



# Transportation Security Administration

*Office of Security Technology*

*Airport Perimeter Security Projects for FY08-09*

## **FINAL REPORT**

*Ronald Reagan Washington National Airport  
(DCA)*

*Senstar Corp. OmniTrax® Buried Cable System*

U.S. Department of Homeland Security  
Transportation Security Administration  
Office of Security Technology  
Advanced Surveillance Program  
701 South 12<sup>th</sup> 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

This project pertained to the evaluation of the Senstar Corp. OmniTrax® buried cable intrusion detection system installed at Ronald Reagan Washington National Airport (DCA). This buried cable detection system was installed to provide continuous monitoring of critical areas along the outer perimeter boundaries.

DCA integrated the OmniTrax with its existing C•Cure and Aegis2 operator programs. The final product relayed information across both systems, however the end user controlled the OmniTrax via the Aegis2, which security personnel in the Public Safety Communication Center (PSCC) used to monitor security throughout the airport.

[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 intelligent video/neural networking solution enhancements met the airport's security expectations. The IV&V was concluded January 28, 2011.

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 DCA airport authorities. Representatives of TSA, Safe Skies, and DCA convened to discuss and verify the system requirements prior to the implementation of evaluation procedures. The resulting operational data was analyzed by the Safe Skies statistical team and combined with the site survey information to generate the final report.

## SUMMARY

From the data presented in the final report, it is clear that the intelligent video/neural networking solution had a positive effect on the DCA perimeter security efforts.

Installation of the OmniTrax was an intensive process, requiring trenching and additional power and communications infrastructure throughout the farthest regions of the facility. Integration of the OmniTrax into the existing subsystems, C•Cure and Aegis2, proved to be less intensive, and was reported by DCA and dispatch personnel as being a smooth transition.

[REDACTED]

The integration of OmniTrax with the existing access control systems minimized the adverse impact the end user might have faced in learning to use a new system interface. Rather than teach a new system to all end users, the existing software (C•Cure and Aegis2) continued to be the primary source of information, and the output from the OmniTrax was modified and incorporated into those software packages.

At the time of the evaluation, only senior operations staff and equipment maintenance personnel had been briefed on the OmniTrax software. All others use continued to use the existing alarm protocols of the existing systems.

[REDACTED]



<p>DHS/TSA 2600.02.01.11-024</p>	<h2 style="text-align: center;">Airport Perimeter Security (APS) Program – DCA – Operational Test and Evaluation Report</h2> <p style="text-align: center; font-size: small;">COPYRIGHT © 2011 National Safe Skies Alliance, Inc. ALL RIGHTS RESERVED</p>	
	<p><u>Project Performed by:</u> National Safe Skies Alliance, Inc. 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:</u> U.S. Dept. of Homeland Security Transportation Security Administration 601 S. 12<sup>th</sup> Street Mail Stop TSA-16 Arlington, VA 22209</p>	<p><u>TSA Technical Review Team</u> Charles Kelley John Nestor</p>
	<p><u>Project Funded by:</u> Federal Aviation Administration William J. Hughes Technical Center Acquisition &amp; Grants Team, AJA-4730 Atlantic City Int'l Airport, NJ 08405</p>	<p><u>FAA Technical Monitor</u> Jim Patterson</p>
	<p>April 2011</p> <p>Final Report</p>	





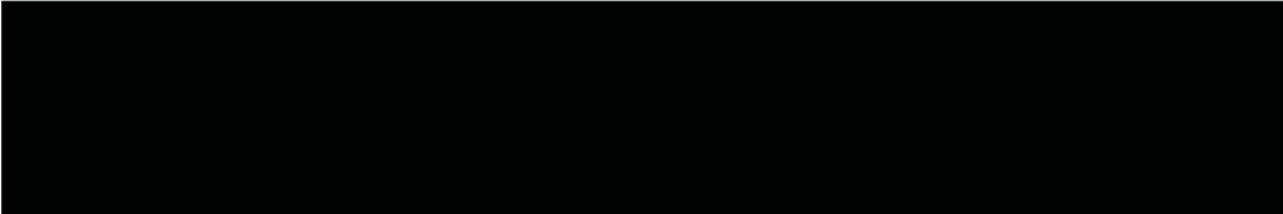
## NOTICE

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 © 2011 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.

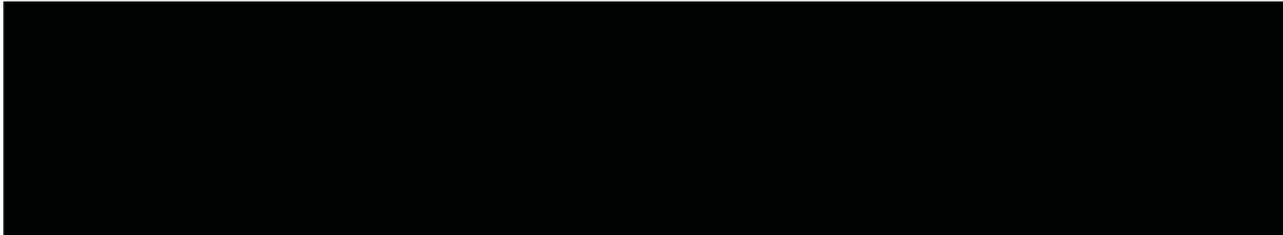
For permission to use material from this text or program, submit a request to National Safe Skies Alliance by email at [safeskies@sskies.org](mailto:safeskies@sskies.org).



**Technical Report Documentation Page**

<b>1. Report No.</b> DHS/TSA—11-024		<b>2. Government Accession No.</b>		<b>3. Recipient's Catalog No.</b>	
<b>4. Title and Subtitle</b> Airport Perimeter Security (APS) Program— DCA – Operational Test and Evaluation Report				<b>5. Report Date</b> April 2011	
				<b>6. Performing Organization Code</b>	
<b>7. Author</b> John Hunsucker, Jeff Vanvactor				<b>8. Performing Organization Report No.</b> DHS/TSA 2600.02.01.11-024	
<b>9. TSA Reviewer(s)</b> Charles Kelley, John Nestor				<b>10. Work Unit No. (TRAIS)</b>	
<b>11. Performing Organization Name and Address</b> National Safe Skies Alliance 110 McGhee Tyson Blvd. Suite 201 Alcoa, TN 37701				<b>12. Contract or Grant No.</b> 09-G-011	
				<b>13. Type of Report and Period Covered</b> Final Report, January 2011	
<b>14. Sponsoring Agency Name and Address</b> U.S. Department of Homeland Security Transportation Security Administration 601 S. 12 <sup>th</sup> Street Mail Stop TSA-16 Arlington, VA 22209				<b>15. Sponsoring Agency Code</b> TSA-16	
<b>16. Supplementary Notes</b> This report was prepared by John Hunsucker of National Safe Skies Alliance.					
<b>17. Abstract</b> Through the Transportation Security Administration Airport Perimeter Security Program, DCA integrated the OmniTrax <sup>®</sup> buried cable intrusion detection system, which is a product of Senstar Corp. DCA submitted the system for Operational Test and Evaluation, which National Safe Skies Alliance (Safe Skies) conducted onsite during the period of January 23-28, 2011. Safe Skies personnel performed intrusion scenarios, and collected performance and user survey data to determine the system's operational effectiveness.					
<b>18. Key Words</b> APS, Buried Cable, DCA, Intrusion Detection, OmniTrax <sup>®</sup> , Perimeter, Senstar, Volumetric					
<b>19. Security Classif. (of this report)</b> SSI/FOUO		<b>20. Security Classif. (of this page)</b> Unclassified		<b>21. No. of Pages</b> 31	<b>22. Price</b>

Reproduction of completed page authorized





DOCUMENT CHANGE HISTORY

<b>Version</b>	<b>Description/TSA Reviewer</b>	<b>Date(s)</b>	<b>TSA Approval</b>
0.1	Initial Draft/Charles Kelley	March 2011	
1.0	Final Draft/Charles Kelley	April 2011	



## TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	v
ACRONYMS	vii
1. INTRODUCTION	1
1.1 Background	1
1.2 Purpose of Document	1
2. SCOPE	1
2.1 Testing Limitations	1
3. SITE AND SYSTEM DESCRIPTIONS	2
3.1 Site Layout	2
3.2 OmniTrax Buried Cable	3
3.2.1 Specifications	3
3.2.2 Operating Principles	3
3.3 Installation	3
3.4 Interface	4
4. METHODOLOGY	4
4.1 Site and Schedule	4
4.2 Testing Personnel	5
4.3 Critical Operational Issues (COI)	5
5. RESULTS	6
5.1 COI 1: OmniTrax Detection Effectiveness	6
5.1.1 MOE 1: Intrusion Detection	7
5.1.2 MOE 2: Nuisance and False Alarm Reporting	11
5.2 COI 2: System Reliability	12
5.2.1 MOE 1: System Operational Functionality	12
5.2.2 MOE 2: System Accuracy	12
5.2.3 System Integration	12
5.3 COI 3: System Usability	13
5.3.1 MOE 1: Custom Optimization	13
5.3.2 MOE 2: Training Requirements	13
6. SUMMARY & OBSERVATIONS	14
6.1 Installation and Integration	14
6.2 Intrusion Detection	14
6.3 Interface	15



6.4 Key Performance Parameter (KPP) Assessment	15
7. REFERENCES	17

APPENDIX A – OMNITRAX SPECIFICATIONS

LIST OF TABLES

Table 1. Scenario Test Results Summary	vi
Table 2. Testing Scenario Summary	7
Table 3. [REDACTED] Scenario Results	8
Table 4. [REDACTED] Scenario Results	9
Table 5. [REDACTED] Scenario Results	10
Table 6. [REDACTED] Scenario Results	11
Table 7. [REDACTED] Scenario Results	14
Table 8. Key Performance Parameters	15

LIST OF FIGURES

Figure 1. DCA Perimeter Sector Map and OmniTrax Locations	v
Figure 2. DCA Perimeter Sector Map and OmniTrax Locations	2
Figure 3. AEGIS2 Screen Shots From Server Room Terminal	4



[REDACTED]

## EXECUTIVE SUMMARY

National Safe Skies Alliance (Safe Skies) performed an Operational Test and Evaluation (OT&E) of the Senstar Corp. OmniTrax<sup>®</sup> buried cable intrusion detection system installed at Ronald Reagan Washington National Airport (DCA) under the Transportation Security Administration's (TSA) Airport Perimeter Security (APS) Program. During the period of January 23-28, 2011, Safe Skies evaluated various elements of the system to determine whether it resolved Critical Operational Issues (COI) identified in the baseline assessment, and to gauge the impact of the system on established security protocols and procedures.

### SYSTEM INSTALLATION & INTEGRATION

The OmniTrax buried cable created an electromagnetic field that was approximately 1 m tall by 2-3 m wide, which detected humans or vehicles passing through it. The OmniTrax was installed within three sectors of the DCA perimeter (shown in Figure 1 below) [REDACTED]



Figure 1. DCA Perimeter Sector Map and OmniTrax Locations



## TEST RESULTS

### System Performance

Detection effectiveness was defined as the system's ability to detect and alarm on intruders attempting to bypass the detection field. To test this aspect of the system, Safe Skies personnel simulated intrusions across the system's detection field using four approach methods:

[Redacted]

[Redacted]

As shown in Table 1, the OmniTrax effectively alarmed against the [Redacted] Personnel successfully bypassed the system using the [Redacted] approach in [Redacted] attempts.

Table 1. Scenario Test Results Summary

Scenario	Total Tests	Overall Alarm Rate
[Redacted]		

### Installation & Integration

Installation of the buried cable system required significant construction efforts. Trenching was required throughout the installation areas, and additional communication fiber was required to maintain and control the hardware from the primary server room, which was located in the DCA terminal.

Integration of the OmniTrax into the existing subsystems (C•Cure and Aegis2) proved to be less intensive, and was reported by DCA and dispatch personnel as being a smooth transition.

By the time of the evaluation, only senior operations staff and systems maintenance personnel had been briefed on the OmniTrax software. However, the system was designed to be controlled primarily through the existing subsystem interfaces. This avoided significant operational impact from the users' perspective.





## ACRONYMS

APS	Airport Perimeter Security
COI	Critical Operational Issue
DCA	Ronald Reagan Washington National Airport – FAA designation
EMF	Electromagnetic Field
KPP	Key Performance Parameter
MOE	Measure of Effectiveness
MOP	Measure of Performance
MWAA	Metropolitan Washington Airport Authority
OC	Operations Center
OT&E	Operational Testing and Evaluation
$P_d$	Probability of Detection
PSCC	Public Safety Communication Center
RF	Radio Frequency
TSA	Transportation Security Administration



## 1. INTRODUCTION

National Safe Skies Alliance (Safe Skies), in support of the Transportation Security Administration (TSA) Airport Perimeter Security (APS) Program, performed the Operational Test & Evaluation (OT&E) of the Senstar Corp. OmniTrax<sup>®</sup> buried cable intrusion detection system installed at Ronald Reagan Washington National Airport (DCA). This buried cable detection system was installed to provide continuous monitoring of critical areas along the outer perimeter boundaries.

### 1.1 Background

The TSA established the APS Program to provide U.S. airports with resources to purchase and implement commercial off-the-shelf security technologies intended to address specific perimeter security concerns or susceptibilities. Airport management personnel from DCA applied for APS Program support for their proposed enhancement in January 2009.

Safe Skies performed the baseline assessment in August 2010 and issued a report<sup>1</sup> that detailed the areas in which the APS enhancement would be installed. The enhancement was installed and calibrated throughout 2010; on December 20, 2010, the system was activated and accepted for airport use.

### 1.2 Purpose of Document

This document details Safe Skies' OT&E effort. The following sections include the evaluation methods used to collect data, calculations of quantitative performance data, analysis, and documentation of observations.

## 2. SCOPE

Safe Skies performed the OT&E of the OmniTrax buried cable intrusion detection system in accordance with Critical Operating Issues (COI), which were defined and approved in the project's Final Test Plan (*DHS/TSA 2600.02.01.10-118*, November 2010).

### 2.1 Testing Limitations

OT&E procedures were only performed in those areas of the perimeter where the OmniTrax buried cable equipment was installed and functional. Because the system was not designed to detect intrusion attempts that do not pass through the detection field, the OT&E did not include  methods of entry.

The length of the OT&E period was not sufficient to either establish rates for nuisance or false alarms or study the conditions that caused them. Information gathered through personnel

---

<sup>1</sup> *DHS/TSA 2600.02.01.10-095 Airport Perimeter Security (APS) Program – DCA Baseline Report*, September 2010

[REDACTED]

interviews regarding nuisance and false alarms may reflect estimates and inferences, but not actual alarm rates or the causes.

Personnel surveys (15) were completed by emergency communication technicians within the MWAAs dispatch center. However, upon review of the surveys it was concluded that the information could not be used to measure the system's impact on the airport's security resources. Those who participated in the survey commented on the general performance of the entire security system, and not the OmniTrax system specifically. It was not possible to distinguish comments for the OmniTrax, Aegis, camera systems, or microwave sensors. Therefore user survey results are not presented in this report.

### **3. SITE AND SYSTEM DESCRIPTIONS**

#### **3.1 Site Layout**

The OmniTrax was installed in three Sectors of the DCA perimeter (shown in Figure 2) that were not equipped with a physical fence:



Figure 2. DCA Perimeter Sector Map and OmniTrax Locations



## 3.2 OmniTrax Buried Cable

The OmniTrax, manufactured by Senstar Corp., is a buried ported coaxial cable system designed to sense objects that pass through an electromagnetic field (EMF) that is generated by radio frequency (RF) signals transmitted along the buried cables.

### 3.2.1 Specifications

The OmniTrax consists of three main components:

- OC2 Sensor Cables
- Signal Processor Units
- Calibration and Monitoring Toolset (Universal Configuration Module and Silver Network)

The components listed above are proprietary equipment of Senstar Corp. This configuration of the product would be seen at any airport that is similar to DCA. Vendor-supplied specification sheets for the OmniTrax are attached as Appendix A.

### 3.2.2 Operating Principles

The OmniTrax system utilizes a pulse-coded signal generator to transmit an RF signal along a ported (leaky) coax cable that is buried approximately 10 inches beneath the ground. The transmission cable creates an EMF that is approximately 1 m tall by 2-3 m wide; a second cable receives the signal to measure variations or reflections within the EMF that are created when an object of sufficient mass passes through it. Variations that are characterized as humans or vehicles passing through the field should prompt alarms, while variations characterized by small animals, rain, wind or debris may be ignored.

## 3.3 Installation

Installation of the APS enhancement required significant construction along the airport perimeter. Trenching was required throughout the installation areas to position the set of two cables and additional fiber optic communication cable, which was required to maintain connectivity between the hardware and the primary server room in the DCA terminal.

Five processors, which controlled the eight individual OmniTrax zones, were installed near power and communication junction boxes along the perimeter. All processor equipment required environmental enclosures that could withstand a broad range of weather conditions.



### 3.4 Interface

The OmniTrax can operate as a standalone system, with its own operator interface, or may be incorporated into an existing security management system. DCA successfully integrated the OmniTrax with its existing C•Cure and Aegis2 operator programs. The final product relayed information across both systems, but the end user controlled via Aegis2 (Figure 3<sup>2</sup>), which personnel in the Public Safety Communication Center (PSCC) used to monitor security throughout the airport. From this array of screens, an operator could quickly identify the location of an alarm, retrieve live video, review history logs, adjust cameras, and acknowledge alarms.



Figure 3. AEGIS2 Screen Shots From Server Room Terminal

## 4. METHODOLOGY

### 4.1 Site and Schedule

Safe Skies conducted OT&E onsite at DCA during the period of January 24 – 28, 2011. All testing was performed 

---

<sup>2</sup> The screen shots in Figure 3 were taken from a security terminal within the primary server room, but are identical to the views from the Public Safety Communication Center.





## 4.2 Testing Personnel

All scenario-based testing was conducted by trained Safe Skies personnel. The Safe Skies evaluation team consisted of [REDACTED]

## 4.3 Critical Operational Issues (COI)

The primary objective of the OT&E was to address the COIs and corresponding Measures of Effectiveness (MOE) and Performance (MOP) that were established in the project test plan.

<b>COI 1: What are the detection capabilities of the OmniTrax?</b>	
<b>MOE</b>	<b>MOP</b>
<b>1</b> Does the OmniTrax detect intruders attempting to breach the perimeter boundary?	<b>A</b> Does the system detect an unauthorized entrance attempt [REDACTED]
	<b>B</b> Does the system detect an unauthorized entrance attempt [REDACTED]
	<b>C</b> Does the system detect an unauthorized entrance attempt [REDACTED]
	<b>D</b> Does the system detect an unauthorized entrance attempt [REDACTED]
<b>2</b> Does the OmniTrax reject non-intrusion disturbances?	<b>A</b> Determine the number of alarms caused by natural or man-made environmental effects that are reported within the observation period.
	<b>B</b> Determine the number of alarms caused by internal system processes that are reported within the observation period.



<b>COI 2: Is the OmniTrax a reliable intrusion detection system?</b>	
<b>MOE</b>	<b>MOP</b>
1 Do the system's components maintain operational functionality?	A Determine the length and causes of system downtime during the observation period.
	B Determine whether observed component failures are discrete or compound.
2 Do the system's components report accurate information?	A Determine whether the system accurately reports locations of alarms.
	B Determine whether the correct information is received by C•Cure and Aegis2.
3 Does the system integrate with DCA's existing security management system?	A Determine whether the system interfaces with existing software (Aegis2 and/or C•Cure).
	B Determine whether the system integrates with existing camera hardware.
	C Describe any significant modifications to infrastructure that were required to install the system.

<b>COI 3: Is the OmniTrax a usable detection system?</b>	
<b>MOE</b>	<b>MOP</b>
1 Can the operator optimize the system for the specific installation site?	A Demonstrate that the operator can define customized zones.
	B Demonstrate that the operator can define sensitivity levels per zone and/or intrusion type.
	C Demonstrate that the system is scalable for future expansion.
2 Can trained personnel operate and interpret the system?	A Determine training requirements.
	B Identify operator-level issues in accessing system information.
	C Identify operator-level issues in interpreting system information.

## 5. RESULTS

### 5.1 COI 1: OmniTrax Detection Effectiveness

Detection effectiveness was defined as the system's ability to detect and alarm on intruders attempting to bypass the detection field. Four approach methods were incorporated into the test and evaluation scheme. The Safe Skies evaluators performed the scenarios individually throughout the evaluation and were continuously monitored to ensure that scenarios were performed to standards stipulated in the test plan.





Table 3. [Redacted] Scenario Results

Sector	Evaluator	Total Tests	% Alarms
[Redacted]			
Overall			

From the collected data, there is not sufficient evidence to conclude that the alarm rates differed by Sector or evaluator.

5.1.1.2 MOP 1B: [Redacted] the Detecton Field

These tests simulated an intruder attempting to defeat the system [Redacted]





Table 4. [Redacted] Scenario Results

Sector	Evaluator	Total Tests	% Alarms
[Redacted]			
<b>Overall</b>			



5.1.1.3 MOP 1C: [Redacted] the Detection Field

These tests simulated an intruder attempting to defeat the system [Redacted]





Table 5 [Redacted] Scenario Results

Sector	Evaluator	Total Tests	% Alarms
[Redacted]			
<b>Overall</b>			



5.1.1.4 MOP 1D: Attempt to Defeat [Redacted] the Detection Field

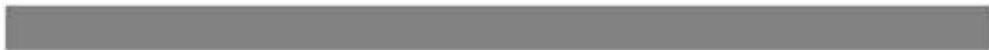
These tests simulated an intruder attempting to defeat the system [Redacted]





Table 6. [Redacted] Scenario Results

Sector	Evaluator	Total Tests	% Alarms
[Redacted]			
<b>Overall</b>		[Redacted]	



### 5.1.2 MOE 2: Nuisance and False Alarm Reporting

The OmniTrax should provide continuous intrusion detection capabilities while eliminating erroneous alarms from environmental stimuli. Nuisance alarms were defined as any alarms that were generated by ambient and/or environmental effects such as weather, animals, noise from aircraft, etc. False alarms were alarm instances that did not have an associated cause, and could be tied more closely to mechanical/electrical failure within the equipment.

Safe Skies reviewed the OmniTrax alarm records from the evaluation period, and in several cases could not determine the cause of an alarm due to current surveillance equipment capabilities. The majority of the perimeter was covered by fixed CCTV cameras, some of which did not have the range to include all OmniTrax regions. Therefore, it was not possible to accurately discriminate and categorize all alarm instances.

Personnel from the PSCC who were interviewed provided informal estimates of [Redacted]  
[Redacted] These alarms would not be categorized as nuisance as the same stimuli could have been a viable threat or incursion.

PSCC feedback provided a reasonable estimate of [Redacted]  
[Redacted]



[REDACTED]

PSCC personnel reported the level of nuisance/false alarm instances to be [REDACTED]

## 5.2 COI 2: System Reliability

### 5.2.1 MOE 1: System Operational Functionality

To determine system operational functionality, DCA Operations staff, PSCC staff, and systems maintenance personnel were interviewed to determine any existing or observed failures or issues relating to the continued use of the OmniTrax.

The OmniTrax has been in use by the personnel in the PSCC since December 20, 2010. PSCC and DCA Operations personnel report no outstanding issues in that time. All relevant components have remained in continuous operation throughout the evaluation period, and there have not been any issues with excessive nuisance alarms due to environmental conditions.

### 5.2.2 MOE 2: System Accuracy

Evaluation coordination efforts were conducted within the DCA Operations Center (OC) at a terminal that was equipped with the C•Cure system. The Safe Skies evaluation team performed [REDACTED] scenarios of which every alarm instance was accurately reported through C•Cure, identifying both the correct Sector and OmniTrax zone. Location details and nearest camera reference numbers were provided with alarm signals.

### 5.2.3 System Integration

There were no significant infrastructure tasks associated with the integration stage of the system installation. Some software modifications were required to integrate the OmniTrax with the C•Cure and Aegis2. This was a multi-tiered effort for which integration with the C•Cure software was the first stage. All signal outputs from the OmniTrax were tested for accuracy then converted into new output signals that would move to Aegis2. When all issues were resolved with the C•Cure integration, Aegis2 software was modified to accept and process the modified alarm signal data from C•Cure. The final integration allowed signal data to pass to and from Aegis2 and OmniTrax through C•Cure. The Safe Skies team did not witness any fluctuation or delay in alarm processing during the evaluation period.

The OmniTrax integration was intended to only provide alarm signals to the larger monitoring software packages (C•Cure and Aegis2) that were actively used by DCA Operations and PSCC staff, respectively. The integration did not include slew-to-queue functionality at the time of the evaluation. Operators could manually enter the appropriate camera reference number to investigate the alarms.



### 5.3 COI 3: System Usability

System usability is the end user's ability to effectively employ the technology and adapt it to their existing protocols and environment.

#### 5.3.1 MOE 1: Custom Optimization

Safe Skies investigated the flexibility and complexity of the OmniTrax to determine whether the system provided DCA personnel with the tools to perform the following tasks:

- Define detection zones
- Define sensitivity levels
- Mask nuisance alarms or malfunctioning zones

The calibration and zone setting functions were located in the core software from Senstar Corp. This was housed and operated from a server within the DCA primary server room. From the software interface, it was possible for DCA personnel to change and redefine settings to customize the existing system. However, this capability was only possible from the server, which could only be accessed with an authorized password.

The original integration strategy was to create a separation between those who maintain the system from those who monitor the system in order to further secure information and eliminate any potential tampering, directly or indirectly, from terminals within OC or PSCC. For this reason, only alarm signal outputs and responses could be accessed via the C•Cure and Aegis2 terminals. As a result, operators could not access the software interface of the OmniTrax from either C•Cure or Aegis2. Calibration and maintenance of the system was dependent on equipment maintenance personnel and Senior Operations staff, and alarm response was performed by PSCC or OC staff.

#### 5.3.2 MOE 2: Training Requirements

To be effective, the operation of the OmniTrax system must be reasonably intuitive. To assess this measure, Safe Skies reviewed vendor training materials and interviewed personnel who had been trained to use the system. Through observation, discussion, and interviews with personnel, Safe Skies found users' opinions of the OmniTrax system's operability to be positive. Supervising operations and equipment maintenance personnel indicated that the software interface was simple and intuitive, but admitted that they had not spent a tremendous amount of time on the software and could not provide additional detail.



## 6. SUMMARY & OBSERVATIONS

### 6.1 Installation and Integration

Installation of the OmniTrax was an intensive process, requiring trenching and additional power and communications infrastructure throughout the farthest regions of the facility. Integration of the OmniTrax into the existing subsystems, C•Cure and Aegis2, proved to be less intensive, and was reported by DCA and dispatch personnel as being a smooth transition.

### 6.2 Intrusion Detection



Table 7. [Redacted] Scenario Results

Sector	Test Subject	Total Tests	% Alarms
[Redacted]			
<b>Overall</b>			





### 6.3 Interface

The integration of OmniTrax with the existing access control systems minimized the adverse impact the end user might have faced in learning to use a new system interface. Rather than teach a new system to all end users, the existing software (C•Cure and Aegis2) continued to be the primary source of information, and the output from the OmniTrax was modified and incorporated into those software packages.

At the time of the evaluation, only senior operations staff and equipment maintenance personnel had been briefed on the OmniTrax software. Because they did not have extensive experience in the system's use, their comments were documented but are not considered relevant to the evaluation.

### 6.4 Key Performance Parameter (KPP) Assessment

Table 8 shows the KPPs that were defined from the baseline assessment, and the disposition as to whether each was met.

Table 8. Key Performance Parameters

Requirement Group	Functional Requirements	Technical Requirements	Expectations Met
Sensor Performance	Must provide enhanced detection capabilities	The system must maintain a consistent probability of detection: <ul style="list-style-type: none"> <li>- Detects intruders running, crawling, or walking through the detection areas and maintains a 95% Probability of Detection (<math>P_d</math>) (95% confidence)</li> </ul>	



Requirement Group	Functional Requirements	Technical Requirements	Expectations Met
		<ul style="list-style-type: none"> <li>- Maintains operation within typical outdoor environments               <ul style="list-style-type: none"> <li>o Precipitation (rain, snow, hail)</li> <li>o Wind</li> </ul> </li> <li>- Temperatures between -40°C and 70°C (-40°F and 158°F)</li> </ul>	TBD
	Nuisance/False Alarms	<ul style="list-style-type: none"> <li>- System shall maintain the specified rate of detection while minimizing alarms classified as nuisance. Ideally, [REDACTED] nuisance alarms per shift.</li> </ul>	Yes – PSCC staff reported [REDACTED]
		<ul style="list-style-type: none"> <li>- System shall allow [REDACTED] a alarm per zone per year generated by internal electronic processes. (False Alarm)</li> </ul>	TBD The system has been on for less than a year. [REDACTED]
	Customizable Sensitivity	Adjustable sensitivity level for each zone’s specific conditions	Yes – Settings and zone configurations were adjustable from the OmniTrax server only.
Central Control Software/GUI	Integration	Integrates with existing Aegis2 and C•Cure systems	Yes
		Cause existing pan-tilt-zoom cameras to automatically slew-to-cue to alarm zones.	No – Camera reference numbers and alarm information appears, but cameras require manual response.
	Usability	Requires minimal training	Training was provided, but without additional commentary and experience it cannot be determined if more is required.

Requirement Group	Functional Requirements	Technical Requirements	Expectations Met
		Controllable via GUI and mouse/keyboard	Yes
		Operator can easily acknowledge and report alarm events	Yes
		Operator can generate and export alarm history logs	Yes
	Scalability	Sensor cable be extended to cover more area	Yes
		Add or redefine zones	Yes
Power and Communications Systems	Specifications	Alerts or creates log entry upon power or communications failure in either (1) processor in the field or (2) the front-end computer system	Yes (both 1 and 2)
		Front-end computer equipped with APS or other backup power supply	DCA utilizes their own power support systems

## 7. REFERENCES

National Safe Skies Alliance. (September 2010). *Airport Perimeter Security (APS) Program – DCA Baseline Report*. (2600.02.01.10-095, Version 1.0). Alcoa, TN: Hunsucker.

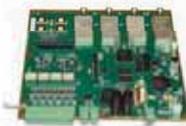
National Safe Skies Alliance. (November 2010). *Airport Perimeter Security (APS) Program – DCA – OT&E Plan*. (2600.02.01.10-118, Version 1.0). Alcoa, TN: Hunsucker.

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



APPENDIX A – OMNITRAX SPECIFICATIONS





## OmniTrax®

### Ranging buried cable detection sensor

**Description** – OmniTrax® is the fifth generation, covert outdoor perimeter security intrusion detection sensor that generates an invisible radar detection field around buried sensor cables. If an intruder disturbs the field, an alarm is declared and the location of the intrusion is determined. Targets are detected based on their conductivity, size and movement.

**Application** – Cables can be buried into a variety of surfaces (ground, grass, concrete) approximately 23 cm (9 in.) below the surface and are completely covert. The cables are robust enough for direct burial in most surfaces. The terrain-following, volumetric detection field is typically 1 m (3.28 ft.) high by 3 m (9.84 ft.) wide by up to 400 m (1312 ft. or 1/4 mile) long. Systems can be standalone or networked for long perimeters whereby sensor cables are connected together to create a continuous perimeter.

VOLUMETRIC SENSORS - BELOW GROUND

### Features

- Up to 800 meters (1/2 mile) per sensor processor
- Determines the position of intruders to within  $\pm 1$  m (3.3 ft.) with a 95% confidence
- Sensor networking - power and data over cable reduces installation costs and provides inherent data security
- Operates through vegetation (grass, shrubs and trees)
- Insensitive to wind, rain, snow, hail, sandstorms, fog, extreme temperatures, seismic vibration, acoustic, magnetic effects or blowing debris
- Detects and accurately locates multiple simultaneous intrusions
- Low False and Nuisance Alarm Rate (FAR / NAR) and high Probability of detection (Pd)
- Enhanced diagnostic tools - using Universal Configuration Module (UCM)
- Up to 7 processors protecting up to 5.6 km (3.5 miles) of perimeter for each power connection point
- Up to 32 processors protecting up to 25.6 km (16 miles) of perimeter can be networked on one network loop

### Benefits

- Completely covert
- Site aesthetics left unchanged
- Alarm assessment and response can be focused exactly on the point of intrusion
- Tamper proof

### Benefits (continued)

- Silver Network™ - enhanced communications
- Graded sensitivity cables - optimal performance
- Operates in wide range of soil conditions
- Lowest Vulnerability to defeat (Vd) of any outdoor perimeter intrusion detection sensor
- A single processor covers twice the length of previous generation systems
- Longer cables, fewer processors = cost-effective

### Markets

- Correctional facilities
- Military installations
- VIP residences
- Critical commercial / industrial assets
- Utilities
- Petrochemical
- Nuclear power plants
- Nuclear materials storage
- Airports
- Government agencies and laboratories
- Important historic / cultural sites
- Communications sites

# OmniTrax

## Ranging Buried Cable Detection Sensor

### How it works

OmniTrax uses ported ("leaky") coaxial sensor cables to create an invisible electromagnetic detection field. The cables are designed with apertures in the transmit cable's outer conductor which allow energy to escape and be received by the corresponding parallel receive cable. OmniTrax uses a coded pulse signal technique (patent pending) to determine the exact intrusion location, which can identify multiple intruders simultaneously.

Detection is based on the intruder's electrical conductivity, size and speed. The Probability of detection (Pd) for an upright 35 kg (77 lbs.) intruder, penetrating through the detection field and moving between 50 mm (2 in.) per second to 8 m (26 ft.) per second is greater than 99%, with 95% confidence. Objects weighing less than 10 kg (22 lbs.) are rejected with a statistical confidence level of 95%. Separate detection thresholds are set on a per meter basis. Any attempt to tamper with the cables, the processor or its enclosure, causes an alarm.

OmniTrax sensor calibration is simple. Walking down the sensor cables while in calibration mode allows the system to automatically adjust to the sensitivity of each meter (3.3 ft.) and thus compensate for site variations. Buried cable installation has never been so easy with calibrated thresholding.

Each OmniTrax processor can divide the perimeter protected by its two cable sets into as many as 50 alarm reporting zones. Zones can be changed at any time by technical personnel using the UCM software.

### Ranging technology – a primer

Knowing exactly where an intruder enters the perimeter is vital to assessing the situation and initiating a response. Senstar pioneered buried cable ranging technology with the launch of Guider in 1996 and has now further refined the technology to locate intrusions with pinpoint accuracy.

## Able to locate intruders with pinpoint accuracy.

### Ranging technology - features

**Calibrated thresholding** - separate threshold per meter of cable.

**Software zoning** - up to 50 zones per processor, easily adjusted

### Pinpoint target location

**Precise diagnostics** - locate faults and sources of nuisance alarms.

**Simplified installation** - fewer constraints, installation via cable trough possible

### Ranging technology - benefits

- Reduced installation costs.
- Uniform detection field reduces nuisance alarms.
- Flexibility for any environment.
- Simplifies troubleshooting.
- Source of nuisance alarms accurately located.
- Minimal sensor downtime.
- Support analysis done remotely over secure links.

### Integral power and data

In addition to detecting intruders, OmniTrax cables are used to distribute power from a single source to the sensor processors, as well as collect alarm and status data from each processor over the Silver Network for transmission to a control and display system like StarNet™ 1000. OmniTrax is unique in providing detection, power distribution and data collection over the same set of buried cables. Full redundancy for both power distribution and data collection is also possible.





**Sensor cables**

Sensor cables carry alarm information and low voltage power throughout the perimeter, saving installation time and money. Cables can provide bi-directional power and communications to provide full redundancy in the event that a cable is cut or damaged.

**Sensor cables are available in 3 configurations:**

1) OC2 has transmit and receive cables buried in separate trenches and can be spaced from 1.5 to 2 m (4.9 to 6.6 ft.) apart. The maximum spacing results in a detection field of roughly 1 m (3.3 ft.) high by 3 m (9.9 ft.) wide. The actual field size will depend on burial depth, burial medium, cable separation and the threshold settings of the sensor. The cables are graded to extend the cables' range to 400 m (1312 ft.) in length, the longest offered by any buried cable system. OC2 comes with 30 m (99 ft.) of integral lead in and 20 m (66 ft.) of integral lead out cables. The cables can be cut to fit any application. OC2 is typically used in applications that allow for longer cables (post savings) and / or require wider detection fields compared to SC1 cable. These cables are available in active lengths of 300 m (984 ft.) and 400 m (1312 ft.).

2) SC1 has transmit and receive cables in a single jacket. These cables are used in single trench or single slot applications, thus reducing installation time and expense. The resulting detection field is typically 1 m (3.3 ft.) high and 2 m (6.6 ft.) wide. The actual field size will depend on burial depth, the burial medium and the threshold settings of the sensor. SC1 cables are offered in 50 m (165 ft.) increments up to 200 m (656 ft.).

3) SC2 has transmit and receive cables buried in separate trenches and can be spaced from 1.5 to 2 m (4.9 to 6.6 ft.) apart. The maximum spacing results in a detection field that is typically 1 m (3.3 ft.) high and 3 m (9.9 ft.) wide. The actual field size will depend on burial depth, burial medium, cable separation and the threshold settings of the sensor. SC2 cables are offered in 50 m (165 ft.) increments up to 200 m (660 ft.). SC2 is typically used in applications that require wider detection fields compared to SC1 cable but do not require longer OC2 sensor cables.

**Universal Configuration Module (UCM)**

The UCM is an easy-to-use software tool that provides real-time feedback for use during OmniTrax calibration and setup. The UCM is Windows® based and can be used on a personal desktop or laptop computer. It is connected directly to the processor using a Universal Serial Bus (USB) interface or through the Silver Network™. The UCM eliminates the need for specialized electronic measurement equipment, greatly reduces the configuration time and effort, and facilitates factory support with its enhanced diagnostic tools.

**Silver Network**

OmniTrax processors can communicate alarm, status, and configuration information to and from a central control point using an integral networking capability referred to as Silver Network. Senstar's Silver Network uses a loop topology with separate Transmit (Tx) and Receive (Rx) point-to-point links between each OmniTrax processor or other connected Silver Network-compatible equipment. Silver Network is designed to be polled from both ends of the loop, thus providing redundant data paths to the field equipment. Point-to-point links can be RS-422, single or multi-mode fiber, or over the OmniTrax

sensor cables. The data signal is completely regenerated at each node in the loop to ensure proper signal integrity and reliable data transmission. Running Silver Network over the same cables as OmniTrax saves costs by eliminating the need for a separate perimeter network and provides an inherently tamper-proof communications path.

Communications over Silver Network is managed by a Windows® XP-based PC running Silver Network Manager (SNM) software. SNM controls network communications and passes OmniTrax alarm and status information to a control and display system such as StarNet 1000. The interface between the PC hardware and Silver Network-compatible field units, such as the OmniTrax processor, is provided by the Silver Network Interface Unit (SNIU). The SNIU is a 1U rack-mountable unit and provides the choice of USB, Ethernet, and RS-232 for connecting to the PC. Communication between the SNIU and OmniTrax processors can be either RS-422 or multimode fiber optic cables.

The SNM software provides an interface to third party Security Management System (SMS) software via the Network Manager Interface (NMI). Via the NMI a third party SMS can communicate to the SNM in two ways - either by an exchange of messages at the TCP/IP level or by making calls to the NMI Dynamic Link Library (DLL). To enable third party integration to the SNM software Senstar provides a detailed Applications Programming Interface (API) document, a network manager simulator, and sample code. With the network manager simulator, a developer has the ability to simulate the full range of OmniTrax sensor and supervisor alarms including the ability to define at what range an alarm is to appear. The simulator also covers a wide range of other Senstar products.

## Technical Specifications

### PERFORMANCE

- Probability of detection (Pd) - Optimized for the detection of an upright 35 kg (77 lbs.), or larger person moving between 50 cm (2 in.) per second to 8 m (26 ft.) per second, with a probability of detection of 99% with 95% confidence. This is based on penetration of the intruder through the detection zone
- False Alarm Rate (FAR) - Fewer than 1 per zone per month alarms from unknown causes with full visual assessment
- Nuisance Alarm Rate (NAR) - Site dependent

### PROCESSOR MAIN FEATURES

- Direct digital receiver
- Alarm reporting:
  - Up to 50 functional segments per cable
  - Up to 50 alarm reporting zones per processor
- Relay outputs:
  - Alarm A, Alarm B, Supervision, Fail
  - Form C, 1.0 A 30 VDC max
  - Expandable with relay output card
- Auxiliary inputs:
  - 2 supervised inputs
  - Expandable with universal input card
- Lightning protection:
  - Transorb and non-radioactive gas discharge devices on all I/O ports
- USB port

### PROCESSOR OPTIONS

#### RS-422 communications card

- Mounts on processor expansion header
- Supports two RS-422 (4-wire) data paths
- True regeneration of signal (removes distortion at each node)

- Every processor in a network configuration requires a communications card

#### Fiber optic communications card

- Mounts on processor expansion header
- Supports two fiber optic data paths or one fiber optic data path and one RS-422 path
- Multimode fiber optic communication card allows distances of up to 2.2 km (7,200 ft.)
- Multimode card fiber card operates at 820 nm, comes with ST connectors and is compatible with 50/125 µm, 62.5/125 µm, 100/140 µm, and 200 µm HCS® multi-mode fiber
- Single-mode fiber optic communication card allows distances of up to 10km (32,000 ft.)
- Single-mode fiber card operates at 1310 nm, comes with ST connectors and is compatible with 9/125 single-mode fiber
- True regeneration of signal (removes distortion at each node)

- Every processor in a network configuration requires a communications card
- #### Input / output card
- Mounts on processor expansion header
  - The OmniTrax processor can accept 1 optional input / output card in addition to a communications card
  - Relay output card: 8 form C relay outputs (1.0 A, 30 VDC max)
  - Universal input card: Inputs with configurable thresholds and supervision modes

#### Auxiliary power supply

- Accepts 18 to 56 VDC
- Output 12 VDC, 150 mA

### PACKAGING / ENVIRONMENTAL

Processor on a base plate in a white aluminum NEMA 4 (or equivalent) enclosure:

- Size - 40 H x 235 W x 16.5 cm D (15.75 H x 9.25 W x 6.5 in. D)
- -40°C to +70°C (-40°F to +158°F)

Protective telecom enclosure accepts OmniTrax NEMA 4 enclosure:

- Size - 98.4 H x 2.5 W x 27.3 cm D (38.8 H x 16.8 W x 10.8 in. D)
- Color - light green enamel over steel
- Protection - IP33

### POWER REQUIREMENTS

- 10 to 52 VDC network input voltage at less than 9 watts
- Integrated internal 5 ah battery backup

### SENSOR CABLE OC2

- Two pairs of sensor cable per processor (A and B)
- Contiguous graded design with lead-in, active cable and lead-out
- Lead-in length 30 meters (98.4 ft.)
- Active cable length 40 meters (131.2 ft.) or 300 meters (984 ft.)
- Lead-out length 20 meters (66 ft.)
- Cable jacket diameter 12.67 mm (0.475 in.)
- Each cable set comes with a kit of 6 TNC connectors and 40 ferrite beads for field installation

### SENSOR CABLE SC2

- Two pairs of sensor cable per processor (A and B)
- Contiguous graded design with lead-in and active cable (no lead-out)
- Lead-in length 20 meters (66 ft.)
- Active cable lengths of 50, 100, 150 or 200 m (164, 328, 492 or 656 ft.)
- Cable jacket diameter 8.0 mm (0.315 in.)

- Each cable set comes with a kit of 4 TNC connectors and 20 ferrite beads for field installation

### SENSOR CABLE SC1

- Two cables per processor
- Transmit and receive cable in a single jacket
- Contiguous graded design with lead-in and active cable (no lead-out)
- Lead-in length 20 meters (66 ft.)
- Active cable lengths of 50, 100, 150 or 200 meters (164, 328, 492 or 656 ft.)
- Cable jacket size 8.5 x 15 mm (0.335 x 0.590 in.)
- Each cable set comes with a kit of 4 TNC connectors and 10 ferrite beads for field installation

### CABLE ACCESSORIES

- Standalone and network decouplers
- Terminator kits / connector tool kits / cable repair kits
- Ferrite beads / connectors

### SILVER NETWORK™

- Silver Network Interface Unit (SNIU) - reliable lightning protected computer interface
- Silver Network Manager (SNM) - software interface to Trend® Security Management System (SMS) such as StarNet 1000 or 3rd party system
- Alarm data including pinpoint target location
- Diagnostic data to support remote UCM operation
- Point-to-point interconnection provides reliable communication - no signal degradation as with multi-drop networks
- Facilitates fail safe communication

### SILVER NETWORK™ REPEATERS FOR LONG NETWORK RUNS

- RS-422 to RS-422
- Multi-mode fiber to multi-mode fiber
- RS-422 to multi-mode fiber
- Accepts 10 - 52 VDC
- Built-in battery charger

### GENERAL ACCESSORIES

- 48 V outdoor-rated network power supply
- 48 V indoor-rated dual redundant network power supply
- 12 V outdoor-rated single processor supply
- Lightning arrestor kit

The OmniTrax buried cable detection system is protected by US patents 5,914,655 and 5,834,688 (with others pending) and other international patents.

Specifications are subject to change without prior notice.



www.senstar.com

100 1000 Ave.  
St. Hubert, Quebec J3V 1K1  
Canada (514) 333-3333

Copyright ©2004. All rights reserved. Features and specifications are subject to change without notice. Senstar, StarNet, Silver and the StarNet logo are registered trademarks of Senstar. Silver Network™ is a trademark of Trend. StarNet 1000 and 3rd party are trademarks of Trend. StarNet, Silver Network, and the StarNet logo are trademarks of Senstar. Silver Network is a registered trademark of Senstar.

Printed in Canada

Senstar is represented by dealers in over 80 countries.

International  
Lang, Telford, Canada  
Tel: +1 (514) 333-3333  
www.senstar.com

United States  
Phoenix, AZ, USA  
Tel: Fax: +1 (602) 475-0000  
info@senstar.com

United Kingdom  
Hemel Hempstead, UK  
Tel: +44 (0) 1494 24977  
www.senstar.com

Latin America  
Guatemala, Guatemala  
Tel: +52 (977) 245 0000  
info@senstar.com

Europe  
Melsbroek, Belgium  
Tel: +31 (0) 20 480 9779  
info@senstar.com

Spain  
San Polo, Spain  
Tel: +34 (91) 496 9000  
info@senstar.com