Abraxas Corporation

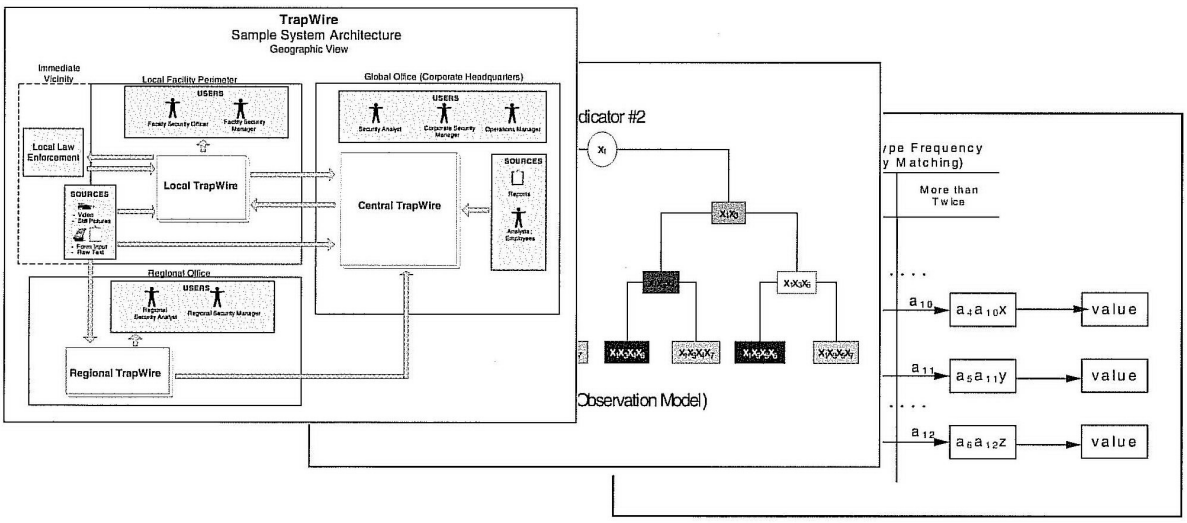
6845 Elm Street ♦ Suite 310 ♦McLean, VA 22101 ♦ Tel 703.821.8930 ♦ www.abraxascorp.com

TrapWire™
Pre-Attack Terrorist Detection System
For Protecting Critical Infrastructure

The prevention of terrorist attacks on critical infrastructure requires the ability to detect various discreet but identifiable indicators of pre-attack preparations. Only by uncovering such attack preparations can we take actions designed to deter or intercept a terrorist strike before it begins. While international terrorist organizations are using increasingly sophisticated methods, their modus operandi does contain a critical vulnerability: meticulous pre-attack preparations require the terrorists to approach a target facility on multiple occasions to identify physical and procedural vulnerabilities, probe for weaknesses and conduct practice missions. For example, the terrorists planning the Khobar Towers attack in Saudi Arabia reportedly surveilled the facility on 40 occasions.

Terrorists will typically surveil multiple facilities prior to selecting an appropriately vulnerable target. Therefore, as the number of facilities on the TrapWire network increases, so does the probability of detecting pre-attack preparations. TrapWire is specifically designed to exploit this vulnerability by combining deep counterterrorism experience, proven counter-surveillance techniques, unique sensor systems, and data mining capabilities to detect attack preparations and allow security personnel to deter or intercept terrorist operations.

TrapWire dramatically increases the ability to detect pre-attack preparations and to take appropriate action to detect, deter and intercept terrorist attacks. A visual monitor of the entire system—a map with dynamic status indicators for each entity connected to the TrapWire network— facilitates the ability of decision-makers to absorb vast quantities of information quickly and efficiently. The dynamic status indicators show the threat level at each facility and highlight those that have moved to a higher threat level over the preceding 24 hours. Security officials can thus focus on the highest priorities first, taking a proactive and collaborative approach to defense against attacks. The information collected by TrapWire can also be shared with law enforcement agencies to assist in their counterterrorism efforts.



TrapWire's architecture offers significant technological and financial advantages as well:

- **Robust and Proven Technology**—Use of best of breed, emerging and commercially available off-the-shelf components dramatically reduces system cost and development time while increasing reliability and upgradeability.

- **Force Multiplier Effect**—TrapWire increases the return on investment in security by leveraging existing security assets to provide comprehensive and predictive intelligence.

- **Bridge to the Future**—TrapWire provides a foundation for future technology upgrades that can be added as plug and play modules.

ABRAXAS CORPORATION

North American Headquarters
6845 Elm Street, Suite 310
McLean, Virginia 22101
703-821-8930 ex. 121

Asian Headquarters
Plaza 66
Shanghai PRC 200040
86-21-6288-1479 ex. 8235

For further information, please visit our website at www.abraxascorp.com or call 703-821-8930 ex. 121.

TrapWire is a trademark of Abraxas Corporation
Patent pending
Copyright 2004, Abraxas Corporation

1. BACKGROUND

The standard approach to counterterrorist security is to "harden" facilities by strengthening perimeter security. Recent terrorist attacks, however, have demonstrated that while improving perimeter security may mitigate the consequences of an attack, it will not prevent a determined attacker. The use of suicide bombers and large vehicle-borne explosives gives a significant advantage to the attackers. Even when facility defenders see the attack coming, as has often been the case, experience shows that it is too late to stop the attack. Our ultimate goal – the protection of human life – demands prevention, not mere mitigation. Abraxas Corporation (through its affiliate Abraxas Applications, Inc., collectively, "Abraxas") has developed the TrapWire™ counter-terrorism system to provide those responsible for protecting critical infrastructure with the advanced warning necessary to detect and prevent terrorist attacks.

While terrorists have developed ingenious methods of attack, their modus operandi contains a critical vulnerability: their need for extensive pre-attack site surveillance necessitates that they approach the target facility on multiple occasions. TrapWire is specifically designed to exploit this vulnerability by enabling the defenders to detect patterns and anomalies indicative of pre-attack terrorist surveillance. As a result, facility security managers and personnel may now have weeks or months advance notice of an attack, which enables them to take measures to ensure that the attack never occurs.

The basic premise behind the TrapWire system is as follows: Through the systematic reporting of suspicious events and the correlation of those events with other event reports for that facility and for related facilities across the network, terrorist surveillance operations can be identified, appropriate countermeasures can be employed to deter attacks, and steps can be taken to apprehend the perpetrators.

The TrapWire system provides the following capabilities:

- A mechanism for a facility's personnel to record suspicious activity data in a structured format;
- A mechanism to identify and link related events following human review;
- The ability for a facility's Chief Security Officer (CSO) to identify threat trends at his/her facility (increasing or decreasing) and to drill down into the specific event reports that generated those threats;
- Alerts to the CSO of events that do not affect the threat score but may nevertheless be of interest;

- The ability to notify a facility of a changing threat level within its industry or geographical location;
- A mechanism to correlate external events such as watch list events for suspected terrorists or stolen vehicles with other observed event data already within the system;
- The ability to correlate events occurring at different facilities by related individuals, and to notify all affected facilities of the increased threat to their facility based on this related activity;
- A mechanism to reduce the system-calculated threat level at a facility, based upon the time since the last threatening event; and
- Notifications, alerts, and possible action recommendations based on a particular site's security plan, implemented via a set of rules that act upon event information.

2. OPERATIONAL CONCEPT

2.1. Operations

The installation of the TrapWire system begins with the identification of a facility's critical vulnerabilities as viewed through the eyes of a terrorist attacker. To attack these vulnerabilities, terrorists will need to conduct surveillance operations and will seek specific locations that offer both line-of-sight to the vulnerability and effective cover for surveillance activity. Once our experts have identified the facility's vulnerabilities, they will survey the surrounding areas to identify the zones and locations where terrorist surveillance is most likely to occur. We then work with facility security personnel to ensure that all available collection resources are properly sited to cover the critical surveillance zones. We also can advise security personnel on how to eliminate as many of these surveillance zones as possible to effectively channel the terrorists into areas controlled by the defenders.

To collect and process suspicious event data, TrapWire utilizes a facility's existing technologies (such as pan-tilt-zoom [PTZ] cameras) and humans (security personnel, employees, and neighbors). The collected data is recorded and stored in a standardized format to facilitate data mining, information comparison and information sharing across the network. TrapWire records descriptions in two standard formats: PersonPrint™, a 10-characteristic description of individuals; and VehiclePrint™, an 8-characteristic description of vehicles. TrapWire also standardizes descriptions of potential surveillance activity, such as photographing, measuring and signaling. TrapWire matches

this human-entered data with information collected by sensors and enters the reporting into the TrapWire database.

Once the information is entered into the database, it is processed by the TrapWire rules engine, an expert software system designed by Abraxas personnel with extensive experience in the areas of counterterrorism, surveillance operations, surveillance detection techniques, and intelligence analysis. The rules engine identifies the patterns of terrorist pre-attack preparation and provides the critical advance warning needed to prevent the attack.

The TrapWire rules engine continuously searches for similarities, links and patterns among threat data collected across the network and shares correlated data with all affected facilities. Facility managers and security personnel can view threat information related to their own site and associated reporting collected across the entire TrapWire network (it is important to note that facility vulnerability information is NOT shared across the network; only threat information is shared). This allows TrapWire to leverage the "network effect," making each facility on the network more secure as a result of its access to surveillance threat information collected at other facilities. For example, if facility security personnel enter event reporting on an individual engaged in suspicious activity, TrapWire will automatically provide those security personnel all similar reporting – i.e. linked via PersonPrint or VehiclePrint – from other facilities on the network. TrapWire thereby converts a group of isolated facilities into an information collection and dissemination network that significantly enhances each facility's ability to detect terrorist surveillance and deter the attack. The threat reporting can also be shared with law enforcement officials to facilitate the identification and capture of terrorist surveillants.

2.2 TrapWire Reporting

TrapWire continuously assesses all event reporting and automatically provides threat analyses to network members. Each facility on the network will have its own TrapWire Threat Meter (TTM), which measures identified, suspected surveillance activity at that facility. The TTM operates on a scale of 0-100 and is correlated to the DHS color-coded threat alert. Green reflects a score of 0-20, blue 21-40, yellow 41-60, orange 61-80, and red 81-100. TrapWire will also provide Threat Reports to security personnel. Threat Reports, which drive the TTM, are generated by the analytical portion of the rules engine. A Threat Report links together various individual Event Reports and generates a threat score based upon algorithms within the rules engine. By clicking on a Threat

Report, a user can read the Event Reports that generated the Threat Report. The Event Reports provide a short description of the Event, the date and time stamp of the Event, the name of the individual who entered the Event data, the location of the Event, a PersonPrint and VehiclePrint, if recorded, and any sensor generated information (video attachments, photographs, etc.).

TrapWire provides clients with a web-based monitor displaying the protected facility and surrounding neighborhood. The display identifies surveillance zones, sensor coverage, and symbols showing where recent events have occurred. When moving the mouse over the symbol, basic information on the Event is displayed. Clicking on the symbol displays the full Event Report with attached photographs/videos. The Event Report also displays links to any related reporting from that facility or other facilities on the network. A time scale provides the ability to examine events over a user definable timeframe and with geographic locations.

Abraxas can also provide several TrapWire-associated services, as required and requested by the client. We offer:

- Systems integration services associated with the TrapWire system. In the technology area, this entails providing sensor technologies, customized software, data mining capabilities, technology operations and maintenance support, and other products or services necessary for the operation of the TrapWire system.

- Specialized Threat Assessments (typically conducted "outside the perimeter" of a facility), "Red Team" exercises, professional surveillance detection teams, surveillance detection training, and security operations consulting (e.g. planning designed to alter a facility's existing security profile).

- Analysis of potential surveillance activity at the facility, regional, industry, national and global levels. With the prior approval of each client on the network, event reports from all facilities would be aggregated and analyzed to detect patterns indicative of terrorist surveillance activity. The results would be shared with all relevant facilities. In addition, isolated networks could be formed when wider information sharing is undesirable.

- Maintenance of TrapWire's core rules engine. TrapWire will be updated on the basis of Abraxas' counterterrorism expertise, and the rules engine will change to reflect changes in terrorist modus operandi.

- Customized TrapWire site profiles. As a client's facility or surrounding neighborhood changes, Abraxas will update the client's site profile to reflect the changed environment. We can provide security managers at client sites with a reporting mechanism for notifying us when their environment is altered.

- Maintenance of the technical aspects of the TrapWire network. We'll dispatch trouble-shooting teams to client sites to address technical anomalies and other problems, as requested by the client.

For additional information, contact Abraxas Applications at: 703-821-8930, ext. 101 or 158