



Technology-Based Border Security Solutions & Services



www.raptorglobalinc.com

September 11, 2011



Technology-Based Border Security Solutions & Services



This document outlines the processes, systems and services involved in the design, deployment and operation of electronic security systems for border perimeter surveillance, security and control. It should be noted that this document does not address any number of physical or architectural aspects to border control, such as fences, walls, gates, turnstiles, access control barriers, bollards, security berms, or any other structure or system used to restrict access along a border or at an access point. It is assumed that these areas will be supported by the general contractor, or another entity involved in this project.

The resources employed in planning, designing, constructing, operating and maintaining an effective electronic border surveillance and security system requires a unique approach that cannot be supported by 'off-the-shelf' or 'one-size-fits-all' applications.

Therefore, as part of a comprehensive approach to supporting a project of this magnitude the following factors must be addressed:

- ▶ **Needs Ascertainment:** The processes required to identify and define the scope and nature of the project; then directing the resources and manpower to develop a well-documented response to those needs.
- ▶ **Threat Assessment:** Bringing the proper skill-sets to play in assessing potential threats and recommending the appropriate solutions in securing the border from covert incursions by terrorists and/or overt military action.
- ▶ **Design Criteria:** The development of a comprehensive technology-based security system design that takes into account variances along the border in terrain, weather, environment, wildlife migration, and population density.
- ▶ **Access Authorization and Detection Systems:** The specification and selection of advanced systems such as passport authentication, facial recognition, license plate recognition (LPR), chemical, radiation and biological detection systems and other advanced technology at border entry points.
- ▶ **Overt Surveillance Systems:** Deploying overt video surveillance, acoustic, seismic and proximity sensors along physical barriers (fences, wall, gates, etc.) where the potential for unauthorized incursion may exist, but the threat of tampering with or destroying equipment is low.
- ▶ **Covert Surveillance Systems:** Deploying covert video surveillance, acoustic, seismic and proximity sensors in locations where physical barriers may be limited or non-existent, and the threat of tampering with or destroying equipment is high.
- ▶ **Advanced Technology:** The systems, applications and hardware that have been specially developed by **Raptor**, and its partners, for border surveillance and perimeter security applications.
- ▶ **Rapid Response Systems:** Providing rapidly deployable portable systems for video surveillance, perimeter sensors and communications/control in situations where the need for increased security may be temporarily required.



- ▶ **Communications Network:** Designing and constructing an advanced communications network to accumulate and transport data accumulated by cameras, sensors and support systems, as well as provide reliable communications for security personnel.
- ▶ **Support Systems:** Selection of the applications, software and equipment required to integrate various components into a seamless security system.

Needs Ascertainment

Perhaps the most important part of a project of this magnitude is to determine the specific needs and requirements of the project. For example, the architecture of a 'controlled' border, between countries enjoying friendly relations, requires a completely different approach to planning, design and ongoing support than does a 'militarized' border in a hostile environment.

With this in mind, **Raptor** has developed an approach to needs ascertainment that encompasses a two-stage assessment process:

- ▶ **Preliminary Assessment:** This is the initial work necessary to perform a preliminary evaluation of the project in order to determine the appropriate responses required to meet the project's intended objectives. It is usually possible to acquire the necessary data to accomplish this goal if there has been a detailed scope of work (SoW) developed by the client or general contractor. If no scope of work is available, or if it is lacking in detail, **Raptor** will work with the general contractor, and others involved in the project, to develop a comprehensive document.
- ▶ **Field Survey:** This process is an on-site evaluation of the physical area to be served, an assessment of existing video surveillance and/or security infrastructure, and the selection of potential camera, sensor and support locations and network support sites. While the duration of the site survey is dependent on the magnitude of the project, gathering information for a detailed design is usually accomplished in ten to fifteen days.

Threat Assessment

In concert with the physical data, accumulated during the needs assessment stage, the ability to determine the level and nature of the potential threats facing the security system is just as important. Therefore, it is critical that during the period of time in which needs ascertainment data is accumulated, and the physical site survey is conducted, a focused effort be directed at assessing security threats that may be directed at border crossing points, remote locations along the border, highly populated sites near the border or any other point that may be vulnerable to unauthorized crossing or incursion.



Three of the most common threats to a secure border are:

- ▶ Unauthorized border crossing by refugees, undocumented aliens or smugglers,
- ▶ Incursions by potential terrorists, sappers or enemy agents,
- ▶ Penetration of the border by limited or full-scale military action.



Raptor will bring to bear its internal resources, and that of its highly qualified strategic partners, to work with government authorities to provide a comprehensive assessment of these and other potential security threats. **Raptor** threat assessment personnel are:

- ▶ Highly-trained professionals with years of military special operations and security experience.
- ▶ Specially trained in threat analysis, interpretation of local conditions, and identifying and analyzing the profiles of potential adversaries.
- ▶ Experienced in identifying the nature and magnitude of threats that may exist in a perimeter or border security situation.

Design Criteria

This stage includes the preparation of a detailed design and implementation plan that shows recommended camera placement, sensor installation, specific types of systems, and preparation of a detailed bill of materials that itemizes projected cost.



In preparing the system design, particular attention is paid to the physical aspects of the border to be secured. Some of the critical design criteria that must be addressed include:

- ▶ Topography of the terrain along the border has a significant impact on the video ‘view shed’ (the area that can be viewed by a camera) and the placement and type of sensors.
- ▶ Weather plays an important role in choosing the appropriate systems for electronic security. For example, high winds can result in reduced capability of acoustic or proximity sensors, and rain, fog and dust storms can restrict the capability of video cameras.
- ▶ One of the most common causes of ‘false alarms’ is frequent wildlife incursions. If seasonal animal migrations, or a high number of large animals, are present it is necessary to accommodate for this situation by employing more sophisticated threat interpretation software.
- ▶ Another major design consideration is the ability to identify and provide solutions for high population densities that may be present along certain border locations. Normal day-to-day activities in towns and villages along a border can produce a higher potential for inaccurate data and false alarms.

It is important to stress that the reliability of an electronic security system is critical to a project of this magnitude. If a system produces a high number of ‘false’ or ‘unverifiable’ alarms its credibility will quickly come to question. A **Raptor** border or perimeter security system is based on supporting ‘multiple levels’ of authentication. This is accomplished by deploying three-level (or higher) redundancy, coupled with the latest in video analytic and threat interpretation software, to create a highly reliable platform that limits the frequency of ‘false alarms’ and produces data that can be accurately interpreted.

Raptor will develop a complete system design based on the data accumulated in both the needs ascertainment and threat assessment stages.



Access, Authorization and Detection Systems

Raptor is uniquely positioned to support a wide range of security technology specifically dedicated to perimeter and border security. As part of the 'holistic' perimeter security approach, **Raptor** is prepared to seamlessly integrate a number of advanced technology security systems into a comprehensive border crossing and checkpoint access, surveillance and security program:

- ▶ **Access Systems:** **Raptor**, and its partners, can provide a wide variety of border crossing and checkpoint access control systems including:
 - ◆ Biometric systems, such as retinal and fingerprint scanners,
 - ◆ Sophisticated verification software and data archival systems,
 - ◆ State-of-the-art video analytics for license plate and facial recognition,
- ▶ **Authorization Systems:** **Raptor** can provide a complete line of authorization and border guard safety systems including:
 - ◆ Passport data scanners and fast data retrieval systems,
 - ◆ Encrypted and 'tamper proof' identification cards for authorized personnel,
 - ◆ Lone worker or 'man-down' tracking systems,
- ▶ **Detection Systems:** **Raptor** has teamed with some of the world's leading providers of border crossing/checkpoint detection systems including:
 - ◆ Fixed and portable radiation detectors,
 - ◆ Chemical and explosive detection systems,
 - ◆ Biological sensors and bio-hazard threat response systems,

These systems are available to **Raptor** through its strategic relationships with some of the world's foremost providers of specialized perimeter security products, applications and services. **Raptor's** extensive experience and technical capability as a project management and systems integration company ensures that individual systems, hardware and applications are fully integrated into the overall system architecture.

Overt Surveillance Systems



The most common systems employed in border security are overt or 'unconcealed' fixed and stationary systems that are visible and easily identified. Many times these systems are intentionally made to be highly visible to serve as a deterrent to incursions in their coverage area. These systems are normally employed in areas where there are adequate physical barriers and a manned presence.

The overt border perimeter security package incorporates multiple detection devices; microwave, passive infrared, acoustic, seismic, proximity and hard-wired alarms with a sophisticated multi-spectral surveillance video imagery system that transmits real-time video streamed images, or continuously updated high resolution *snapshots*, via wireless, cellular or satellite back to the tactical operations center (TOC).



Raptor offers some of the most advanced video surveillance products, applications and services for perimeter security in 'at-risk' or hostile environments. **Raptor's** advanced video surveillance systems provide high-resolution wide-spectrum equipment and software that monitor the status of personnel to ensure their safety in potentially hostile situations; prevent the intrusion of unauthorized personnel along sensitive perimeters; and monitor and assess potential threats of terrorism or crime at border crossings and checkpoints.

For this application, **Raptor** proposes an all-inclusive video surveillance and security support package that can meet the demanding needs of an all-inclusive border incursion and counter-terrorism program. A 'typical' border perimeter surveillance system of this type would include the following equipment, systems and applications:

- ▶ Multiple levels of video surveillance equipment, strategically located in key locations to include:
 - ◆ High resolution fixed wide-angle cameras in specified locations,
 - ◆ Remote pan/tilt/zoom cameras in specified locations,
 - ◆ Low-light, infrared (IR) and thermal imaging (heat sensitive) cameras in locations where it has been determined it is advisable to have this type of capability,
- ▶ Deployment of related support systems to include:
 - ◆ High quality audio pickup devices at strategic locations,
 - ◆ Seismic, acoustic and motion-sensitive proximity sensors to trigger alarms in the event of an unauthorized entry or perimeter penetration,
 - ◆ Special illumination devices for low light and IR capabilities,
 - ◆ Wireless connectivity to allow for maximum flexibility in camera placement.
- ▶ Sophisticated video analytic software, with supporting hardware, including,
 - ◆ License plate recognition systems,
 - ◆ Facial recognition systems,
 - ◆ 'Intuitive' threat recognition systems that can detect, interpret and respond to potential threats,
 - ◆ Biometric systems,
- ▶ One or more highly secure tactical operations/monitoring center(s) (TOC) to include:
 - ◆ High resolution monitors and large screen monitors
 - ◆ Dedicated computer systems
 - ◆ Supporting communications systems
 - ◆ Equipment for on-site caching of surveillance data
- ▶ Optional equipment to support the secure off-site caching of data accumulated by the surveillance network for a defined period of time,
- ▶ Personnel training and operational assistance,
- ▶ Ongoing maintenance, applications updates and system upgrades.



Covert Surveillance Systems

The most sophisticated systems used in border security are those that cannot be easily seen or identified as being a part of a perimeter security system. The design, construction and placement of covert security systems are not new or unique requirements for **Raptor** and its partners. In fact, two of **Raptor's** strategic partners are highly qualified to support this requirement, having provided covert security systems for a number of the most sensitive and secure facilities in the world.

Many of the systems used in this application perform in a similar manner to those employed in open or 'overt' applications, but their architectural 'form-factor' may be radically different. For example, **Raptor** has extensive experience in the installation of clandestine or 'disguised' cameras in sensitive locations where it is inadvisable to reveal the area is under surveillance. Cameras and sensors can be built to blend into any number of terrain features, shrubbery, trees or local structures in the area. In addition, systems can be 'hardened' to prevent damage caused by vandalism or sabotage.

The need to deploy covert systems and the selection of equipment to be used in this application is determined by the threat assessment, needs ascertainment and design stages.

Rapid Deployment Security Systems

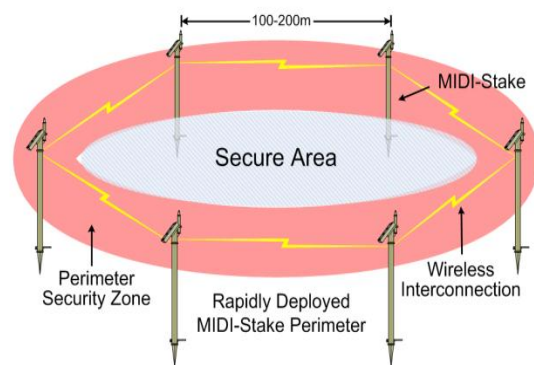
Security systems that can be rapidly deployed, and at the same time are unobtrusive, are vitally important to an end-to-end solution to border perimeter security and surveillance. These systems are employed in situations where existing systems are over-burdened, or where an increased threat level requires immediate supplemental capability.

In response to these requirements, **Raptor** provides for the rapid deployment of pre-packaged perimeter security solutions intended to recover and sustain critical infrastructure.

Raptor rapid response and recovery perimeter security systems are used to support border patrol and military agencies in mitigating the effects of a loss of perimeter surveillance or border monitoring and control capability.

- ▶ **Raptor** rapid response perimeter security systems are designed to bridge the gap between a loss of video surveillance or monitoring capability, and the resumption of normal security infrastructure, during times of natural or manmade disasters.
- ▶ **Raptor** rapid response perimeter security systems are designed to provide a high level of electronic security restoration and augmentation within a wide variety of hostile and devastated environments.
- ▶ In addition, **Raptor** rapid response systems can provide a wide range of remote voice, video and data communications to support both operational and tactical communications.

The advanced technology products described in the next section showcase a number of these rapid response and easily deployable systems.





Raptor 'Showcase' Technology

'MIDI-Stake': One of the 'showcase' security products recently introduced by **Raptor** and WaveTeq Communications is a rapidly deployed integrated perimeter security and surveillance device that includes a wireless mesh interconnection, wireless data transport platform, multiple sensors, and a number of 'add-on' modules that extend the system's performance. The advanced **'MIDI-Stake'** perimeter security system is relatively inexpensive and easily deployed. It is capable of operating in a variety of environmental and terrain conditions.

'SITE MAST-R': The **Raptor SITE MAST-R** system is another rapidly deployed security system designed to support perimeter security, public safety and telecom needs by providing remote video surveillance, perimeter sensors, personnel status and communications from remote high-risk locations along a border perimeter to a central monitoring or tactical operations center via the Internet.

The **SITE MAST-R** system provides continuous monitoring of activities along the perimeter by providing a real-time view of the site using a combination of high-resolution, high-definition, infrared, low light and thermal imaging cameras. The **SITE MAST-R** is available in two rapid deployment configurations, a portable system in five ATA cases and a mobile trailer.

'Raptor VSM': One of the key features of the **Raptor** video surveillance product and service offering package has been the development of an integrated 'Video Surveillance Module' (VSM) that includes a high-resolution wide-spectrum camera, a wireless data transport platform, 'intuitive' video analytics and a variety of powering options. Some of the characteristics of the VSM include:

- ▶ The capability of providing high-resolution video over a broad spectrum of lighting conditions,
- ▶ A secure network, with access available only to qualified personnel,
- ▶ Highly reliable performance in a wide variety of weather conditions,
- ▶ The ability to link a great number of camera locations into a single network,
- ▶ An IP-based platform that allows software and applications to be modified or upgraded remotely,
- ▶ A 'modular' design, allowing additional features and enhancements to be easily added in the field by non-technical personnel.

An easily deployed wide-application module such as the VSM allows **Raptor** to deploy and operate video surveillance systems at a fraction of the cost of current systems. It also provides the added advantage of 'mobility' in that a video surveillance module can be moved from one location to another at very little cost. This feature is high on the list of public safety officials since it allows them to 'tailor' the video surveillance system to a particular event or location.

'TraceGEO': Many of the products and services supported by **Raptor** are branded under the **'TraceGEO'** name, a product and service line specializing in providing safety and security solutions and services to the energy, maritime and industrial sectors. **Raptor** has commercially adapted some of the most sophisticated tracking, status monitoring and perimeter security products available today, many of which are in use by the US



Government in critical applications worldwide. **TraceGEO** systems incorporate a proprietary 'multi-tier' wireless platform (RFID, Wi-Fi, GSM, GPS, A-GPS and satellite) delivery system that provides continuous and ubiquitous coverage worldwide.

- ▶ **TraceGEO-AST:** is a complete line of asset, vehicle and personal tracking, status monitoring and incident management and resolution solutions and services.
- ▶ **TraceGEO-PST:** wireless systems that support the monitoring and safety of personnel working in hazardous or potentially hostile environments.
- ▶ **TraceGEO-FST:** a complete line of fleet tracking and status/performance monitoring systems.
- ▶ **TraceGEO-PSM:** includes a complete line of advanced pipeline status and monitoring solutions including: remote cathodic monitoring, flow disruption notification and major spill surveillance and prevention; domestically or on a worldwide basis
- ▶ **TraceGEO-IPM:** is an advanced perimeter protection and monitoring solution that incorporates video, motion detection, passive IR, acoustic and seismic transducers, coupled with an intelligent incident management system, to remotely detect intrusions in the harshest environments.
- ▶ **TraceGEO-IMS:** is an intelligent incident management system that manages and tracks remote assets, vehicles and personnel and 'intuitively' manages the appropriate response in the event of a threat to life or property.
- ▶ **TraceGEO-PSR:** Protective security incident response and resolution designed for the protection and rescue of personnel and the recovery of high value assets.

Communications Network



Traditionally, one of the weakest links in supporting a comprehensive electronic security program is the communications network necessary to accumulate and transport data and video information from remote sensors back to a central monitoring facility or tactical control center (TOC). This is due to the fact that while security technology designers are usually very good at their specializations (video surveillance, detection systems, interdiction and intrusion systems), they rarely have a similar level of expertise in the networking side. This has become even more apparent now that a majority of security systems are designed to Internet Protocol (IP)-based standards.

Raptor Global has extensive experience in the design, construction and support of IP-based networks in support of security initiatives. One of **Raptor's** partners has developed a unique 'hybrid' network design that combines the best of fiber optic technology with a variety of wireless systems to produce a highly reliable and cost effective method of collecting, distributing and transporting video surveillance and sensor data to remote monitoring locations. These systems can be 'hardened' to military specifications and as well as encrypted to ensure the security of communications and data within the network.



Support Systems

'Operator Overload' is one reason why many tactical operations centers (TOCs) encounter serious problems when tasked with identifying and responding to critical and potentially life threatening situations. That is why **Raptor** uses the proprietary '**Raptor-IMS**' (Incident Management System) in equipping its client's TOCs. '**Raptor-IMS**' is a specially designed suite of software and applications originally deployed by US Department of Defense, designed to minimize the number of *events* an operator must observe and to separate potentially serious incidents from the normal *clutter* of day-to-day activities.



The intelligent and intuitive '**Raptor-IMS**' system accumulates millions of bits of data that is generated during *typical* activities at a specific location and establishes a normal *signature* for that location. Any event that occurs outside of this signature is compared to previously established *threat* signatures and if the signature matches one of these pre-defined conditions, or if it is outside of established boundaries, an *incident* is declared and the operator is notified in a number of ways, including visually and audibly.

'**Raptor-IMS**' automatically determines the threat level, recommends the appropriate action and undertakes the proper incident response solution, all within seconds. It notifies all concerned parties following a previously established notification/escalation list, and ensures that follow-through activities are underway on a minute-by-minute basis.

Contact Information

Raptor provides end-to-end security technology solutions for homeland security, military, energy, maritime, transportation and enterprise applications. For more information about **Raptor Global Services, Inc.**, please visit our website at www.raptorglobalinc.com or contact:

James Shearer at: jims@raptorglobalinc.com or call 206-388-3743 or 253-380-2575.

Paul Brandenburg at: paulb@raptorglobalinc.com or call 360-540-2058.