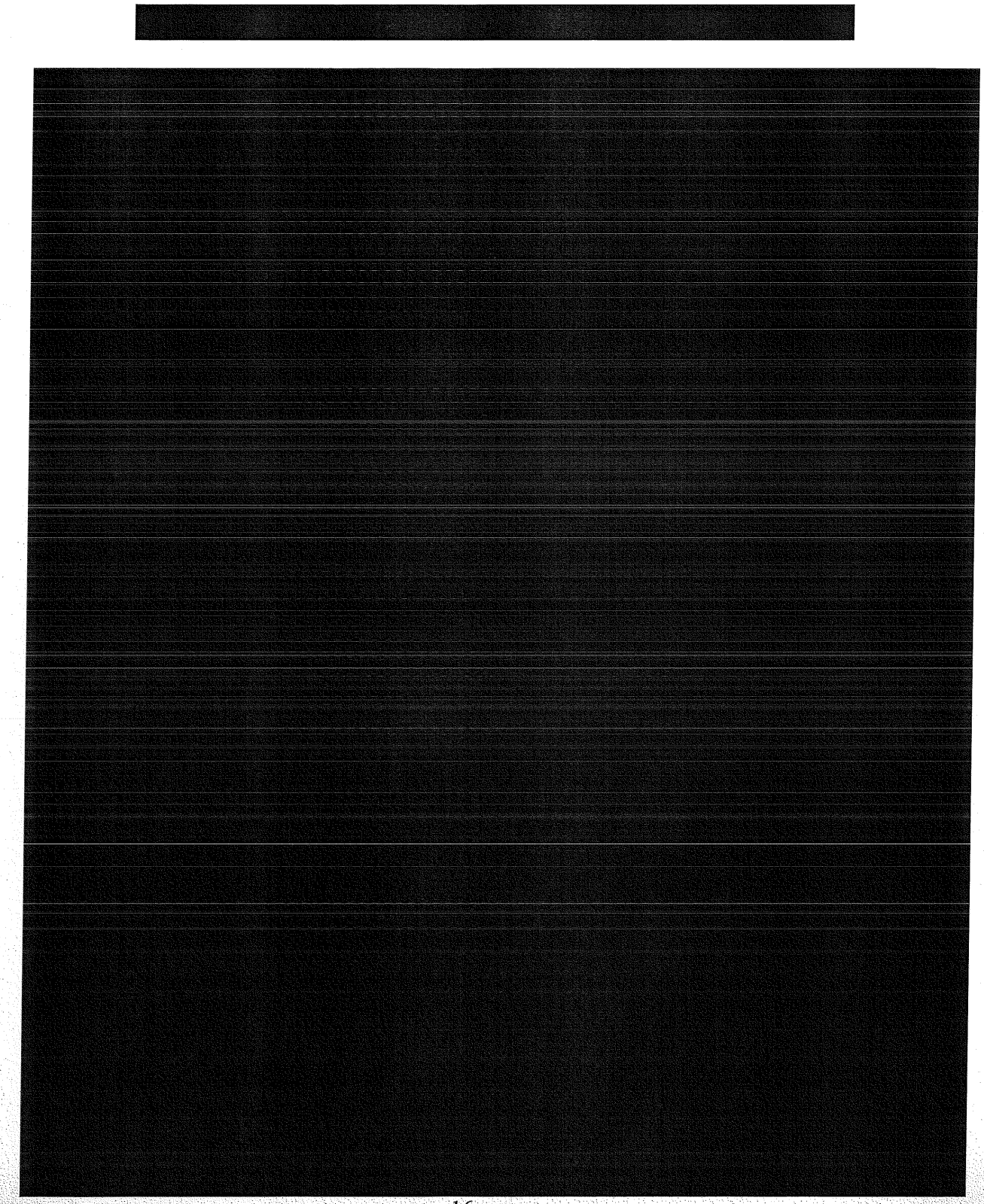
[redacted]

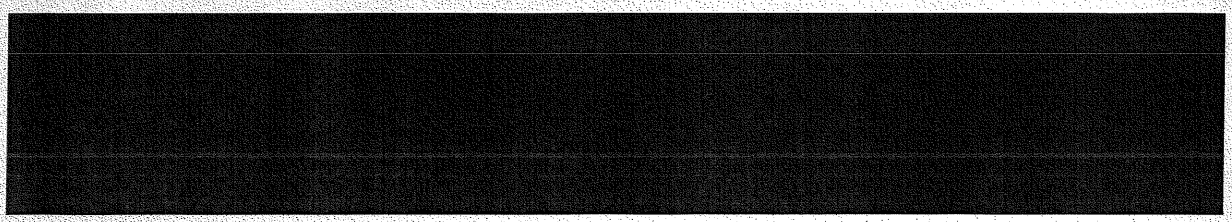
5.2.2 MOE 2.2

This measure is designed to determine the maintenance and usage requirements that are necessary to maintain continuous operation of the new system and components.

[redacted]

[redacted]





[redacted]

6. REFERENCES

NIST (2006). *NIST/SEMATECH e-Handbook of Statistical Methods*, http://www.itl.nist.gov/div898/handbook/, January 07, 2009.

SAS Institute, Inc. (2008). *Documentation for SAS ® 9.2 Products.* http://support.sas.com/cdlsearch?ct=80000, January 07, 2009.

Simonoff, Jeffery S. (2003). *Analyzing Categorical Data.* New York: Springer-Verlag.

[redacted]

[redacted]

APPENDIX A – PERIMETER ZONE CLASSIFICATION METHOD

[redacted]

[redacted]

The Perimeter Zone Classification Method was designed to provide a consistent guide that any airport could use to identify critical infrastructures, liabilities, and overall weaknesses in perimeter security quickly and easily. Zone definitions are based on several factors including:

- Security liabilities and perceived threat levels
- Boundaries, terrain, and artificial structures
- Existing regulations and definitions
- Airport operations (general and commercial aviation)

[redacted]

[redacted]

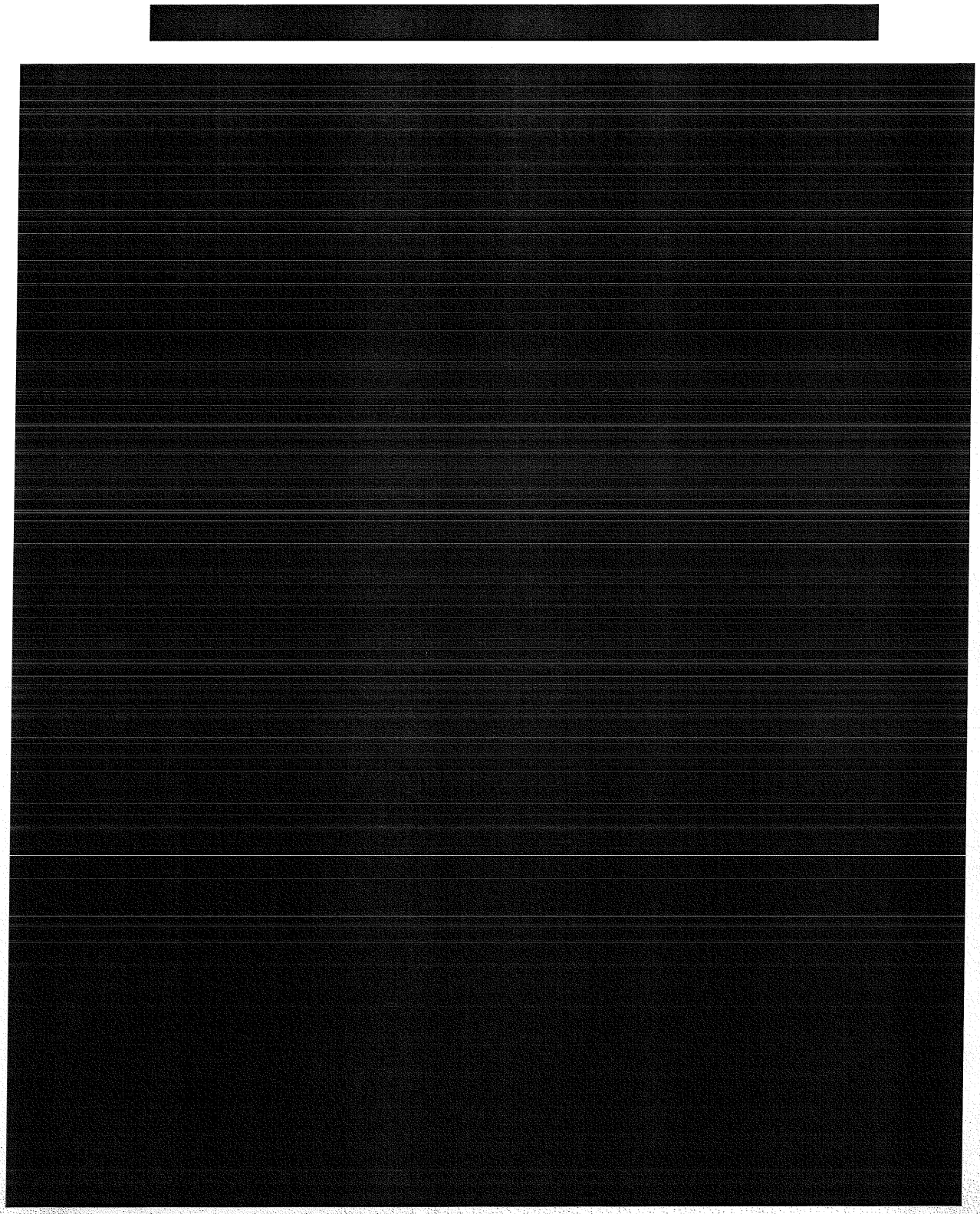
[redacted]

Restricted Zones (RZ)

Typical Restricted Zones (RZ) are those in which some form of biometric or identification verification method is required for entry or performing operational tasks. These areas are vital to airport operations and pose the highest probability of generating short- and long-term collateral damage in the event of a catastrophic event. Examples of areas that fall into this category are:

[redacted]

[redacted]



[redacted]

Outer Zone (OZ)

The OZ, an indefinable area that can be any size and shape, is the area that lies between the SZ and the BZ. It can be superseded by all other zones, but can only be adjacent to SZs and BZs. At no point can the OZ be in direct contact with a TARZ, RZ, or perimeter barrier.

Four areas in Figure 10 are classified as OZ; each area is variable in size and conforms to the shapes of the superseding zones.

[redacted]

[redacted]

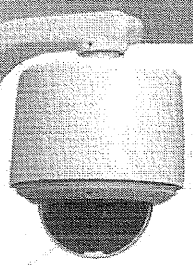
APPENDIX B – VICONNET SURVEYOR VFT-M CAMERA DOME TECHNICAL SPECIFICATIONS

[redacted]

VICON NET
IP Video Solutions

SurveyorVFT-M

Impact-Resistant Camera Dome Series



- **Metal housing and polycarbonate lower dome protect camera from impact and vandalism**
- **RS-422/485 or coaxial PTZ control; available with TCP/IP, fiber and UTP transmission card options**
- **Compatible with all Vicon SVFT mounts**
- **Lowest current draw in its class**
- **Versions available with high-resolution color 22X or day/night 23X or 35X**

The rugged SurveyorVFT-M Series of impact-resistant maximum security domes provides surveillance coverage in environments where it's needed most. Built to withstand vandalism and tampering, the SurveyorVFT-M Camera Domes include a camera, pan/tilt drive, receiver and CPU-based electronics all enclosed in a metal housing with an impact-resistant polycarbonate lower dome. The attractive, yet covertly rugged enclosure boasts an impressive IP-66 rating.

The basic SVFT-M model provides video transmission over standard coaxial cable. In addition, interface boards are available to expand transmission options to include TCP/IP (using the ViconNet® platform), fiber-optic transmission or twisted-pair (UTP). Compatible with Vicon's line of SurveyorVFT mounting equipment, the SVFT-M Series is ideal for any security installation where even the cameras require that extra level of protection.

World Headquarters
Hauppauge, New York
631-952-CCTV (2288)
800-645-9116

European Headquarters
Fareham, PO 15 5TX
United Kingdom
+44 (0) 1489 566300

Brussels Office
Zaventem
Belgium
+32 (2) 712-8750

Hong Kong Office
Shatin
New Territories
852-2745-7116

VICON

Specification Overview

Model Number	Product Code	Camera Type/Format	Optical Zoom/Total Zoom
SVFT-M22/ SVFT-M22C	8747/8747-01	Color NTSC/PAL	22x/264x
SVFT-M22E/SVFT-M22EC	8748/8748-01	Color with ExView Technology NTSC/PAL	22x/264x
SVFT-M23/SVFT-M23C	8749/8749-01	Color (Day/Night with Wide Dynamic Range) NTSC/PAL	23x/276x
SVFT-M35/SVFT-M35C	9104/9104-01	Color (Day/Night with Wide Dynamic Range and Image Stabalization) NTSC/PAL	35x/420x

For ViconNet version 3 option, add -25 (-26 PAL) to the product code; Fiber Optic option, add -30 (-31) to the product code; for UTP (T) option, add -40 (-41) to the product code.

[redacted]

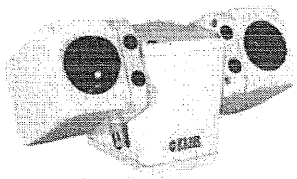
APPENDIX C – FLIR PATROLIR TECHNICAL SPECIFICATIONS

[redacted]

[redacted]

LAW ENFORCEMENT





FLIR PatrolIR and PatrolIR PRO

Versatile, low-cost thermal imagers for law enforcement vehicle applications

FLIR's new PatrolIR is a new, low cost, thermal imager engineered for law enforcement vehicle applications. Thermal imaging is a powerful tool in law enforcement because suspects can't hide their heat, and since it's passive, suspects don't know they are being watched. There are three versions of the PatrolIR; a fixed version designed for integration onto existing pan and tilt devices, a pan and tilt version that accommodates 360° surveillance, and the PRO version which includes a powerful lowlight camera for long range surveillance when lighting conditions permit.

Feature	Benefit
• **State of the art thermal imaging technology**	See suspects and activity in total darkness without revealing your position using the same technology as the US Military
• **Requires no illumination**	Thermal imaging is a passive technology, so suspects don't know that you can see them
• **High sensitivity detector**	Reveals subtle temperature differences, making it difficult for suspects to camouflage their heat signature
• **320 x 240 resolution**	4x the resolution of most competing systems, with superior range performance and image quality
• **Compact panning enclosure**	Easily scan a 360° area from the safety of your vehicle
• **Fully automatic image optimization**	Requires no manipulation or adjustment to get high contrast imagery
• **It's all FLIR inside**	FLIR's military-quality products are built to endure, and have been patrolling the skies with airborne law enforcement since the 1980's

Applications:

- **Vehicle Based Surveillance**
- **Searches**
- **Security**
- **Patrol**


FLIR

[redacted]

LAW ENFORCEMENT

PatrolIR	Static Version	Pan/Tilt Version	PRO Version
Thermal Imaging Performance			
Sensor type	320 x 240 Microbolometer	320 x 240 Microbolometer	320 x 240 Microbolometer
Field of View	35° H x 27° V	35° H x 27° V	14° H x 10° V
Spectral band	7.5 - 13.5 µm	7.5 - 13.5 µm	7.5 - 13.5 µm
Pan-Tilt Azimuth Range	-	+ / - 190°	+ / - 200°, 1-180° /sec
Pan-Tilt Elevation Range	-	+/-45	+ / - 60°, 1-60° /sec
Video	NTSC or PAL Video	NTSC or PAL Video	NTSC or PAL Video
Connector types	BNC at primary cable end	BNC at primary cable end	Proprietary connector
Daylight Imaging Performance			
Sensor type	-	-	Sony 960 Block Camera with 1/4 in. CCD
Resolution	-	-	>850,000 (NTSC); >800,000 (PAL) pixels
Optical zoom	-	-	(26x) 42° to 1.6° Continuous
E Zoom	-	-	10x, Continuous
Power			
Power Requirements	12 VDC	12 VDC	24 VDC
Power Consumption	3 W nominal, 50 W (max)	5 W nominal, 30 W (max)	<50W nominal at 25 °C
Power Cable Length	15 feet	15 feet	40 feet
Environmental			
IP Rating	IP X5	IP X5	IP X5
Operating Temp	-20°C to 55°C	-20°C to 55°C	-32°C to 55°C
Storage Temp	-50°C to 80°C	-50°C to 80°C	-50°C to 80°C
Dimensions and Weight			
Dimensions	7.3" x 4.0" x 6" (L x W x H)	7.3" x 4.0" x 10" (L x W x H)	12" D x 9" H
Camera Weight	7 lb	10 lb	<11 lb.

Specifications subject to change

FLIR Systems, Inc.
CVS World Headquarters

FLIR SYSTEMS, INC.
70 Castilian Dr.
Goleta, CA 93117
USA
PH: + 1 877 773 3547
PH: + 1 805 964 9797
FX: + 1 805 685 2711

EUROPE
CVS Eurasian Headquarters

FLIR SYSTEMS CVS BV
Charles Petitweg 21
4847 NW Teteringen - Breda
Netherlands
PH: +31 (0) 765 79 41 94
FX: +31 (0) 765 79 41 99
flir@flir.com

FLIR Systems, Inc.
Corporate Headquarters

FLIR SYSTEMS, INC.
27700A SW Parkway Ave.
Wilsonville, OR 97070
USA
PH: + 1 877 773 3547
FX: + 1 503 498 3804
sales@flir.com

www.flir.com

FLIR

[redacted]

APPENDIX D – VICON KOLLECTOR ELITE XG DVR TECHNICAL SPECIFICATIONS

[redacted]

VICON

Corporate Headquarters
[redacted]
Syosset, New York 11791
631-952-CCTV (2288)
800-645-9116
Fax 631-364-2385

Vicon Europe Headquarters
[redacted]
Farnham, GU9 8TV
United Kingdom
+44 (0) 1483 538300
Fax +44 (0) 1483 538333

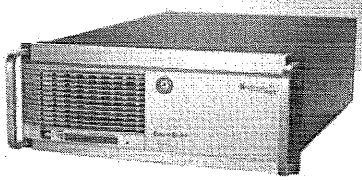
Germany
[redacted]
+49 (0) 4921 8738
Fax +49 (0) 4921 87377

Far East Office
[redacted]
Hong Kong
(852) 2145 7117
Fax (852) 2145 7177

www.vicon-cctv.com

KOLLECTOR ELITE XG

16-CHANNEL HYBRID DIGITAL NETWORK VIDEO RECORDER AND WORKSTATION



Premium Kollector model provides the ability to view, record, operate and configure all units within a ViconNet system

- Powered by ViconNet software
- Compatible with Virtual Matrix Controller
- Uses ViconNet MPEG-4 compression to optimize data and maximize picture quality
- Simultaneously records and transmits up to 16 digital video channels
- Macros for programming, recording, alarm and display events
- Geographic mapping and control GUI
- Logical camera groups
- System updates over the network
- 8 alarm output relays
- High-resolution image quality 720 x 488 (4 CIF or D1)
- Flexible frame-per-second settings; view video at one fps while recording at another

Kollector™ Elite XG, Vicon's top of the line DVR, is a true workhorse. Combined with ViconNet® Version 4.0, the line of Kollector Elite XG Hybrid Digital Network Video Recorders have evolved beyond ordinary DVR design. With the full ViconNet software suite that includes geographical map control and an active 4-output analog matrix, these units are now unrivaled as a total system control station, capable of viewing, controlling and configuring every ViconNet NVR/DVR and IP device on the network. Use them as the centerpiece of smaller, single location systems or as part of enterprise scale ViconNet solutions.

As with all Kollector models, the Elite XG allows for integration between your ViconNet system and solutions from industry leaders in access control and video analytics. Enjoy the benefits and efficiencies of controlling all security operations from a unified system. The Elite also provides seamless support of PTZ cameras via the back panel.

As a DVR, Kollector Elite XG is Vicon's premium recorder, capable of 120, 240, or 480 fps with storage configurations that range up to 3 TB internally and up to 10 TB with optional external RAIDs. Models available with internal RAID.

VICON NET

[redacted]

APPENDIX E – GE VIDEOIQ TECHNICAL SPECIFICATIONS

[redacted]

GE Infrastructure
Security

By accurately detecting human activity, **VideoIQ** can help security teams identify potential threats more quickly and minimize false alarms caused by non-human movement. VideoIQ shows both alarms and associated video, and works even in challenging outdoor environments.

VideoIQ is an eight-camera, PC-based system that can identify human movement with high accuracy and sound an alarm.

When VideoIQ is running, active regions of interest are displayed on the Live Video screen of the VideoIQ monitor. Humans moving within the region are identified with a red bounding box. All other moving objects are marked with yellow bounding boxes for easy identification.

The technology behind VideoIQ works by separating objects from a camera image into foreground and background elements. After the separation from the foreground elements, VideoIQ ignores dynamic background motion such as moving tree branches and rippling water.

By continually building a database of object characteristics, VideoIQ can identify one object from another. VideoIQ can then distinguish these objects across the eight-camera system.

The system's robustness is unaffected by adverse conditions such as dynamic backgrounds, poor scene illumination, inclement weather, transient light conditions, and poor quality video sources.

VideoIQ continues to learn after installation. New objects can be analyzed and identified without operator intervention.

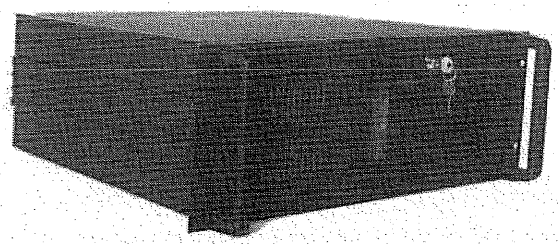
The VideoIQ unit can either stand alone or be integrated with a GE Security DVMRe.

Features

- Video-based human detection system that provides both alarms and associated video
- Detects humans in dynamic outdoor environments
- Distinguishes between humans and other moving objects
- Ignores dynamic background motion and focuses on foreground objects of interest
- NTSC and PAL compatible
- Eight-channel, PC-based system that integrates with existing DVMRe systems (5.02 or higher)
- Eight individual alarm outputs with programmable duration

VideoIQ

Human detection surveillance technology



Specifications

Americas
503-885-5700
888-GE-SECURITY
(437-3287)
faxback 800-483-2495
info@gesecurity.com
www.gesecurity.com

Asia
tel 852-2907-8108
fax 852-2142-5063

Australia
tel 61-3-9259-4700
fax 61-3-9259-4799

Europe
tel 32-2-725-11-20
fax 32-2-721-86-13

Latin America
tel 305-593-4301
fax 305-267-4300

PC
- CPU: 3.2 GHz
- RAM: 512 MB
- Hard disk drive: 80GB EIDE
- Internal drive: Floppy drive, CD-ROM
- Ports: DB-9 male RS-232 port; VGA port
- Monitor VGA (optional): 15-in. LCD flat panel monitor
- Operating system: Windows XP Professional and VideoIQ application
- Power: 100 to 250 VAC, 50/60 Hz
- Power consumption: 350 W

Inputs
- Video inputs: 8
- Video format: NTSC or PAL

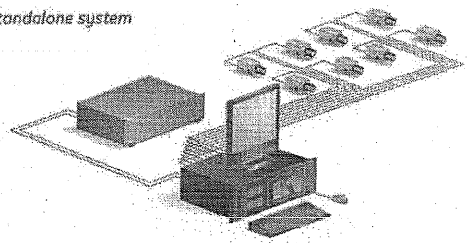
Outputs
- Video output: 1 VGA
- Alarm output: 8 TTL levels
- Alarm I/O levels: Active high or low, selectable

Physical and Environmental
- Dimensions (WxHxD): 19.0 x 7.0 x 17.7 in. (441 x 177 x 450 mm)
- Weight: 32.5 lb (16 kg)
- Operating temperature: 32 to 133°F (0 to 55°C)

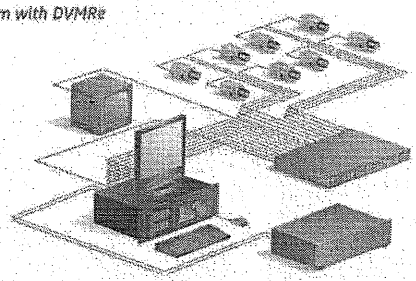
Connections
- RS-232: 10-ft. DB-9 (female) to DB-9 (female) null modem
- I/O Board for alarm output

Compatible Digital Video Multiplexers and Recorders
- DVMRe multiplexer/recorder: Version 5.02 or higher

Standalone system



System with DVMRe



Ordering information

VIQ-8HD	8-channel human object detector (PC, monitor, VIQ software, RS-232 cable, alarm I/O board)
VIQ-8HDX	8-channel human object detector (PC, VIQ software, RS-232 cable, alarm I/O board)

[redacted]

APPENDIX F – NEXTIVA S3100 WIRELESS TECHNICAL SPECIFICATIONS

[redacted]

VERINT
POWERING ACTIONABLE INTELLIGENCE

Nextiva

S3100

Multi-Band Outdoor Wireless Bridge/Access Point/Repeater

The Nextiva™ S3100 is a versatile outdoor wireless solution designed for a wide range of applications and operating environments:

Wireless Bridge: Two S3100 devices can be used to form a wireless bridge between two LANs when a wired connection is not available or too costly to install.

Wireless Access Point: The S3100 may be used as a wireless access point to aggregate traffic from multiple Nextiva S1100w wireless transmitters in point-to-multipoint applications.

Repeater: Two S3100 units may be used as a range extender for wireless links; that is, when a device is needed to retransmit signals from Nextiva wireless products to a wired LAN. This is especially useful in long-distance deployments or when transmitting around RF path obstructions.

Reliability, Manageability, Performance

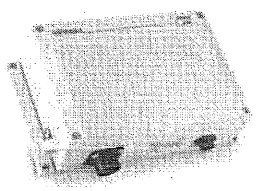
Optimized for video transmission over license-free wireless bands, the S3100 enables organizations to transmit images from virtually anywhere with high reliability. A proprietary Verint polling protocol resolves Wi-Fi "hidden node" and quality of service problems when using conventional 802.11 products, with no degradation in video signal quality over extended range transmissions. SSL-based authentication and AES encryption with rotating 128-bit key enable a high level of security during wireless video transmission.

Nextiva Wireless Solutions: Leading the Industry in Innovation and Value

The S3100 is part of the Nextiva portfolio of intelligent wireless edge devices, which lead the industry in innovation and value. Built on accepted industry standards, these intelligent edge devices are designed for high availability, easy interoperability with IT infrastructure and video equipment, and superior performance.

Key Features

- Supports video transmission over license-free 2.4 and 5 GHz wireless bands
- Versatile solution for use as wireless access point, wireless bridge, or repeater
- SSL-based authentication and AES encryption
- Compact, weatherproof enclosure for outdoor use
- Autosensing serial ports for device connectivity
- Resolves hidden node and quality of service issues
- Automated configuration, health monitoring, and diagnostics with Nextiva



[redacted]

APPENDIX G – NEXTIVA S1100W VIDEO ENCODER & WIRELESS TRANSMITTER TECHNICAL SPECIFICATIONS

[redacted]

[redacted]

VERINT

Nextiva

S1100w

Video Encoder and Wireless Transmitter

The Nextiva™ S1100w combines video encoding and wireless transmission in a single, compact device, enabling organizations to transmit images from virtually anywhere with high reliability, superior scalability, and lower operational costs.

The S1100w digitizes video from analog cameras and transmits it over license-free, wireless bands. Auto-sensing serial ports connect the S1100w to motorized domes, PTZ cameras, and other asynchronous serial devices. SSL-based authentication helps secure configuration access, and AES encryption with rotating 128-bit key enables a high level of security during wireless video transmission. And, dual streaming allows video to be viewed at high resolution for superior clarity, yet recorded at lower frame rates to reduce data transport and storage requirements.

Two wireless modes of operation are supported:

- Nextiva proprietary SPCF/SDCF protocol (optimized for video surveillance data)
- The standard 802.11a/g protocol and WPA2 personal and enterprise security standards, which allow interoperability with most commercial and mesh access points that are compliant with the 802.11a/g and WPA2 standards

Cost-Effective Deployment Virtually *Anywhere*

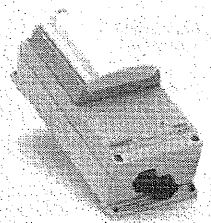
When paired with the Nextiva S3100 wireless access point, the S1100w provides a powerful point-to-multipoint wireless solution. With state-of-the-art wireless technology and a compact, weatherproof enclosure, the S1100w can be cost-effectively deployed wherever it is needed—from parking lots and perimeters to city-wide implementations and waterways. By eliminating the need to install separate encoders and wireless units, the S1100w decreases installation, equipment, and maintenance costs, speeds deployment, and reduces power and space requirements.

Nextiva Wireless Solutions: Leading the Industry in Innovation and Value

The S1100w is part of the Nextiva portfolio of intelligent wireless edge devices. These devices integrate radios, encoders, and antennae in small, NEMA-rated enclosures for secure, reliable operation in real-world video applications. Built on accepted industry standards, Nextiva intelligent edge devices are designed for high availability, easy interoperability, and superior performance.

Key Features

- Video encoding and wireless transmission over license-free 2.4 and 5 GHz bands
- Dual-stream, MPEG-4 based video up to 4CIF, 30 FPS, depending on the operating environment
- WPA2, SSL-based authentication and AES encryption
- Compact, weatherproof enclosure for outdoor use
- Auto-sensing serial ports for device connectivity
- Automated configuration, health monitoring, and diagnostics with Nextiva



[redacted]

[redacted]

NETWORK	
RF Interface	Nextiva SPECTRASOFT 802.11a/802.11g PHY with proprietary MAC protocol mode or 802.11a/802.11g with WPA2 standard compliant mode
Frequency	2.402-2.4835 GHz (ISM) 5.250-5.350 GHz (U-NII-2) 5.470-5.725 GHz (DFS) 5.725-5.825 GHz (U-NII-3/ISM)
Modulation	OFDM
Max. Output Power	2.4G-2.4835 GHz: 19 dBm 5.x GHz: 18 dBm
System Gain	2.402-2.4835 GHz with 8.5 dBi gain antenna: 128 dB 2.402-2.4835 GHz with 16 dBi gain antenna: 141 dB 5.250-5.350 GHz with 13 dBi gain antenna: 131 dB 5.250-5.350 GHz with 18 dBi gain antenna: 136 dB 5.725-5.825 GHz with 13 dBi gain antenna: 132 dB 5.725-5.825 GHz with 18 dBi gain antenna: 142 dB
Range (RF Line of Sight)	2.402-2.4835 GHz (8.5 dBi): up to 3.9 miles (6.3 km) 2.402-2.4835 GHz (16 dBi): up to 11.4 miles (18.3 km) 5.250-5.350 GHz (13 dBi): up to 2.2 miles (3.2 km) 5.250-5.350 GHz (18 dBi): up to 5.3 miles (8.5 km) 5.725-5.825 GHz (13 dBi): up to 3.3 miles (5.3 km) 5.725-5.825 GHz (18 dBi): up to 6.2 miles (10 km)
Data Rate (Max Burst Rate)	6, 9, 12, 18, 24, 36, 48, and 54 Mbps
Channel	2.4 GHz: 11 5.3 GHz: 4, non-interfering 5.4 GHz: 11, non-interfering (DFS) 5.8 GHz: 5, non-interfering
Encryption	128-bit AES with auto key rotation, WPA2, WEP
Protocols	RTP/IP, UDP/IP, TCP/IP, or multicast IP, DNS and DHCP client
VIDEO	
Input	1 composite, 1 Vpp into 75 ohms (NTSC/PAL)
Compression	Proprietary MPEG-4 based (480 lines resolution) MPEG ISO 14496-2 Simple Profile (480 lines resolution)
Frame Rate	1-30 FPS programmable (up to 60 fields per second)
ALARM AND AUDIO	
Alarm	Input: 2 dry contacts (1 mA max.) Output: 1 relay contact (up to 48V at 100 mA)
Bi-Directional Audio	Input: 0 dBm into 600 ohms / Output: -8 dBm into 600 ohms
SERIAL PORT	
Electrical Levels	Autolevel sensing RS-232 or RS-422/485
Operating Mode	Transparent (supports any asynchronous PTZ serial protocol)
POWER	
Input Voltage	24V AC +/- 10% (optional 12V DC +/- 10%)
Consumption	12W (1.0 A at 12V DC) 28 VA at 24V AC
PHYSICAL	
Enclosure	NEMA 4X/IP 66 powder coat painted die cast aluminum with wall-mount brackets
Size	9.0L x 3.9W x 3.8H in. (230L x 100W x 96H mm)
Weight	2.6 lbs (1.2 kg)
Environment	22°F to 122°F (-30°C to 50°C)
Humidity	Humidity 100% at 122°F (50°C)
MANAGEMENT	
Configuration	Remote: via Verint Nextiva, nDVR™, Loronix Video Manager™, SiConfigurator, or Telnet Local: via the serial port using any ASCII terminal
Firmware Upgrade	Flash memory for upgrade of video codec and application firmware over the network
CERTIFICATIONS	
USA	RoHS compliant FCC CFR47 part 15 (15.247, subparts B, C and E)
Canada	Industry Canada RSS-210, RSS-139, and ICES-003
WARRANTY	2-year limited warranty, covering parts and labor

Note: All transmitters come with 9-pin cables for video, data, and power and wall-mount and pole mount brackets. Cat-5e cable for audio sold separately.

Verint.
Powering Actionable Intelligence.®

Verint® Systems Inc. is a leading global provider of analytic software-based solutions for security and business intelligence. Verint solutions help organizations make sense of the vast voice, video, and data available to them, transforming this information into *actionable intelligence* for better decisions and highly effective performance.

Since 1994, Verint has been committed to developing innovative solutions that help global organizations achieve their most important objectives. Today, organizations in over 50 countries use Verint solutions to enhance security, boost operational efficiency, and fuel profitability.

videoinfo@verint.com
1-866-NEXTIVA
www.verint.com/videosolutions
330 South Service Road
Melville, NY 11747 USA

June 2007
VINE0206070

[redacted]

[redacted]

APPENDIX H – NEXTIVA 1970E-R DECODER TECHNICAL SPECIFICATIONS

[redacted]

[redacted]

VERINT

Nextiva

S1970e-R

Compact Decoder for Single, Quad, or Guard Tour Display

The Nextiva™ S1970e-R is a highly compact, single-output decoder that helps organizations leverage the power of IP-based digital video without sacrificing investments in analog technology.

Designed to deliver DVD-quality video to analog monitors, this powerful edge device lets users view video from a single camera or view up to four video streams in quad or guard tour viewing mode. Additionally, users can determine how cameras are sequenced during guard tour viewing, to address the specific security challenges of various environments and situations.

Easy to Configure and Manage

The S1970e-R is built on accepted industry standards for easy interoperability with existing IT infrastructure and video equipment.

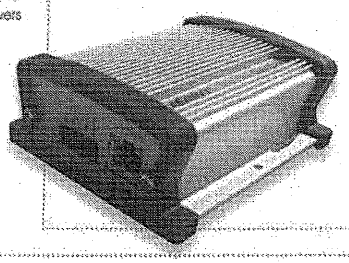
Nextiva Control Center, an easy-to-use management portal, simplifies deployment and enables configuration and administration of the S1970e-R from a single location and application. The S1970e-R can also be configured and managed using Verint® nDVR™ or Loronix Video Manager™.

Nextiva HealthCheck™ continuously monitors the performance of the S1970e-R, with automated diagnostics and problem correction for greater uptime and lower service costs.

Part of the Nextiva portfolio of Intelligent Edge Devices, the S1970e-R adds value to existing investments and delivers superior functionality, flexibility, and value.

Key Features

- Highly compact decoder that delivers DVD-quality video to analog monitors
- Single, quad, or guard tour display
- 4CIF video output at 30 FPS for 1 video stream; CIF video output at 30 FPS for 4 video streams
- SSH-based authentication
- RS422/485 serial port to support keyboard control for PTZ cameras
- Standards based and firmware upgradeable
- Automated configuration, health monitoring, and diagnostics with Nextiva



[redacted]

Technical Specifications

NETWORK	
Interface	Ethernet 10/100Base-T
Connector	RJ-45 jack
Protocols	Transport: RTP/IP, UDP/IP, TCP/IP, or multicast IP Others: DNS and DHCP client
Security	SSL-based authentication
VIDEO	
Output	1 composite, 1 Vpp into 75 ohms (NTSC/PAL)
Connector	BNC female
Compression	MPEG-4 SP
Resolution	Scalable from 176x128 to 704x480 pixels NTSC and 176x144 to 704x576 pixels PAL
Frame Rate	1-30 FPS programmable (full motion)
Bandwidth	Configurable 30 Kbps to 6 Mbps
ALARM AND AUDIO	
Alarm	Input: 1 dry contact Output: 1 relay contact (48V AC/DC at 100 mA max)
Bi-Directional Audio	Input: -46 to -3 dBV into 35-10kΩ (line or microphone input) Output: -46 to -3 dBV into 8 ohms min
Audio Connectors	0.14 in. (3.5 mm) stereo jacks
SERIAL PORT	
Electrical Levels	RS422/485 2/4-wires
Connector	5-position terminal strip
Operating Mode	Transparent serial port supporting any asynchronous serial protocol
POWER	
Supply Voltage	12VDC ±10% (5 W)
PHYSICAL	
Size	4.2 x 3.5 x 1.7 in. (106 x 90 x 42 mm)
Weight	8.7 oz (248 g)
Environmental	32°F to 122°F (0°C to 50°C)
Humidity	95% non-condensing at 122°F (50°C)
MANAGEMENT	
Configuration	Verint NextIva, nDVR, Loronix Video Manager, or SConfigurator
Firmware Upgrade	Flash memory for upgrade of video codec and application firmware over the network
CERTIFICATIONS	
USA	FCC part 15 (subpart B, class A)
Canada	ICES-003/NMB-003
Europe	CE marked, EN 55022:1998 class A, EN 55024
MODELS	
S1970e-R	Compact, DVD-quality, Ethernet video server with 1 bi-directional audio channel; power supply included
S1970e-RXT	With extended temperature range (-30 to +60°C); power supply included
WARRANTY	3-year limited warranty, covering parts and labor

Verint.
Powering Actionable Intelligence.®

Verint Systems Inc. (NASDAQ: VRNT) is a leading global provider of analytic software-based solutions for security and business intelligence. Verint solutions help organizations make sense of the vast voice, video, and data available to them, transforming this information into *actionable intelligence* for better decisions and highly effective performance.

Since 1994, Verint has been committed to developing innovative solutions that help global organizations achieve their most important objectives. Today, organizations in over 50 countries use Verint solutions to: enhance security, boost operational efficiency, and fuel profitability.

info@verint.com
1-866-NEXTIVA
www.verint.com/videosolutions
330 South Service Road
Melville, NY 11747 USA

October 2006