



**INVEST**TREND

INVESTREND RESEARCH

# HOMELAND SECURITY SECTOR REPORT 3<sup>rd</sup> QUARTER 2005



COMMISSIONED BY



**CRONUS CAPITAL MARKETS**



R.C. FUHRMANN CFA

# Homeland Security Sector Report

## *Table of Contents*

Introduction to Homeland Security.....	3
National Strategy .....	3
Government Agencies and Initiatives.....	5
Private Sector Initiatives.....	6
Sector/Macro Overview .....	6
Characteristics – Market Size, Growth Arenas.....	6
Regulatory Environment.....	9
Secular Trends .....	9
Commercial Opportunities.....	10
<i>Biometrics</i> .....	10
<i>Vaccines/Pharmaceuticals</i> .....	12
<i>RFID</i> .....	12
<i>Screening, Scanning, Surveillance</i> .....	13
<i>Border Security</i> .....	13
<i>Chemical Industry</i> .....	13
<i>Transportation Industry</i> .....	13
<i>Cyber Security</i> .....	13
<i>Information Technology (IT)</i> .....	14
<i>Communication</i> .....	14
Industry Overview .....	14
Industry Drivers & Characteristics .....	14
Six Defining Missions.....	15
Intelligence & Warning.....	15
<i>Domestic Intelligence</i> .....	15
<i>Foreign Intelligence</i> .....	16
Border & Transportation Security .....	16
<i>Land/Air/Sea Transport</i> .....	16
<i>Land/Air/Sea Border Control</i> .....	17
Domestic Counterterrorism.....	17
Protection of Critical Infrastructure and Key Assets .....	17
Defense Against Catastrophic Threats.....	18
<i>BioDefense</i> .....	18
Emergency Preparedness & Response.....	18
<i>Preparedness</i> .....	18
Investment Characteristics .....	19
Investment Merits/Drawbacks .....	20
Valuation Methodologies/How to Analyze .....	20
Major Industry Players.....	20
Homeland Security – Recent Developments .....	21
ISE-CCM Homeland Security Index .....	23
Summary & Conclusion.....	24

*Table of Contents (ctd.)*

Company Research Directory:

BlastGard International  
Bulldog Technologies  
Cyber Defense Systems  
Digimarc Corporation  
Groen Brothers Aviation  
Viscount Systems

Bibliography

## Introduction to Homeland Security

Homeland Security, as defined by the National Strategy for Homeland Security<sup>i</sup> (“the Strategy”), is as follows:

“Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.”

Despite the now ubiquitous and straightforward ‘color-coded’ threat system (e.g. red/orange/yellow/green) used to inform the nation as to the probability of a terrorist attack, Homeland Security represents an exceedingly complex topic to define and understand. It involves efforts both at home and abroad and demands a range of government and private sector capabilities as well as a coordinated and focused effort from different entities that have not historically been compelled to focus on security efforts. The Strategy established three objectives based on the definition of Homeland Security as previously stated:

1. Prevent terrorist attacks within the United States;
2. Reduce America’s vulnerability to terrorism;
3. Minimize the damage and recover from attacks that do occur.

The events of September 11 have had a profound effect on the way in which the United States views national security. Since that time, federal, state, and local law enforcement agencies have been pushed onto the national stage and subjected to redefined and newly evolving roles. According to the Strategy, they should now ‘assign priority to preventing and interdicting terrorist activity within the United States.’<sup>ii</sup>

### National Strategy

The unanticipated events of September 11 ushered in a new era of urgency and devotion by the Bush Administration to protect the United States and its citizens from future terrorist attacks. Immediately following the attacks in New York, the Administration moved quickly to consolidate the functions of national security into one agency – the Department of Homeland Security (“the Department”). On November 26, 2002, after months political negotiating, the agency became official as President Bush signed legislation approving the largest reorganization in the U.S. government since the creation of the Department of Defense in the 1940’s. Tom Ridge, a former governor of Pennsylvania, became its first head. The new entity consolidated an estimated 22 former agencies and 180,000 employees into one department. Additionally, resources committed increased three fold (see below for further budgetary details). Since September 11, there have been no additional significant terrorist tragedies within U.S. borders. The Bush Administration has announced numerous advances from its initiatives, including the arrest or death of approximately 75% of senior al Qaeda officials, the capture of an estimated 4,000 terrorist ‘operatives’ globally, and the capture of roughly \$140 million in terrorist funds throughout the world.<sup>iii</sup>

In July 2002, the Office of Homeland Security debuted its [National Strategy for Homeland Security](#) in which it stressed the necessity to focus on six main missions to combat terrorism:

1. **Intelligence & Warning** – Stresses the need to develop systems aimed at eliminating the element of surprise in attacks, accomplished by sharing intelligence and anticipating threats.
2. **Border & Transportation Security** – Enhances the ability to protect and monitor the nation's land/air/sea entry and exit points for citizen travel as well as the transport of goods.

3. **Domestic Counterterrorism** - Intends to prevent or 'counter' acts of terrorism, represented as one of the most important acts in the fight against terrorist activities.
4. **Protecting Critical Infrastructure & Key Assets** – Identifies the need to protect physical, intellectual and virtual fabrics of society. This includes any intended target of terrorists to adversely affect or cripple the way in which the nation operates (economically, socially, and logistically).
5. **Defense Against Catastrophic Threats** - Include initiatives such as ways to document inventories of chemical, biological, radiological substances and weapons or key inputs used to manufacture items such as nuclear weapons. Additionally, it is important to prevent the theft or improper use of such inventories, both domestically and internationally.
6. **Emergency Preparedness & Response** - Improves the national ability to quickly and resolutely respond to potential breaches of national security. References the importance of the 'first responder community', or individuals such as firefighters, policeman, medical professionals, and other public officials that proved extremely poised and responsive after the events of 9/11.

To complement and expand on the six defining missions, in 2004 the Department of Homeland Security offered a strategic plan in which it outlined six guiding principals:<sup>iv</sup>

1. **Protect Civil Rights and Civil Liberties** – A major guiding principle is to protect individual rights and civil liberties while protecting the homeland.
2. **Integrate Our Actions** – The combination of approximately 22 previously discordant agencies into one department to better combat terrorism.
3. **Build Coalitions and Partnerships** – Encourage and enhance cooperation among agencies and between international, federal, state, and local governments and the private and academic sectors
4. **Develop Human Capital** – Agency employees are viewed as the most important asset in combating terror.
5. **Innovate** – To build and encourage new ideas, approaches, and methodologies in the global fight against terrorism.
6. **Be Accountable** – Learn from results and outcomes to continually enhance performance and fix what may currently be broken.

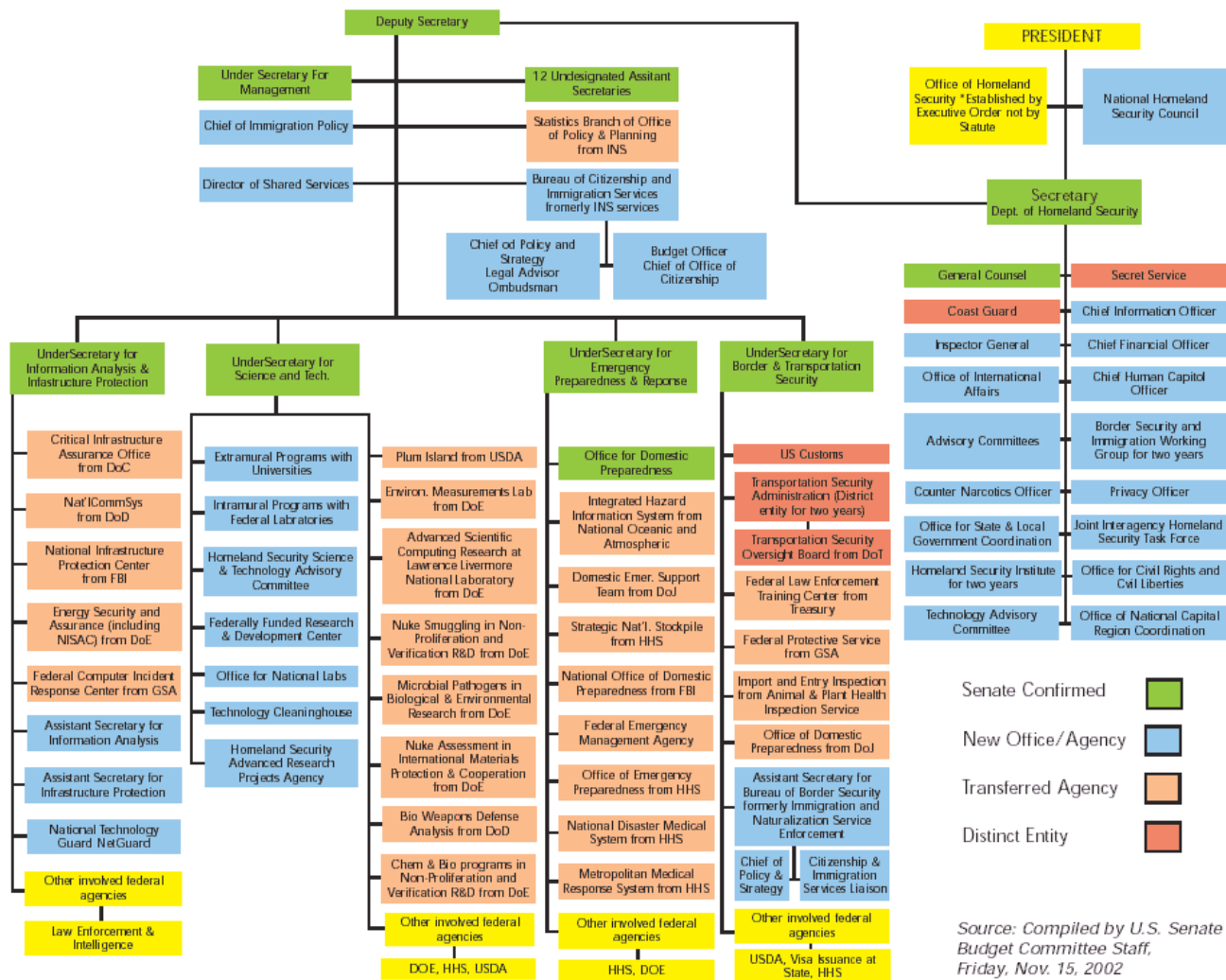
In July 2004 [The 9/11 Commission Report](#)<sup>v</sup> was released. This study was a final report compiled by the National Commission on Terrorist Attacks upon the United States. It offered a detailed history of developments pre- and post-9/11 and also offered its interpretations of certain failures or systemic flaws in U.S. national security that could have possibly prevented such an attack. The report cited operational failures such as a lack of information sharing between agencies (e.g. the inability of the FBI to effectively compile data from its field agents to assist with national priorities, or that one hijacker had links to attacks on the battleship USS Cole), problems at the CIA and FBI regarding very decentralized organizations that inhibited information gathering, 'permeable borders' and weak immigration controls (e.g. false documents, incomplete watch lists, 'permeable aviation security' that led to the use of U.S. planes as weapons against its citizens), and the fact that U.S. banks and financial institutions were used to funnel resources to terrorists living within U.S. borders. Currently, there are a number of initiatives and improvements to Homeland Security that are being undertaken by public and private organizations to address systemic security failures.

In the first quarter of 2005, [Michael Chertoff](#)<sup>vi</sup> was chosen to head the Department. In a recent interview with *BusinessWeek*<sup>vii</sup>, Mr. Chertoff highlighted his ambition to make the private sector more accountable for defending the nation against terrorist attacks and to act as a first responder should such attacks occur. With the exception of the airline industry that has received and will continue to receive attention, other industries are expected to face increased scrutiny. Mr. Chertoff ordered a sixty-day review of the agency to realign priorities and strategies. His focus has been on a cost-benefit study of Homeland Security and to ensure that major security threats are properly being addressed.

In July 2005 Mr. Chertoff announced a reorganization to the Department.<sup>viii</sup> He announced a number of changes intended to allow the Department to evolve from its 2002 creation and remove bureaucratic inefficiencies and increase ‘nimbleness’ and focus more closely on higher probability events. Mr. Chertoff announced other changes as well such as by adding a Chief Intelligence Officer.

### Government Agencies and Initiatives

Below is an [organizational chart](#) detailing the hierarchy for the Department<sup>ix</sup>:



Source: <http://www.govexec.com/homeland/HSchart.htm>

A number of major agencies were consolidated under the umbrella of the Department. Major agencies centralized into the Department include the Department of Immigration and Naturalization Services (INS), U.S. Customs Services, U.S. Coast Guard, and the Transportation Security Agency (TSA). This was seen as necessary from the standpoint of having a more unified front to respond to threats and attacks. For instance, before government agencies were realigned, it was estimated that twelve different federal agencies could have responded to a chemical or biological attack.<sup>x</sup>

### **Private Sector Initiatives**

The private sector has adapted quickly to federal Homeland Security initiatives and is expected to further develop and eventually overtake the public sector as a driving force in technological innovation. Initiatives are vast and were only accelerated by the events of 9/11, which amounted to an adverse economic impact in the neighborhood of \$70 billion. Those considered most compelling in the investment community include automated identification (e.g. radio frequency identification (RFID)), surveillance, biometrics, and monitoring services. Compelling private sector commercial opportunities will be described in further detail later in this report.

## **Sector/Macro Overview**

### **Characteristics – Market Size, Growth Arenas**

Homeland Security market dynamics permeate into a countless number of private and public arenas. In the public sector, major players in the Homeland Security market include federal agencies, state governments, and first responder organizations such as local municipalities. In the private sector, major players can be divided into incumbent security firms, large firms with a security presence, and smaller, entry-level players with niche products or burgeoning technologies.

At the highest level, national defense is a useful arena with which to analyze the size of the Homeland Security market. Large defense contractors believe that the war on terrorism is driving defense spending and the push for new and enhanced technologies to better prepare for and respond to threats. As will be detailed further below, national defense initiatives have quickly evolved from larger, standing armies towards more mobile, agile forces capable of rapid deployment to a great number of small-scale conflicts. In terms of total spend, defense firms have benefited from an increased federal focus on security efforts. President Bush's 2006 budget request for \$420 billion in defense spending represents an estimated 5.0% increase from the previous year (approximately \$400 billion in FY '05). Of this \$420 billion, an estimated \$147 billion has been earmarked for procurement and research & development (R&D). FY '05 vs. FY '01 defense growth has been approximately 30.0%. Clearly, initiatives in Iraq and Afghanistan have been the main drivers of this above average growth. In September 2004, Congress approved \$25 billion in additional funding for Operation Enduring Freedom and has requested an additional \$80 billion for the remainder of 2005. As part of the 2006 budget request, a Future Years Defense Play (FYDP) was submitted and stressed the need to focus on 'transforming' defense capabilities and a commitment to research and development for longer-term evolution in the security landscape.

The federal government is currently seen as driving economics in the Homeland Security industry due to an increased commitment of time and resources to protecting the nation from future terrorist attacks.

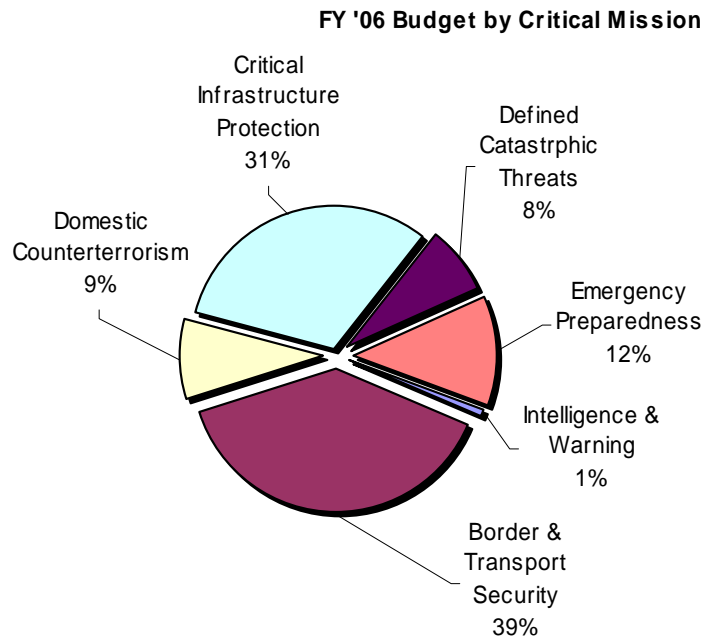
The Bush Administration requested \$49.9 billion in Homeland Security spending for fiscal year (FY) 2006. This represents nominal growth of approximately 8.6% from FY '05. Approximately 54.7% of this amount has been earmarked for the Department of Homeland Security, down from an estimated 57.4% in FY '05.<sup>xi</sup> Spending has also been earmarked for areas such as enhanced

domestic security, improved counterterrorism measures, infrastructure protection, and improved services for other federal programs and agencies. Critical missions will be defined in further detail below.

At the end of September, the Senate approved a \$31.9 billion budget which represents an approximate 5% increase from the previous budget request. The bill included a 10% budget increase for two border security agencies that would allow for an additional 1,500 border patrol agents and approximately \$618 million to customs and immigration organizations. Democrats criticized the bill as cutting back on first responder grants for state and local governments and shifting focus to more urban areas (e.g. New York, Los Angeles) to the detriment of smaller, rural states. The bill was also critiqued for not doing enough to enhance transit security (current funding of approximately \$150 million) in light of multiple recent London subway bombings. The bill was estimated to have increased funding to improving and upgrading explosive detection systems and equipment at airports but proposed limiting the number of full-time security screeners at the Transportation Security Agency (TSA) at 45,000 and decreasing the \$2.67 billion budget by \$125 million. The bill also included stipulations requiring the Federal Emergency Management Agency (FEMA – part of the Department of Homeland Security) to more fully disclose the \$62 billion allocated to hurricane relieve efforts.<sup>xii</sup> Additionally, approximately \$3.9 billion has been earmarked for the Center for Disease Control (CDC) in regard to combating potential avian flu outbreaks in the U.S. Of this amount, \$3.1 billion is estimated to be devoted to creating inventories of antiviral drugs, such as Roche’s Tamiflu. Finally, the budget for the Office of Domestic Preparedness was estimated to be decreased \$210 million to \$3.35 billion.<sup>xiii</sup>

Figure 1.1 represents a graphical depiction of the percentage of the FY '06 budget earmarked for each of the Six Defining Missions. Border & Transport Security represents the highest proportion of funding, followed by Critical Infrastructure Protection.

Figure 1.1



Source: <http://www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=75635>

Figure 1.2 quantifies the FY 2006 budget breakdown. Though Border and Transportation Security represents the highest proportion of funding, both Intelligence & Early Warning and

Defending Against Catastrophic Threats account for higher year over year growth, although from a much smaller initial base.

Figure 1.2

<b>Funding by National Strategy Mission Area</b>			
(\$ billions)	FY '05	FY '06	YoY
<b>Mission Area</b>	<b>Actual</b>	<b>Est.</b>	<b>Growth</b>
Intelligence and Early Warning	\$0.35	\$0.43	22.9%
Border and Transportation Security	17.55	19.29	9.9%
Domestic Counterterrorism	3.94	4.47	13.5%
Protecting Critical Infrastructure & Key Assets	14.94	15.63	4.6%
Defending Against Catastrophic Threats	3.40	3.90	14.7%
Emergency Preparedness and Response	5.77	6.12	6.1%
Other	0.05	0.10	100.0%
Total	\$46.00	\$49.94	8.6%

Source: Office of Mgmt. And Budget; 03.14.05

Additionally, the FY 2006 budget can be analyzed in terms of individual department funding. As should be expected, the Department of Homeland Security garners most of the funding, followed by the Department of Defense. Justice and State Department funding is expected to experience the highest year over year growth, although from a smaller funding base.

Figure 1.3

<b>Homeland Security Funding by Dept.</b>			
(\$ billions)	FY '05	FY '06	YoY
<b>Dept.</b>	<b>Actual</b>	<b>Est.</b>	<b>Growth</b>
Defense	\$8.57	\$9.51	11.0%
Energy	1.56	1.67	7.1%
Health & Human Services	4.23	4.41	4.3%
Homeland Security	24.87	27.33	9.9%
Justice	2.68	3.10	15.7%
State	0.82	0.94	14.6%
Other	3.26	2.98	-8.6%
Total	\$46.00	\$49.94	8.6%

Source: Office of Mgmt. And Budget; 03.14.05

At a more local level, the Department of Justice estimates that protection services grew approximately 7.0% annually from 1984 through 1999 to \$65.4 billion. These services include the first responder network which the Bush Administration estimates at 1.9 million individuals, broken down as follows:

- Greater than 1 million firefighters nationwide, of which approximately 75% are on a volunteer basis
- 700,000 full-time law enforcement individuals from 17,000 state and local law enforcement agencies
- Approximately 155,000 emergency medical individuals
- 88,000 personnel from approximately 70 federal law enforcement agencies

From a private sector perspective, the landscape is highly fragmented and expected to undergo aggressive consolidation as larger firms look to strengthen their product offering and broaden

their share of public funding. Individual firm details will be provided in the *Company Spotlight Reports* section.

Figure 1.4 details Lehman Brothers' estimates on the size of certain Homeland Security markets:

Figure 1.4

Estimated Market Size (\$ million)	2004
<b>Equipment</b>	
Homeland Security - Detectors	\$2,200
Alarm Monitoring - Equipment	7,000
Fire Monitoring - Equipment	4,000
Video Surveillance	5,500
Biometrics	1,200
Door/Fence/Perimeter Access Equipment	18,000
Smart/Token Cards	1,500
Bar Code Scanning Systems	6,500
RFID	1,800
Armor- Vehicles and Individuals	4,500
<b>Services</b>	
Commercial Alarm Monitoring	9,000
Residential Alarm Monitoring	7,000
Guard Services	34,000
Consulting - Intel & Investigation	8,000
Cash Armored Transport	1,500
Logistics/Ancillary Armored Transport	1,500
Systems Integration	4,500
Computer Security	7,000
<b>Source: Lehman Brothers Estimates</b>	

Morgan Keegan performed its own analysis of the Homeland Security market size and also detailed its expectations for growth through 2007. (Figure 1.5)

Figure 1.5

	2004	2007E	CAGR
Tracking & Identifying - Individuals and Equipment	\$4,800	\$10,700	22.2%
Physical Security Technology	20,000	36,300	16.1%
Detection and Screening Technologies	8,500	15,300	15.8%
Surveillance and Monitoring	4,500	11,000	25.0%
Risk Mitigation	9,600	14,600	11.1%
<b>Source: Morgan Keegan</b>			

### Regulatory Environment

Government regulations are currently under review by the Department. U.S government contracts are traditionally entered into with provisions allowing the government to unilaterally void or suspend agreements as a result of violations of laws, regulations, and guidelines.

### Secular Trends

Federal spending on Homeland Security has increased dramatically since September 2001. Barron's estimates that the federal government has spent approximately \$130 billion since the attacks in New York and has requested an additional \$50 billion through 2006.<sup>xiv</sup> Since that time, the government has been preoccupied and focusing internally to adjust its organization to better respond to a new security landscape. In the short-term, the public and private sectors have been working frantically to understand a newly organized government and identify ways in which it can grab a portion of the vast amount of resources being committed to counter terrorism on a national and global front. From a longer-term perspective, Homeland Security has undergone a positive secular change as it evolves into settling conflict on a smaller, proactive, and more expedient basis. The industry is beginning to adapt to what has been described as one of the biggest reorganizations to the U.S. government in the past half-century.

Prior to 2001, data on security spending by the federal government could not easily be compiled. According to the Heritage Foundation, security expenditures increased from \$9 billion to \$16 billion, or 60%, between FY 1995 and FY 2001. Additionally, Heritage points out that emergency spending in 2001 for Homeland Security came in at \$64 billion, of which \$20 billion was earmarked for FY '01 while \$44 billion was appropriated to FY '02 spending.<sup>xv</sup> Clearly, 2001 marked a new era in the Homeland Security marketplace.

### Commercial Opportunities

Both incumbent and entrepreneurial firms are focused on capturing a share of the massive federal funds being invested in Homeland Security. Of the \$130 billion estimated to have been spent by the federal government since September 11, roughly \$23 billion has been committed to the private sector.<sup>xvi</sup> As the industry matures, private sector initiatives will increasingly drive demand for new products and services to protect things such as the nation's infrastructure. Private sector firms include large defense companies such as Lockheed Martin (NYSE: LMT) or Boeing (NYSE: BA) but also include burgeoning firms that allow investors an opportunity to capitalize on specific technologies and products.

However, the federal government also must dictate certain conditions it believes will encourage and strengthen national security. As traditionally occurs, the private sector habitually combats high levels of government intervention, arguing that it is able to police itself and that efforts to enhance safety and security are unduly burdensome and hurt competitiveness and returns to its shareholders. As such, the Department of Homeland Security must strike a careful balance between creating incentives and properly implementing enhancements to security efforts.

In terms of incentives being directed by the Department, the Homeland Security Advanced Research Projects Agency (HSARPA) actively solicits and awards to entities that apply for and successfully receive grants funding to pursue defense and security initiatives. Solicitations include diverse areas such as Bio-agent, chemical, and biological detection equipment. Sample organizations include large defense firms (e.g. Honeywell) and academic institutions (e.g. Columbia University, Carnegie Mellon, Rutgers University). The HSARPA also solicits recommendations for future topic and grant areas from the private sector.

Current technologies with significant market potential are as follows:

#### *Biometrics*

Biometrics represents perhaps one of the most fundamental and useful ways to identify and track individuals and prevent terrorists from reaching destinations from which to carry out or coordinate attacks. The field of biometrics involves the use of human identifiers to recognize a person based on physiological characteristics or behavioral characteristics. Biometric features include a person's face, fingerprints or hand geometry, retina or iris, or even handwriting and voice.

As stated by the House of Representatives in June, 2002, regarding the security directive:

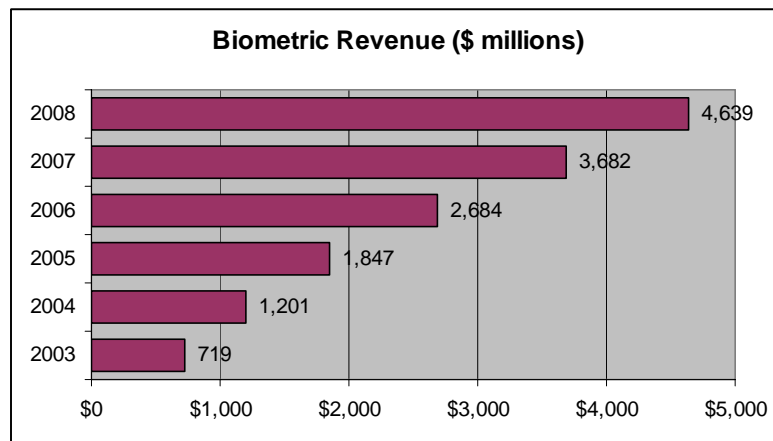
Since September 11th, State and local officials have expressed the need for better access to actionable information that can prevent terrorist attacks on our homeland. Some of this information must be classified, but most will be sensitive but unclassified. This legislation seeks to balance and reconcile the needs of State and local personnel to have access to timely and relevant Homeland Security information to combat terrorism with the need to protect and safeguard both classified and sensitive but unclassified information.<sup>xvii</sup>

A Rand Corporation study highlighted three 'critical' areas in which biometrics could be used to prevent acts of terrorism: 1) Controlling access to sensitive facilities at airports; 2) Preventing identity theft and fraud in the use of travel documents; and 3) Identifying known or suspected terrorists.<sup>xviii</sup>

Homeland Security efforts in the U.S. have increased the usage of biometric equipment and technology as information collection and coordination efforts increase across government entities. It is becoming increasingly necessary to compile and maintain records on citizens and others traveling internationally. For example, the Bureau of Consular Affairs has added more security checks for certain groups of visa applicants from certain countries and established automatic links to the FBI from visa issuers. The Homeland Security Directive also created a Foreign Terrorist Tracking Task Force and intends to better coordinate immigration and customs policies with Mexico and Canada. The following legislative initiatives have specifically requested an increased effort in developing biometric capabilities to enhance security: Aviation and Transportation Security Act of 2001, Enhanced Border Security and Visa Entry Reform Act of 2001, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, USA Patriot Act of 2001, Port and Maritime Security Act of 2002.

The biometric market is currently estimated at approximately \$1 billion in terms of revenue. Figure 1.6 depicts the International Biometric Group's estimate of the current market size and its expectations for growth through 2008.<sup>xix</sup> Public and private demand is currently driving innovation in the industry. Federally, legislation has been passed requiring countries that are not required to apply for a Visa to enter the U.S. to include biometric information in their passports. This requirement is expected to be implemented by October 2005. The International Civil Aviation Organization (ICAO) has stipulated that facial recognition be the primary identification method in these passports. Figure 1.6

International Biometric Group estimates that fingerprint technology currently represents nearly half of the biometric market (48% based on 2004 revenues) and followed by face recognition technologies (12%), hand identification (11%), iris (9%), voice (6%) and numerous other developing technologies.



Source: International Biometric Group (2004)

In August 2004, the Bush Administration released Homeland Security Presidential Directive (HSPD) #12. This directive highlighted the need to create a common identification system across all government agencies with the goal of reducing identity fraud while protecting personal security. Companies such as Fargo Electronics (NASDAQ: FRGO) are competing to be chosen as a major supplier to this initiative; it is also expected that the government will stipulate identification standards for individuals and companies that wish to do business with federal agencies. Other companies in the space include Cogent (COGT- NASDAQ), Identix (IDNX- NASDAQ), ActivCard (ACTI - NASDAQ), Viisage Corp (VISG - NASDAQ) and OSI Systems (OSIS - NASDAQ). Cogent is seen as one of the top providers of fingerprint identification systems. Foreign firms competing in the space include Sagem Morpho (subsidiary of French firm Sagem SA) and NEC of Japan. Firms with significant biometric business unit initiatives include heavyweight firms such as Motorola (via its Printrak division).

### *Vaccines/Pharmaceuticals*

In 2004, Congress provided incentives for healthcare and pharmaceutical companies to develop drugs and vaccines related to combating illnesses and diseases born out of terrorist activities. Incentives included potentially lucrative patent extensions, market exclusivity for certain periods of time, the ability to bypass the FDA in times of emergency, etc. The U.S. government approved \$5.6 billion be earmarked to build a national stockpile for vaccines and medications to counter potentially devastating bioterrorism activities such as the spread of anthrax or smallpox. 2006 efforts include the possibility to limit liability by companies developing drugs and vaccines, tax incentives for investing in the area, and additional patent extension possibilities.<sup>xx</sup>

### *RFID*

RFID technologies are perhaps most ubiquitous as a commercial initiative used to track goods that consumers purchase (e.g. clothing purchased at any retailer- referred to as 'smart tags' in these instances. According to the Economist:

RFID systems are made up of readers and "smart tags"—tiny microchips each with an attached antenna. The tags can be stuck on everything from milk cartons to hospital patients. When prompted by a reader, the tag broadcasts the information on its chip. Unlike the traditional bar code, which smart tags aim to replace, RFID chips give every tagged object a unique identification. (A bar code describes only a class of objects, such as cans of Coke.) Companies hope to use RFID to track the trillions of objects that circulate the world every year in planes, lorries and ships, through ports and warehouses, on to shop shelves, through tills and into homes and offices. Accurate tracking should eventually save hundreds of billions of dollars a year as it improves distribution, reduces theft, cuts labor costs and shrinks inventory. Governments also want to use RFID to reduce drug counterfeiting and improve military logistics, among other things.<sup>xxi</sup>

Lehman Brothers estimates the total RFID market at between \$1.5 - \$3.0 billion based on 2003 revenues. Frost & Sullivan estimates that the market, including related equipment, consulting, and software, will reach \$10 billion by 2009. Venture Development Corporation (VDC) estimated the total RFID market at \$1.5 billion for full year 2004 and expects it to grow at a compound annual growth rate of just under 50% through 2007. Allied Business intelligence (ABI) expects global RFID spending to reach just over \$3.0 billion by 2008 while Frost & Sullivan expects the total global market to reach just under \$12.0 billion in size by 2010. Sector growth is in its infancy and expected to accelerate substantially through the end of the decade. As with a large number of burgeoning technologies that receive initial funding via public security initiatives (such as global positioning systems (GPS); even RFID dates back to WWII as a radar system), the federal government has accelerated RFID research and development as it pursues better ways to track shipping container cargo, reduce counterfeiting, and improve military supply chain management primarily as a result of September 11 . However, RFID is receiving considerable private sector attention as witnessed by Wal-Mart which demanded that its top 100 suppliers utilize RFID for certain shipments. The demand-pull has been primarily retail driven; other firms with RFID mandates include Target, Albertson's, and British-based retailer Tesco. Indeed, International Data Corp (IDC) estimates that the RFID marketplace for U.S retail chain spending stood at \$91.5 million for full year 2003 and projects the market to grow exponentially to over \$1.3 billion by 2008.

There are currently a number of publicly traded RFID companies. These include: Infosys (INFY – NASDAQ), Zebra Technologies (ZBRA– NASDAQ), Symbol Technologies (SBL– NYSE; Symbol acquired major player Matrics in 2004), and I.D. Systems (IDSY – NASDAQ). Major private firms competing in the space include Alien Technology (Alientechnology.com). Firms with significant RFID business unit initiatives include heavyweights such as IBM, 3M, and Microsoft & Sun Microsystems via software initiatives (more integration into Windows, and Java, respectively).

### *Screening, Scanning, Surveillance*

Products and services involving screening and scanning include equipment capable of detecting chemical, biological, and nuclear reagents to mitigate the threat of large scale disasters. X-ray systems and other screening devices exist to detect radiation or simply screen luggage at airports or cargo shipments and major ports. Indeed, technology used to screen luggage and cargo is one of the fastest growing areas in Homeland Security. Additionally, firms market and sell audio and video surveillance systems and communication interception equipment and software. Companies competing in the space include American Science & Engineering (NASDAQ: ASEI), Mercury Computer Systems (NASDAQ: MRCY), Nice Systems (NASDAQ: NICE), OSI Systems (NASDAQ: OSIS), RAE Systems (NYSE: RAE), and Verint Systems (NASDAQ: VRNT). Verint and Nice offer products that monitor voice and e-mail communication. Another e-mail tracking firm is Websense (NASDAQ: WBSN) that verifies if employees are adhering to respective firm Internet and e-mail policies. Video surveillance products have received increased attention due to the recent bombings at the London Underground subway; the market is currently estimated at several billion dollars.

Project 'US-VISIT' was initiated at the end of 2004 and is being led by consulting firm Accenture (NYSE – ACN). This project is meant to track non-U.S. visitors at domestic air, sea, and land ports – estimated at approximately 400 entry/exit points and is will employ biometric information such as fingerprint scanning and photo ID's, as well as RFID systems.<sup>xxii</sup>

### *Border Security*

Border security will receive one of the largest increases in funding as part of the 2006 Homeland Security Budget recently approved by the Senate. Michael Chertoff has advocated increases in border security guards and equipment such as cameras and other monitoring equipment.<sup>xxii</sup> He is also recommending additional room for detention facilities and judicial facilities near borders with additional judges.

### *Chemical Industry*

The chemical industry is viewed as having fought against any required guidelines to protect itself from terrorist attacks.

### *Transportation Industry*

The railroad industry is at the forefront of Homeland Security due to the amount of goods it transports annually and lax security in moving such large volume. Mr. Chertoff, in a recent interview<sup>1</sup>, highlighted that trains carrying chlorine pass closely by Washington D.C. and that these types of activities need to be monitored more closely. He also noted that transportation dynamics vary among industry, e.g. airlines can also be used as a weapon when hijacked while trains represent less of a security concern from this perspective.

Additionally, the aviation industry is understandably a major are of focus by the Department. It is estimated that there are approximately 6,800 commercial airplanes in the U.S. alone. Due to the size of the industry and high degree of regulation, security initiatives tend to be extremely costly. For instance, it is estimated that it would take billions of dollars to equip airliners with anti-missile systems to stem the threat of shoulder-held rocket launchers.<sup>xxiii</sup>

### *Cyber Security*

According to a recent Barron's article<sup>xxiv</sup>, the U.S. government is in the midst of a major overhaul of its national security network as a result of Homeland Security efforts. The article estimates that the government has approximately 1.3 million cryptographic devices and that it plans on revamping nearly 75% of them at an estimated cost of \$8-\$10 billion. Of that amount, an estimated \$2 billion has been earmarked 'Type 1', or equipment for the proper encryption of data used for military, intelligence, and law enforcement agencies. Companies competing in this

space include pureplay SafeNet (NASDAQ: SFNT) and larger defense firms such as General Dynamics (NYSE: GD) and L-3 Communications (NYSE: LLL).

#### *Information Technology (IT)*

Akin to cyber security, information technology is another area that has seen increased resources devoted to securitizing public and private networks to protect information from hackers. Unisys Corporation (NYSE: UIS) competes in this space; it has an estimated \$2.5 billion backlog in government contracts, a portion of which are related to Homeland Security. Other IT outsourcing firms such as CACI International (NYSE: CAI) and SRA International (NYSE: SRA) are actively pursuing federal contracts. Standard & Poor's expects IT outsourcing to be among the fastest growing areas in national security initiatives.<sup>xxv</sup> S&P also detailed that Input, a market research firm, estimates that federal agencies awarded approximately \$115 billion in IT-related contract awards in 2003; this represented over 90% growth from the previous year. Input also projects that federal IT spending will reach \$71 billion in 2005 and grow at least 30% \$92 billion by 2010.

#### *Communication*

As will be further detailed below, federal and local agencies are actively developing and enhancing information sharing regarding the tracking of individuals thought to be planning terrorist actions. Domestic entities are increasingly developing their own communications infrastructure to track and respond to security initiatives. Private sector firms such as Motorola are working with police organizations around the country to share real-time data. In the case of Motorola, approximately 20 police forces are planning on sharing a system in which it will be possible to dial one number and gain direct entrance into a conference call.<sup>xxvi</sup>

#### *Services*

This area includes armored transport, home and personal security (Brinks, ADT), background screening, security clearance, classified services for U.S. intelligence agencies, and other intelligence equipment and systems. Companies competing in the space include CACI International (NYSE: CAI), First Advantage (NASDAQ: FADV), and SRA International (NYSE: SRX).

The above identified certain commercial technologies that are expected to prove useful in the global fight against terror. In the industry overview below we identify areas in which these technologies can be exploited.

## **Industry Overview**

### Industry Drivers & Characteristics

The changing role of the U.S. military represents a significant driver in global defense and related services and preparedness. The Department of Defense is actively working to modernize and reshape the face of national security. On February 16, 2005, Donald Rumsfeld testified before the House Armed Services Committee in Washington and detailed philosophical shifts that have become an integral part in shaping the nations security policy. Transcripts from the testimony described the U.S. as still at "war in a complex and rapidly changing security environment" and that "our armed forces are experiencing the most severe challenges and demands that have been placed on them in decades." This has driven above average growth rates in military spending since 2001 and is expected to continue through at least 2006. According to Standard & Poors (S&P) estimates, military procurement and spending on what it terms research, development, testing, and evaluation (RDT&E) will grow 7.3% and 3.0% for the fiscal period ended December 2006. After that it expects expansion to grow at much lower rate as the government becomes increasingly concerned with other domestic issues such as reforming social security and Medicare. In an industry survey on aerospace and defense<sup>xxvii</sup>, S&P also identified the changing

role in the military as it evolves to fighting larger numbers of smaller conflicts and has less of a need to stockpile large amounts of weapons and 'traditional' weapons systems such as fighter jets, battleships, large numbers of tanks, etc.

Shifts in strategy are having a profound influence on where defense funds are allocated. As a case in point, the government is using homeland security as a criterion in determining whether to keep military bases operational. According to an article on the subject, "Congress agreed to a new round of base closings before the 2001 terrorist attacks, but the new emphasis on homeland security is reflected in the military's closure criteria drawn up after the attacks. The military says it will consider a base's potential use as a "staging area . . . in homeland security missions."<sup>xxviii</sup>

Previously, following the end of the cold war, the Pentagon adjusted its strategy and made arrangements for the ability to fight two large scale conflicts, or 'major regional contingencies' (MRC's) at the same time. Subsequent to the terrorist attacks on the World Trade Center, in late September 2001 this change in philosophy evolved further and immediately shifted focus to homeland defense and counterterrorism measures. The Pentagon has now moved to prevent terrorists from exploiting weaknesses in U.S. defense systems and capabilities. The missions of the National Strategy for Homeland Security is a major by-product of this shift in strategy

#### Six Defining Missions

The National Strategy for Homeland Security defined six missions under which it believes best categorize areas that should represent the primary focus on to prevent future domestic attacks. Though introduced previously, each mission will be explained further below.

#### Intelligence & Warning

The Strategy details that it is necessary to have systems in place to eliminate the element of surprise as much as possible such as an early warning mechanism made possible by sophisticated intelligence and warning capabilities. The report pointed to the Pearl Harbor attacks in 1941 as an example where intelligence and warning failed the country; the events of 9/11 represent another systemic breakdown in our national intelligence: a bipartisan commission named to investigate the shortcomings in national security described that a number of the 9/11 hijackers were able to pass through to the U.S. without having received stamps on their passports.<sup>xxix</sup> A success referred to were the billions of dollars spend during the cold war to "detect indications of a nuclear attack by the Soviet Union", which provided an effective deterrent to the Soviet Union and possibly prevented any significant widespread conflict during this period. Further details of the United State's domestic intelligence are provided below, as are foreign initiatives

#### *Domestic Intelligence*

The Strategy noted the need to perform a timely and thorough analysis of intelligence to prevent future terrorist acts. It also stressed the need to have a "deep understanding" of the enemy and how it is organized in order to proactively determine where and how it may act. With proper systems in place, government agencies are expected to be able to warn the private and public sector and how to best take protective action. The Office of Homeland Security also listed its major initiatives:

- Enhance the capabilities of the FBI
- Build new capabilities through the Information Analysis and Infrastructure Protection Division of the Department.
- Implement a Homeland Security Advisory System
- Utilize dual-use (equipment and material that have both terrorist and legitimate commercial uses) investigations to prevent attacks

### *Foreign Intelligence*

Foreign intelligence also has an important role to play in identifying possible attacks and preventing such action. The U.S. is actively cooperating with foreign governments and entities to share information and intelligence to prevent attacks on an international scale. Countries that share borders with the U.S. are clear priorities in terms of sharing information regarding the flow of individuals, goods, electricity, oil and gas pipelines, etc.

Of course it will always be difficult to corroborate specific or actual threats as witnessed over recent speculation that threats on New York City's transit systems were a hoax.

### **Border & Transportation Security**

According to the Strategy, the U.S. coastline represents an astounding 95,000 mile border across the country. Additionally, it shares a very large land border with Canada (5,525 miles) and also a significant border with Mexico (1,989 miles). Modes of transportation and entry are possible via the following sources: seaports, airports, highways, pipelines, railroads, and waterways. The overriding mission is to create 'smart borders' that efficiently manage the process and flow of goods and people and better identify and prevent suspicious and illegal activities.

Following is a brief description of each important initiative:

#### *Land/Air/Sea Transport*

The use of maritime shipping containers has been identified as a serious deficiency in national security. Approximately 90% of international cargo is transported via shipping containers; in the U.S. it is estimated that 50% of all imports reach the U.S. in over 16 million containers annually. Homeland Security initiatives are in place to better identify 'risky' containers or entities shipping them, increasing the number of maritime inspectors on site, and focusing on large ports that represent the majority of shipments into the U.S. RFID technology is expected to play a role in tracking goods shipped and received via major maritime ports as it allows for a more detailed inspection of goods as compared to physical, human inspection. A study conducted by Bearingpoint, a U.S.-based consulting firm, estimated that enhanced security efforts could lead to financial benefits totaling \$220 per container, implying that security efforts could lead to efficiency gains in terms of cost reduction and the more timely shipment of goods.

It is currently estimated that nearly all maritime cargo shipments are screened in terms of who the shipper is, what the source and destination of the goods are, and details of the ship being used. The Department of Homeland Security intends on working towards a pre-clearance of shippers, thus decreasing the almost impossible task of inspecting every container that enters through national ports.

Other areas of focus include an increased commitment on better capitalizing the U.S. Coast Guard. The U.S. Budget for 2003 included what amounted to the largest increase in funding in the Coast Guard's history for a proposed improvement in the organization's aging fleet and enhanced 'command and control' systems. As previously detailed, 95,000 miles of border between the U.S. and its coastline represents an almost unfathomable amount of area to cover and prevent illegal entry into the country. Other significant government initiatives include the Container Security Initiative (CSI) and the Smart and Secure Tradelanes (SST) program.

So far, according to AIM Global, CSI has been implemented at the top 20 foreign ports that the organization estimates account for about 66% of the volume of containers to U.S. ports. Governments involved in these ports such as Thailand and China have agreed to implement CSI according to AIM.<sup>xxx</sup>

CSI consists of four core elements<sup>xxx1</sup>:

1. Establish security criteria for identifying high-risk containers based on advance information.
2. Pre-screen containers at the earliest possible point.
3. Use technology to quickly pre-screen high-risk containers.
4. Develop secure and "smart" containers.

*Land/Air/Sea Border Control*

The Department of Homeland Security is in the process of improving the way it collects and analyzes data at its borders. This includes an increase in information gathered, and better record keeping systems identifying a person's reason for entering and exiting the country, frequency of visit, and goods brought into or out of U.S. borders. Agencies are in the process of creating effective biometric capabilities which are able to record items such as fingerprints, retinal scans, etc.

**Domestic Counterterrorism**

Counterterrorism, or the intent to prevent or 'counter' acts of terrorism, represents one of the most important yet difficult acts in the fight against acts of terror. To effectively be proactive in identifying future threats, it becomes necessary for all intelligence agencies to share information in a more timely and efficient manner (for instance, it has been noted that international agencies (e.g. those tracking information regarding attacks on the USS Cole) had information on terrorists who committed the acts of 9/11 but did not share this information with the FBI). It is also necessary to identify how terrorists receive their funding and 'interdict', or prevent the means with which they obtain money, weapons, and capital. This function is seen as resting in the jurisdiction of the FBI.

The prevention of terrorism also includes the ability to apprehend fugitives, question potential terrorists, and track their activities. Countermeasures include watch/wanted databases, intergovernmental information sharing as well as the coordination of data flow with private entities such as airlines, transportation organizations, and companies that produce dual-use goods and services. An overhaul of the FBI is also seen as improving counterterrorism efforts, as is the intent to continually work to improve and enhance intelligence efforts among private and public organizations.

**Protection of Critical Infrastructure and Key Assets**

"The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack. Our country will continue to take immediate and decisive action to protect assets and systems that could be attacked with catastrophic consequences. We will establish a single office within the Department of Homeland Security to work with the federal departments and agencies, state and local governments, and the private sector to implement a comprehensive national plan to protect critical infrastructure and key assets."<sup>xxxii</sup>

Figure 1.7

<i>Sectors Critical to Protecting U.S. Infrastructure</i>
<i>Agriculture</i>
<i>Food</i>
<i>Water</i>
<i>Public Health</i>
<i>Emergency Services</i>
<i>Government</i>
<i>Defense Industrial Base</i>
<i>Information and Telecommunication</i>
<i>Energy</i>
<i>Transportation</i>
<i>Banking/Finance</i>
<i>Chemical</i>
<i>Postal</i>
<i>Shipping</i>

The Strategy, as quoted above, clearly identifies the need to protect physical, intellectual and virtual fabrics of our society. This includes any intended target of terrorists to adversely affect or cripple the way in which the nation operates (economically, socially, and logistically). Critical infrastructure is defined by the USA Patriot Act as "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or

any combination of those matters.” Key sectors of our economy are detailed in figure 1.7.

In addition, it is important to protect the nations ‘morale’ against acts of terrorism. The events of 9/11 clearly exacerbated the effects of an already weak economy towards the end of 2001; the stock market also was adversely affected and certain industries suffered more than others; several even have yet to fully recover. 9/11 was also seen as having contributed to an increase in ‘cocooning’, or an increase in citizens staying at home rather than traveling, eating out, etc.

Initiatives in the arena of protecting critical infrastructure include:

- Compiling a list of what constitutes America’s key infrastructure and assets.
- Enhancing cooperation between the private and public sector
- Determining how to effectively protect key assets and minimize fallout and further damage if acts of terrorism should occur
- Protecting cyberspace from attacks and inhibit the perverse gathering of information with the intent of causing harm to the nations infrastructure and key assets
- Minimizing ‘inside threats’, or the ability of existing employees in sectors identified above to breach confidential information and share with terrorists. (Lee Harvey Oswald example – employee of book depository).

### **Defense Against Catastrophic Threats**

“America will have a coordinated national effort to prepare for, prevent, and respond to chemical, biological, radiological, and nuclear terrorist threats to the homeland. We will seek to detect chemical, biological, radiological, or nuclear weapons and prevent their entry into the United States. If terrorists use chemical, biological, radiological, or nuclear weapons, our communities and emergency personnel will be organized, trained, and equipped to detect and identify dangerous agents, respond rapidly, treat those who are harmed, contain the damage, and decontaminate the area.”<sup>xxiii</sup>

The main priority at the Department of Homeland Security is to prevent a catastrophe more devastating than the events of 9/11. Initiatives include ways to document inventories of chemical, biological, radiological substances and weapons or key inputs used to manufacture items such as nuclear weapons. Additionally, it is important to prevent the theft or improper use of such inventories, both domestically and internationally. Cooperation with the Centers for Disease Control and Prevention (CDC - <http://www.cdc.gov/>) is important, as is the need to work effectively with the scientific community to develop the knowledge and systems to prevent tragedies.

### *BioDefense*

Project BioShield is estimated to receive \$2.5 billion in funding. This initiative is meant to encourage the preparation for attacks by creating medical countermeasures and creating the ability to better monitor biologic agents in cities and other high threat areas.

### **Emergency Preparedness & Response**

“We will strive to create a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic, as well as all manner of natural disasters. Under the President’s proposal, the Department of Homeland Security will consolidate federal response plans and build a national system for incident management.”

### *Preparedness*

The Department for Homeland Security has been working to improve the nation’s ability to quickly and resolutely respond to a breach of national security. The Strategy references the importance of the ‘first responder community’, or individuals such as firefighters, policeman, medical professionals, and other public officials that proved impressively poised and effective after the events of 9/11. To enhance the nation’s ability to respond to threats, major initiatives include:

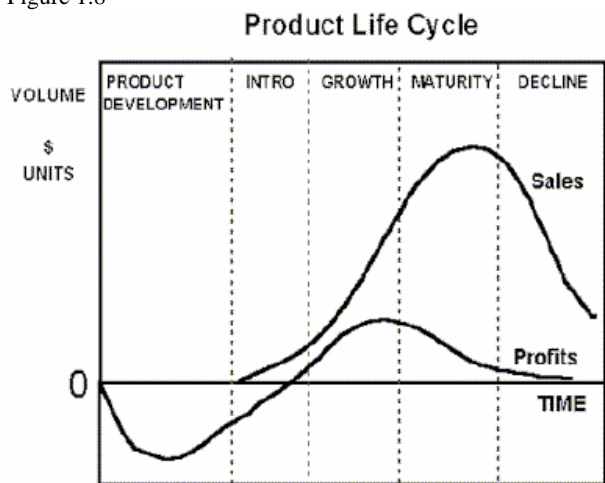
- Create a national system to respond to threats and disasters in a coordinated fashion.
- Enhance communication between agencies and organizations that are expected to be first responders as well as those that will deal with the medium-term and long-term effects of any disaster
- Ensure that the nation has access to and an adequate inventory of vaccines, medical supplies, antibiotics, antidotes, etc. This will help individuals survive attacks and provide for quick decontamination from chemical, biological, or radioactive materials released.
- Coordinate military involvement on a civil scale
- Practice disaster relieve efforts to enhance preparedness should an actual disaster occur.

A recent Wall Street Journal article<sup>xxxiv</sup> highlighted deficiencies in federal initiatives to coordinate communication between federal agencies and first responder entities. The article cited that police agencies in major metropolitan areas such as Los Angeles, Washington D.C., and Houston, among others, that are working with foreign police agencies and global entities to share information regarding terrorist actions and co-develop response programs.

### Investment Characteristics

Homeland Security stocks have experienced significant share price appreciation since 2001. As witnessed by any industry thrown into the forefront of development and hype for a multitude of reasons (witness automotive stocks in the early 1900's, Internet and biotechnology companies in the late 1990's), Homeland Security stocks have been subject to volatile (and often impressive) performance over the past 3 1/2 years. Numerous security-related indices have outperformed the S&P 500 over this timeframe. Sell-side investment research firm Lehman Brothers estimates that its basket of 27 security stocks appreciated nearly 320% in a three-year period that began in August, 2001 while the S&P 500 returned only 5% during that period. Recent report also detailed that its index far outperformed the market in 2004 and during a 12-month period through October 2004.<sup>xxxv</sup> Morgan Keegan, another sell-side research firm, estimates that its own index of 13 security firms outperformed the market in 2004. The ISE-CCM Homeland Security Index will also be tracking performance of its broader index going forward.

Figure 1.8



Homeland Security companies in general are in the product development/introduction phase of the product life cycle (Figure 1.8). These phases are characterized by large amounts of R&D to develop technology and know-how, infusions of capital from outside sources as most companies are not yet generating significant amounts of internally-generated funds, and insignificant revenues to date. Larger defense companies most likely operate in the maturity phase of the product life cycle due to large, recurring amounts of revenue and already established products. The creation of the Department of Homeland Security and initiatives to drastically change the

nation's security efforts have shifted the industry towards the left-hand side of the life cycle as focus has shifted to innovation and as-of-yet unproven technologies.

#### Investment Merits/Drawbacks

In the public sector, major players in the Homeland Security market include federal agencies, state governments, and first responder organizations such as local municipalities. In the private sector, major players can be divided into incumbent security firms, large firms with a security presence, and smaller, entry level players with niche products or burgeoning technologies.

#### Valuation Methodologies/How to Analyze

More incumbent Homeland Security companies can be analyzed employing traditional valuation techniques such as Price/Earnings ratios, Enterprise Value/Sales, or Price/Growth metrics. For younger firms, R&D as a percentage of revenue is a useful measure to gauge the amount being invested in future technologies. It is also useful to look at macro trends and attempt to identify significant technologies with potentially lucrative commercial opportunities. The potential of investing in the space is also one of its main drawbacks: the relatively small size of companies competing in the space means that they can grow rapidly and quickly take advantage of new opportunities. However, this means that the companies have less diversified product mixes and customer bases; as such, any contract or customer loss can adversely affect profitability and at times survival of smaller firms.

#### Major Industry Players

In addition to firms identified above in the *Commercial Opportunities* section, large, incumbent firms are best able to offer a broad range of services to the federal government and other security organizations. Companies such as Honeywell (NYSE: HON - security equipment) Siemens (NYSE: SI - fire monitoring, systems integration), General Electric (NYSE: GE - security equipment and services), Ingersoll Rand (NYSE: IR - systems services and integration) United Technologies (NYSE: UTX - monitoring, guard services), Tyco (NYSE: TYC - through ADT, its home security segment) Marsh McLennan (NYSE: MMC - through its acquisition of Kroll O'gara), Stanley Works (NYSE: SWK - systems integration and services), and Diebold (NYSE: DBD - systems services and integration) are already well established in the space and are expected to remain dominant as customers demand 'turn-key' solutions, or the ability of one provider to offer a broad array of services and allow one source for a number of services.

Defense Companies are a logical fit in terms of being able to offer a multitude of Homeland Security services and products. Due to longstanding relationships with government entities, international security expertise, and well-established infrastructure, defense firms are serious competitors in the space. Examples of such firms include Armor Holdings (NYSE: AH), Lockheed Martin (NYSE: LMT), Boeing (NYSE: BA), L-3 Communications (NYSE: LLL), General Dynamics (NYSE: GD), Northrop Grumman (NYSE: NOC) and Raytheon (NYSE: RTN).

Medium-size players that usually represent pure plays in the areas in which they do business. Medium players include firms such as The Brink's Company (NYSE: BCO), Symbol Technologies (NYSE: SBL), and Identix (NASDAQ: IDNX), among others.

## Homeland Security – Recent Developments<sup>xxxvi</sup>

Excerpted from the Department of Homeland Security Press Room:

### **DHS Announces \$30 Million in Competitive Grants to Strengthen Preparedness Training**

September 30, 2005

The Department of Homeland Security (DHS) announced today \$30 million in Competitive Training Grants. DHS awarded funding to fifteen organizations for training initiatives that further the Department's all hazards mission of preparing the nation to prevent, deter, respond to, and recover from incidents of terrorism and natural disasters.

The training programs developed from the grants will strengthen preparedness training for first responders, public officials and citizens. The new training programs will enhance preparedness in a variety of areas, including intelligence assessments, citizen readiness, transit and port security and mass casualty care.

### **National Cyber Security Alliance and Department of Homeland Security Promote Online Safety for National Cyber Security Awareness Month**

September 27, 2005

The National Cyber Security Alliance (NCSA) and The Department of Homeland Security today announced the launch of key programs and events to educate Internet users of all ages about safe online practices throughout October in observance of National Cyber Security Awareness Month.

National Cyber Security Awareness Month unites entities from federal, state and local government as well as the education and business communities, all of whom share a common goal to educate the public and provide tools to help them engage in safe online activity. The NCSA is recognized as a central clearinghouse for consumer education and information about online safety. The organization works closely with Homeland Security, the Federal Trade Commission (FTC) and a variety of other public and private organizations to ensure that messages about online safety and security are accurate and consistent.

### **New Smart Card System to Coordinate First Responders in the National Capital Region**

August 25, 2005

The National Capital Region (NCR) is leading the nation in identifying first responders with a new smart card credentialing effort. The First Responder Partnership Initiative (FRPI) is designed as a model for other regions to enhance cooperation and efficiency between state and local first responders and their federal counterparts.

“We are excited to launch an effort that will help the country better coordinate its most valuable resources -- its people -- during an incident,” said Tom Lockwood, Director of the Department of Homeland Security’s Office of National Capital Region Coordination. “I encourage state and local governments to adopt the interoperable technology to support mutual aide across jurisdictional lines.”

The architecture of the card, which uses the FIPS 201 and 14443 contactless standards, will identify first responders and their qualification(s) at the site of an incident, so they may move rapidly into, out of, and within an area in a trusted and secure manner. The card will be recognized across all NCR federal, state, and local multi-jurisdictions.

The smart card technology is standards-based and can serve as a platform for:

- physical access into buildings
- logical access to networks
- human resource asset accountability
- incident command and control
- property/firearms accountability
- National Incident Management System (NIMS) integration

**Statement by Homeland Security Secretary Michael Chertoff on Lowering the National Threat Level for the Mass Transit Sector**

August 12, 2005

Since raising the threat level for mass transit systems on July 7, the Department of Homeland Security has been working closely with our federal, state and local partners to develop and implement sustainable mass transit security measures tailored to the unique design of each region's transit system. In light of these increased long-term measures, DHS is lowering the national threat level for the mass transit portion of the transportation sector from Code Orange, or "high," to Code Yellow, or "elevated."

These changes will be effective at 8:00 p.m. local time on Friday, August 12, following local rush hours across the country, at the discretion of state and local authorities. Concurrently, the Coast Guard will lower the Maritime Security level for large passenger ferries from level two to level one, which corresponds with Code Yellow.

Although the overall national threat level is being lowered for mass transit systems, many transit systems, particularly the larger systems, will maintain a strengthened baseline level of preparedness beyond what existed before the London attacks, including a number of the security enhancements that were put into place for the July alert. Additionally, individual transit systems should vary these security measures at any given time in order to make it more difficult to predict the security regime at any given location.

The Department of Homeland Security will continue to closely coordinate with our federal, state, local and private sector partners and we will share any information developing from the London bombing investigation to continue to address potential vulnerabilities in the mass transit sector. At this time, there is no specific, credible intelligence information indicating that an attack in the United States is imminent. However, we are also aware that the London and Madrid bombings were conducted without warning. Therefore, we will continue to closely monitor and analyze threat information and share that information, together with guidance for protective measures, with state, local and private sector authorities as well as the general public as part of the sustained national effort to prevent terrorist attacks and protect our homeland.

While we are changing the threat level at this time, we continue to urge state and local officials, transportation authorities and the general public to remain alert. Public vigilance is very important, and we encourage all citizens to keep a watchful eye for items left unattended or suspicious behavior and report any incidents to local authorities immediately.

**US-VISIT Begins Testing Radio Frequency Identification Technology to Improve Border Security and Travel**

August 8, 2005

The U.S. Department of Homeland Security (DHS) has begun testing the US-VISIT Program's next phase of implementation, which uses radio frequency identification (RFID) technology to more efficiently record the entries and exits of visitors who are currently issued an I-94 (Arrival/Departure Record) at our land borders. Five U.S. land border ports will test the RFID technology from August 4, 2005, through early summer of 2006. The ports are Nogales East (Deconcini) and Nogales West (Mariposa) in Arizona; Alexandria Bay (Thousand Islands) in New York; and Pacific Highway and Peace Arch in Washington state.

US VISIT is a continuum of security measures that collect biometric and biographic information from visitors at U.S. visa-issuing posts around the world, and upon their arrival in and departure from U.S. air, sea and land border ports. Experience has shown that the US-VISIT enrollment process is fast, easy to understand and simple for visitors.

**Statement by Secretary of Homeland Security Michael Chertoff on the Bombings in London**

July 7, 2005

We have been closely monitoring the bombings in London. Our sympathies and condolences go to the victims of this incident and the people of London.

We have been in direct communication with officials at the state and local level and with public and private sector transportation officials. We have asked them for increased vigilance and additional security measures for major transit systems.

The Department of Homeland Security has stood up the Interagency Incident Management Group to ensure full situational awareness around this incident and in the United States. We do not have any specific intelligence indicating this type of attack is planned in the United States, but we are constantly evaluating both intelligence and our protective measures and will take whatever actions are necessary.

Additional Homeland Security news can be found at: [www.ccmsectorinvest.com](http://www.ccmsectorinvest.com)

## **ISE-CCM Homeland Security Index**

The International Security Exchange – Cronus Capital Markets (ISE-CCM) Homeland Security Index (HSX) includes companies engaged in contractual work with the Department of Homeland Security, law enforcement agencies, or providing products or services for the following efforts: intelligence and warning; border and transportation security; domestic counterterrorism; protection of critical infrastructure; defense against catastrophic threats; and, emergency preparedness and response.

The following is excerpted from the most recent ICE-CCM Homeland Security Index September report:<sup>xxxvii</sup>

The index is a sampled, fixed-number constituent, modified market capitalization-weighted index that is adjusted for free-float shares. It is a “RIC”(Regulated Investment Company) compliant index of 30 select, small, mid, and large capitalization US companies. These Homeland Security companies are described as some of the largest, most liquid, and most mature of the entire sector. The index is intended to represent, in a balanced fashion, the complete Homeland Security Sector and related missions. Due to the non-uniform weight distribution across the sector, a “modified” market capitalization-weighted methodology is used to limit individual component weightings to 25%. This modification prevents a few large component stocks from dominating the index and distorting an index return that is representative of an industry sector. The modified approach is seen as promoting portfolio diversification by retaining the economic attributes of capitalization ranking.

The index is calculated on a price and total return basis. The price Index is calculated in real-time and disseminated via the Options Price Reporting Authority (OPRA) and market data vendors every day the U.S. equity markets are open. The total return Index is calculated on an end-of-day basis. Both sets of values are available on ISE’s website at [www.iseoptions.com](http://www.iseoptions.com). HSX intends to continually contain 30 different component stocks at all times. New companies are added to the Index only when there is a vacancy. Companies may not apply, and may not be nominated, for inclusion in the Index. Companies are added or removed by the ISE and CCM based on the methodology described herein. Whenever possible, ISE will publicly announce changes to the index on its website at least five trading days in advance of the actual change.

The HSX was jointly developed by ISE and CCM. CCM, an independent and privately owned capital market research and consulting firm, provides specific research and support for the Index. The index includes thirty stocks. It is also a modified cap-weighted index. Therefore, the larger companies within the index will have a slightly greater weighting within the index compared to smaller firms. Figure 1.8 shows the components of the HSX. L-3 Communications, McAfee (NYSE: MFE), and Thermo Electron (NYSE: TMO) are the three largest and account for approximately 30% of the overall index.

Figure 1.8  
ISE-CCM Homeland Security Index (HSX)

Symbol	Name
ACTI	ACTIVCARD CORP
ANT	Anteon International Corp.
APSG	Applied Signal Technology
CAI	CACI International Services
CHKP	Check Point Software
COGT	Cogent Inc
CPHD	CEPHEID INC
FLIR	FLIR Systems
HEPH	HOLLIS-EDEN PHARMACEUTICALS
HRS	Harris Corp.
IDNX	Identix Inc.
ISSX	Internet Security Systems
LLL	L-3 Communications Holdings
MANT	ManTech International 'A'
MFE	McAfee, Inc.
MSA	MINE SAFETY APPLIANCES CO
OSIS	OSI Systems Inc.
RAE	RAE Systems
RSAS	RSA Security Inc.
SINT	SI INTERNATIONAL INC
SRX	SRA INTERNATIONAL INC-CL A
STE	STERIS Corp.
TASR	Taser International
TMO	Thermo Electron
TTEK	Tetra Tech
UIS	Unisys Corp.
VISG	Viisage Technology Inc.
VRNT	VERINT SYSTEMS INC
WGII	WASHINGTON GROUP INTL INC
ZBRA	Zebra Technologies'A'

Like most index options, the contract settles European style and for cash. Therefore, exercise and assignment can only take place at expiration. In addition, exercise involves the transfer of cash and not shares as with stock options. Strike prices of HSX options are set at 2.5-point intervals. Therefore, with the index up 11 cents to \$63.84 Tuesday afternoon, the HSX was midway between the 62.5 and 65 strikes.<sup>xxxviii</sup>

### Summary & Conclusion

As detailed, the unanticipated events of September 11 ushered in a new era of urgency and devotion by the Bush Administration to protect the United States and its citizens from future terrorist attacks. The resulting creation of the Department of Homeland Security is currently driving security efforts and will continue to have a profound influence on how the private sector evolves to address national security initiatives. Security efforts and initiatives are global in nature and expected to allow U.S. companies to expand international efforts and capture additional global market share.



**INVEST**TREND

**INVESTREND RESEARCH**

**COMPANY RESEARCH DIRECTORY**  
**3<sup>rd</sup> QUARTER 2005**



COMMISSIONED BY



**CRONUS CAPITAL MARKETS**



**R.C. FUHRMANN CFA**



# BlastGard International, Inc.

(OTC BB – BLGA)

## SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY CRONUS CAPITAL MARKETS

Q3 2005

*BlastGard International, Inc. engages in the design, development, manufacture, and marketing of proprietary blast mitigation materials. Its BlastWrap technology mitigates blast effects and suppresses post-blast fires.*

Stock Metrics	
Recent Price	\$0.52
52 Week Range	\$0.45 - \$5.00
Market Capitalization	\$ 16.4 million
Enterprise Value	n/a
Trading Volume	17,000
Beta	n/a

### Company & Homeland Security Products Overview

BlastGard has a unique and potentially soon-to-be very sought after product, BlastWrap™. This new blast mitigation technology profoundly reduces the shock and thermal blast effects of explosives, and accordingly offers significant protection to people and assets in the blast area. BlastGard's products are currently in use on mitigated trash receptacles. This 'trash can' manages a very large blast (charge size is restricted info). In comparison, a competitor's product can only handle a very small (1.6-pound) bomb, and even that charge only in the

less-demanding center of the can. BlastGard's product is the only product available that mitigates all blast effects, the fragments, shock wave and fireball.

### The Product Pipeline

BLGA has developed a product pipeline, in conjunction with its customer base, which will put its product on:

Product	Customer / Partner
Weapons Carriers – Munitions Packaging	Insys, Ltd; UK MoD; Nigerian Army
Vehicle Protection	Colt Rapid, ASI, ONR/USMC
Containerized Cargo	Nordisk Aviation Products
Non-Containerized Cargo	TSA, Battelle Memorial Institute
Buildings	USAF, US Navy
Pipe Bomb Mitigators	Security Science - Proof Testing in Thailand/Bakersfield
BlastGard's Mitigated Trash Receptacles	Amtrak, US Navy, Media Metrica, DHS, Washington Metro

### Product Description

BlastWrap™, in its basic form, is a "bubble-wrap" style material that reduces, or mitigates, the effects of an explosive blast using an attenuating media inside the "bubbles". Often BlastWrap™ is married with other technologies to accomplish a complete solution. For example, an armored vehicle may use BlastWrap™ on the underside. The BlastWrap™ would be covered by a thin frangible hard skin to provide a durable outer surface, and it may include additional armor on the backside. The skin protects the BlastWrap™ in regular vehicle use (rocks, sticks, etc.), keeping the passive BlastWrap™ "sandwich" ready to mitigate a blast in less than one millisecond.

### Sales / Revenue Estimates

BlastGard has current sales revenue from its product and is estimating sales revenue for 2006 of over \$6mm. With the acute need for the BlastGard product in the Homeland Security sector, these estimates seem obtainable. Positive test results and product development will need to take place with current and future sales partners to achieve the estimates.

## Financial Overview

<http://finance.yahoo.com/q/ks?s=blga.ob> As can be seen from the Financial Overview, BLGA is a micro cap investment. Float and volume are low, as is normal with this type of investment.

## Positioning in Homeland Security Industry

BLGA operates within the services sector. Its main competitor in trash receptacles is an Israeli security firm that makes a similar product. However, the competitor's product does not provide the same level of blast mitigation and this should prove to be a large advantage for BlastGard.

## Selected Management Biography

*James F. Gordon - Chairman, CEO and Board Member and Co-inventor of BlastWrap*

Mr. Gordon is responsible for the overall policies, management development and the Company's future expansion and promotion of **BlastWrap™** products. Mr. Gordon has 25 years of sales and marketing experience as a licensed real estate broker and appraiser. Mr. Gordon received his Bachelor of Science Degree from Monmouth University, West Long Branch, New Jersey. Mr. Gordon is also a U.S. Army veteran.

*Kevin J. Sharpe - Vice President, Engineering & Product Development*

Mr. Sharpe has over 20 years experience in explosive engineering, structural response to blast loading and ballistic impact, explosives and munitions design and ordnance disposal. From 1981 through 1993, Mr. Sharpe was a research scientist at a defense establishment in Essex, England conducting research into blast mitigation systems, training UK and US military in use and deployment of blast mitigation and related systems. Born in London, England, Mr. Sharpe received his Higher National Certificate in Mechanical Engineering and Applied Physics from Anglia Higher Education College, Cambridge Explosive Engineering.

*Howard Safir – Board Member and Consultant*

Mr. Safir was the 39<sup>th</sup> Police Commissioner of New York City and served during the same period that Rudolph W. Giuliani was mayor of New York City. Mr. Safir has been a distinguished member of law enforcement for over forty years and has held various posts at the Federal Bureau of Narcotics, the Drug Enforcement Agency, the U.S. Marshals Service and he also served as the New York City's 29<sup>th</sup> Fire Commissioner.

*Herbert K. Fallin, Jr. - Consultant*

Dr. Fallin had a long and distinguished career in advanced technology and acquisition. From 1964 to 1978, Dr. Fallin worked in the Ballistic Research Laboratories and then the Army Material Systems Analysis Activity at Aberdeen, Maryland. Dr. Fallin received his Bachelor of Arts degree in Mathematics, Physics and Education from Western Maryland College in 1962, a Master of Arts Degree in Mathematics from West Virginia University in 1964, and a Doctorate in Statistics from the University of Delaware in 1972.

## Concluding Remarks

BlastGard International, Inc has a competitive product that is well suited for the homeland security mission. The company has current sales to finance ongoing product development. BLGA may be a suitable addition to the higher risk portion of a well-diversified portfolio.

**Analyst's Statement:** "I have prepared this report, and the content within it, including all opinions, are solely my own." The analyst is Gary Vassalotti. The analyst's biographical details are at <http://www.investrend.com/articles/secondlevel.asp?level=238>

**BlastGard International, Inc.**, 12900 Automobile Rd, Suite D, Clearwater, FL 33762, Michael J. Gordon., 877-812-7000 Web site:

<http://www.blastgardintl.com/> The company's **InvestorPower™** page is at <http://www.investrend.com/company/list.asp?sPathParam=yes>

**Cronus Capital Markets**, P.O. Box 1022, TD Centre Postal Station, 77 King St. West, Toronto, Ontario M5K 1P2, Phone (888) 901-7090. e-mail: [query@cronuscapitalmarkets.com](mailto:query@cronuscapitalmarkets.com) Web site: <http://www.cronuscapitalmarkets.com>

**Investrend Research and Investrend Research Syndicate, Div.**, Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com). Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com).

**Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply "recommendations" to any reports nor the companies covered. Any usage of the word "recommendation," if any, is to be defined as a "rating" only. We subscribe to the "[Standards for Independent Research Providers](http://www.firstresearchconsortium.com)" at <http://www.firstresearchconsortium.com>

© Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.



# Bulldog Technologies

(OTC:BB – BLLD)

## SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY CRONUS CAPITAL MARKETS

Q3 2005

*Incorporated on 23rd September 1998, Bulldog Technologies (BC) Inc. was founded by Mr. John M. Cockburn. Bulldog Technologies (BC) Inc. was formed to embark on the business of designing and developing an effective and robust security system for the cargo transportation industry.*

Stock Metrics	
Recent Price	\$0.96
52 Week Range	\$0.80 - \$2.42
Market Capitalization	\$24 million
Enterprise Value	n/a
Trading Volume	62,000
Beta	n/a

### Company & Homeland Security Products Overview

Bulldog Technologies Inc. is a designer and manufacturer of wireless security solutions and sensor networks that monitor and secure valuable cargo in the global supply chain. The company's solutions use advanced wireless technologies and web-based software to track, monitor and secure goods in transit, stored in distribution centers, in ports or holding yards. The Company intends to sell products to manufacturers of retail, pharmaceutical and high-tech goods. It also focuses on providing advanced security products to law enforcement, freight haulers and government entities focused on commerce through ports and across international boundaries. Bulldog has pursued a strategy based on three key initiatives: 1) widen product range and market presence; 2) employ key executives to the sales and marketing, engineering and finance functions, and 3) embark on a plan to ramp-up production and sales.

### PRODUCT LINE:

Bulldogs products are currently in development and/or in the process of being released into the marketplace. Products allow clients to track shipments via the Internet, provide real-time information on locations and other data on shipments, monitor the integrity of sealed goods, and track devices via GPS and related technologies. Below are more specific details on the company's five main products.

1. The Bulldog MiniBOSS™ is a cellular based GPSOne AGPS (Assisted Global Positioning System), covert asset tracking, monitoring and recovery device and is designed to work in conjunction with the Bulldog Security Gateway™, a proprietary software application that enables users to securely track their shipments on a simple web based application.
2. The RoadBOSS™ RB-600 is a portable, reusable external seal/sensor for monitoring trailers and containers at any time during the supply chain delivery process.
3. The YardBOSS™ is a portable, external yard security seal/sensor designed to protect loaded containers/trailers while being stored in yards and offers the ability to monitor door seal integrity and any trailer movement.
4. The TankerBOSS™ is a triple-redundant electronic security solution that simultaneously monitors internal fluid levels and all ingress / egress points on tanker trucks. It interfaces to existing Automatic Vehicle Location (AVL) Systems (i.e. GPS, Satellite/Cellular systems) and is scalable - it can be used with various quantities and combinations of level, flow and tamper sensors to match the exact requirement of the application.
5. Bulldog develops open architecture sensor networks and RFID solutions, SensorBOSS™. These solutions come in the form of medium range semi-active sensor tags and network infrastructure, and long range active sensor tags and infrastructure. The Sensor Products are capable of monitoring many types of sensor data.

### Recent News & Developments

New Trackers Help Truckers Foil Hijackings – From WSJ Online Edition

The following excerpt offers brief insight into Bulldog products and target markets: "The devices are supplied mainly by SCintegrity and Bulldog Technologies Inc. of Richmond, British Columbia. SC-trackers go for about \$1,500 apiece, depending on volume, and users pay a monthly fee of \$150 for network airtime associated with

tracking. The Bulldog MiniBOSS trackers cost \$700 apiece, says Richard Booth, vice president of sales at Bulldog Technologies. Air time costs anywhere from \$8-\$80 a month, depending on usage. Sellers say the new trackers will drop in price as the technology spreads, with law-enforcement agencies as well as shippers and carriers using the devices to keep track of goods—particularly high-end products such as the painkiller OxyContin and cigarettes, which can be valued at as much as \$15 million per semi load."

In September, Bulldog's MiniBOSS™ was nominated by Kyocera wireless for Qualcomm's prestigious CDMA 3G A-List Award for Innovation. The A-List Awards are awarded to various technology developers for their work with enterprise wireless data solutions and services. It also received the 2005 Richmond Annual Excellence Award.

Further details on the above and other press releases can be viewed at: <http://www.bulldog-tech.com/>

### **Financial Overview**

<http://www.bulldog-tech.com/investors-filings.asp>

### **Positioning in Homeland Security Industry**

Security products will drive revenue and success at the company. In terms of Homeland Security missions, Bulldog has the ability to serve Intelligence & Warning, Border & Transportation, and even Domestic Counterterrorism initiatives. Specific products include those involved in cargo security, devices for detecting intrusions in shipments and products that are in transit or in storage facilities.

Bulldog estimates the Wireless Location and Services Industry represents an approximately \$25 billion market globally. It also believes the truck and cargo transportation industries are among the largest in the world and need technology to better maintain the integrity of goods in transit and storage. The industry is seen as a slow mover in adaptation of technology but the company believes it is in the midst of a needed technological revolution as a result of increases in terrorism throughout the world. Bulldog has created a line of wireless security systems for the truck and cargo container industry. In North America, this industry has an estimated \$10 billion in reported theft and in excess of \$10 billion unreported theft annually.

### **Competition**

The majority of the company's products are unique with no known direct competition. In terms of other surveillance and tracking firms, those competing in the space include American Science & Engineering (NASDAQ: ASEI), Mercury Computer Systems (NASDAQ: MRCY), Nice Systems (NASDAQ: NICE), OSI Systems (NASDAQ: OSIS), RAE Systems (NYSE: RAE), and Verint Systems (NASDAQ: VRNT).

### **Analyst Coverage Commentary**

Additional research is available at:

<http://www.investrend.com/company/Company.asp?id=1059&sPathParam=yes&sAlias=bld.ob>

### **Management**

Further details on Bulldog's management team can be found at:

<http://www.bulldog-tech.com/corporate-management.asp>

**Analyst's Statement:** "I have prepared this report, and the content within it, including all opinions, are solely my own." R.C. Fuhrmann, CFA, is a member of CFA Institute **Company Contact:** **Unit #301 - 11120 Horseshoe Way Richmond, BC, Canada V7A 5H7 Telephone: (604) 271-8656 Email: [info@bulldog-tech.com](mailto:info@bulldog-tech.com)** This report and other reports regarding this company and others are at: <http://www.investrend.com/articles/secondlevel.asp?level=182>; The company's InvestorPower™ page is at <http://www.investrend.com/company/list.asp?sPathParam=yes> **The analyst's biographical details are at <http://www.investrend.com/articles/secondlevel.asp?level=238>** Investrend Research and Investrend Research Syndicate, Div., Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com) . Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com). **Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply "recommendations" to any reports nor the companies covered. Any usage of the word "recommendation," if any, is to be defined as a "rating" only. We subscribe to the "[Standards for Independent Research Providers](http://www.firstresearchconsortium.com)" at <http://www.firstresearchconsortium.com> © Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.



**Cyber Defense Systems, Inc.**  
(OTCBB: CYDF)

## SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY **CRONUS CAPITAL MARKETS**

Q3 2005

*Cyber Defense Systems, Inc. engages in the design and development of a range of unmanned air vehicles (UAV's). It develops two UAV's, CyberScout that employs a vertical take-off and landing technique, and CyberBug, a scalable unmanned aircraft with day and night vision.*

Stock Metrics	
Recent Price	\$0.48
52 Week Range	\$0.14-\$4.00
Market Capitalization	\$18.6 Million
Shares Outstanding	56.6 Million
Sector	Homeland Security
Avg. Dly Vol. (3-Mo.):	81,000

### Company & Homeland Security Products Overview

Cyber Defense Systems, Inc. ("CYDF" or "The Company") is a development company providing unmanned aircraft ("UAV") chiefly for national defense, but also for law enforcement. Further, it is intended that the Company's UAV's are ideal for fighting terrorism, not only in the U.S but also in products that assist winning conflicts across the globe. The stock is a participant in the currently 'hot'

homeland security sector, offering affordable, proven and important surveillance products. The stock values of the homeland security sector have risen in conjunction with the creation of the Department of Homeland Security and the continuing expectation of a steady stream of government revenue.

CYDF is selling two basic product lines providing low cost solutions with differentiated products in growth niche opportunities around the world with both large and small-unmanned flying aircraft. CYDF is headquartered in St. Petersburg FL, with additional sales and distribution offices located near major customers in both North America and overseas. Recently spun off from Proximity, Cyber Defense Systems, Inc. merged with E City Software, Inc. and began trading under the new stock symbol (BB:CYDF). This merger gave the shareholders of PRXT value for their ownership in CYDF as well as creating additional investment opportunities and allowing CYDF to focus on the security defense security market. The global war on terror has redefined this country and its allies need for security protection throughout the world.

### PRODUCT LINE:

CYDF will be able to offer affordable solutions to all allied countries requiring surveillance, communication or in some cases the delivery of offensive weapons from small UAV's to airships operating up to 20,000 feet with future plans to operate airships in the stratosphere at altitudes beginning at 68,000 feet.

CYDF has completed development on its initial product line and is now offering a very exciting line of small UAV's that will provide surveillance solutions that requires inexpensive airborne tools used to protect civilian and military targets of opportunity from criminals and terrorists. The CyberBug™ as is an innovative product recently introduced to the Defense and Law Enforcement industries. The product is provided at a base system including ground control at a third of the cost of the nearest competitor possibly making this product expendable to many clients. A truly scalable product, CyberBug™ can be built to meet the client's mission requirements. A larger version of the CyberBug™ will provide up to 3 pounds of payload and will fly up to one hour. Flight systems are provided via an autopilot and may be controlled using a combination of handheld joystick with GPS overlay or Internet control. The smaller CyberBug™ comes in a cylindrical tube, which will allow easy transport and product assembly (30 seconds).

On September 19 Cyber Defense acquired 100% of the outstanding shares of Techsphere Systems International, Inc. As a wholly owned subsidiary of Cyber Defense, Techsphere Systems will continue to design, manufacture, sell and lease airships out of its facilities in Georgia. Cyber Defense will continue to work with Techsphere on the sales and

marketing of its Airships as well as the marketing and development of Cyber Defense products. These unique ships in the current configuration hold the world record for altitude. Manufactured by Techsphere Systems International, the spherical airship is ideal for use in persistent surveillance. When completed, these products should provide superior intelligence and communications while maintaining an altitude that will be out of flights patterns and the range of most mobile ground based weapons.

On September 30 Cyber entered into a LOI with VTO Aerospace of Australia creating a new entity called Cyber Aerospace Australia Pty., Ltd. (CAA), and will be a joint venture to manufacture and develop a family of unmanned air vehicles (UAV's). Cyber Defense Systems, Inc. will provide VTOL with solutions that will bridge capability gaps that may be created by a customer's mission requirement.

Cyber Defense recently filed for patent protection with the U.S. Patent and Trademark Office regarding the CyberBug™, CyberScout™ UAV's and the M.A.R.S.™ Modular Airborne Reconnaissance Systems. These products rely on proprietary technology, and CYDF expects that future technological advancements made by us will be critical to sustain market acceptance of CYDF products.

### **DISTRIBUTION**

Cyber Defense is offering both exclusive and non-exclusive reseller agreements for worldwide distribution of the CyberBug™, CyberScout™ UAV's product line. Currently only the CyberBug™, is available for sale. The CyberBug™ is a scalable unmanned aircraft and the Company believes that the product will be a huge success with orders for the product in volumes not simply one or two units. The product has a huge implication in the Homeland environments as well as protecting property across the globe. The Company has defined exclusive resellers as those organizations who will have the exclusive rights within a given geographic area. In order to acquire the exclusive rights to CYDF products the reseller must acquire sufficient product to be able to demonstrate the product in their company's area of influence.

### **DYNAMIC PEER GROUP**

The Homeland Security Group has experienced a soaring share price move. When contracts and the financial profile advance, CYDF emerging presence in this group bodes well for the company stock outlook.

**PEER GROUP:** Armor Holdings (AH), Northrop Grumman (NOC), Lockheed Martin (LMT), CompuDyne (CDCY), Identix (IDNX), Internet Security Systems (ISSX), InVision Technologies (INVN), L-3 Communications (LLL), OSI Systems (OSIS), Symantec (SYMC), Boeing (BA), Viisage Technology (VISG), Zebra Technologies (ZBRA), CompuDyne (CDCY), Allied Defense Group (ADG)

### **MANAGEMENT BACKGROUND & EXPERIENCE**

Seasoned management team found on <http://www.cyberdefensesystems.com> website under Investors section, then Management section.

### **FINANCIALS**

<http://finance.yahoo.com/q/is?s=CYDF.OB&annual>

**Analyst's Statement:** "I have prepared this report, and the content within it, including all opinions, are solely my own." Kipley J. Lytel, CFA, is a member of CFA Institute & Los Angeles Society of Financial Analysts **Company Contact:** Billy Robinson, CEO, 10901 Roosevelt Blvd. Suite 100D, St. Petersburg FL. 33716, 727-577-0878, billy@cduav.com **Sources:** Cyber Defense 10K, 10Q, 8K & other SEC filings, Company Web Sites, public Power Point Presentations, News Releases, Management Discussions, Footnoted References, etc.

**This report and other reports regarding this company and others are at:** <http://www.investrend.com/articles/secondlevel.asp?level=182>; The company's InvestorPower™ page is at <http://www.investrend.com/company/list.asp?sPathParam=yes> The analyst's biographical details are at <http://www.investrend.com/articles/secondlevel.asp?level=238> Investrend Research and Investrend Research Syndicate, Div., Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com). Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com).

**Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply "recommendations" to any reports nor the companies covered. Any usage of the word "recommendation," if any, is to be defined as a "rating" only. We subscribe to the "Standards for Independent Research Providers" at <http://www.firstresearchconsortium.com> © Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.



**Digimarc Corporation**  
(NASDAQ: DMRC)

## SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY **CRONUS CAPITAL MARKETS**

Q3 2005

*Digimarc Corp. supplies personal identification systems in the United States and internationally. The company offers all or part of the issuance systems for national identifications, voter identifications, and driver licenses*

Stock Metrics	
Recent Price	\$6.25
52 Week Range	\$4.44 - \$10.01
Market Capitalization	\$ 137.8 Million
Shares Outstanding	20.7 Million
Sector	Security Software Services
Avg. Dly Vol. (3-Mo.):	34,000

### Company & Homeland Security Products Overview

Digimarc Corporation (“DMRC” or “The Company”) is a leading supplier of secure identity and media management solutions. Digimarc solutions enable governments and businesses around the world to deter counterfeiting and piracy, enhance traffic safety and national security, combat identity theft and fraud, facilitate the effectiveness of voter identification programs, and improve the management of media content. The Company is the leading supplier of driver licenses in the United States, producing nearly two-thirds of all driver licenses issued.

Digimarc has an extensive intellectual property portfolio, with 203 issued U.S. patents with more than 4,000 claims, and more than 400 pending patent applications in digital watermarking, personal identification and related technologies. Specifically, Digimarc's digital watermarking technology provides a persistent digital identity for various media content and is used to enhance the security of financial documents, identity documents and digital images, and support other media rights management applications.

Digimarc's secure identity and media management solutions are built upon an extensive portfolio of intellectual property, and combine innovative software, hardware and materials that we deliver, together with carefully selected and qualified best-of-breed third-party components, to our government and commercial customers. The roots of these technologies are in the pioneering and commercialization of digital watermarking and in the acquisition of the Large Government Programs business unit of Polaroid Corporation in late 2001, following the terrorist attacks of September 11, 2001. The primary focus of this business is the production of driver licenses and other identification documents on behalf of government agencies.

### **PRODUCT LINE:**

The Company currently provides components and subsystems that:

- Digitally capture and archive applicant documents
- Validate the authenticity of documents that an applicant presents as proof of identity
- Verify applicant information by referencing various Social Security, immigration or commercial databases
- Capture digital facial images and fingerprints of individuals
- Verify digital facial image and fingerprint biometrics
- Provide secure production of driver licenses and other IDs
- Deliver technologically advanced and sophisticated machine-readable ID security features such as Digimarc® IDMarc™ digital watermarks to prevent counterfeiting, tampering or duplication along with barcodes, mag stripes and other machine-readable technologies that have publicly defined data elements
- Authenticate driver licenses and other IDs at points of inspection within states and across jurisdictions

Digimarc's IDMarc™ is a covert digital security feature that can be used to fuse multiple elements of identity documents into a coherent, secure ID structure. Millions of digitally watermarked identity documents are in

circulation today, including 20% of U.S. driver licenses issued annually. Indeed, digital watermarking is a strategic component of nearly all of DMRC's product offerings. Digital watermarking has already proven to be a powerful differentiator in banknote security, giving rise to a long-term relationship with leading Central Banks and many leading companies in the IT industry.

Digimarc's ID Validation Suite (IDVS) scans, authenticates and archives images of ID credentials, such as out-of-state driver licenses, passports, birth certificates and other government-issued IDs. The Digimarc Biometric Verification Suite is a modular, scalable component of our secure ID solution that incorporates both fingerprint and facial recognition capabilities. Digimarc was the first to employ facial recognition as a verification step for driver license issuance.

### **REVENUE & CUSTOMERS**

The substantial majority of the Company's revenues arise from provision of critical infrastructure and services pursuant to long-term contracts with government agencies; primarily U.S. state government agencies responsible for driver license issue ("State DL Issuers"), a consortium of leading Central Banks, and national governments of a number of foreign countries. There was no single customer in the three- and six-month periods ended June 30, 2005 or 2004 that accounted for more than 10% of total revenue.

### **MARKETS & INDUSTRY**

Digimarc estimates the size of the U.S. driver license issuance market at more than \$100 million. The Company's products and solutions touch a variety of media objects, from movies and music, to banknotes and secure credentials. The aggregation of these print and digital content markets is huge, creating an enormous overall opportunity for the Company to address. Company believes these are only the early signs of market penetration, representing a nominal share of the potential market for Digimarc's products, services, and technologies.

### **CONCLUDING REMARKS**

The Homeland Security Group has experienced a soaring share price move. DMRC's emerging presence in this group bodes well for the company stock outlook, particularly given a long operating history, consistent revenue and the fact the Company trades on the NASDAQ.

**PEER GROUP:** Armor Holdings (symbol:AH), Check Point Software Technologies (CHKP), CompuDyne (CDCY), Identix (IDNX), Internet Security Systems (ISSX), InVision Technologies (INVN), L-3 Communications (LLL), OSI Systems (OSIS), Symantec (SYMC), Viisage Technology (VISG), Zebra Technologies (ZBRA), CompuDyne (CDCY), Allied Defense Group (ADG)

### **MANAGEMENT BACKGROUND & EXPERIENCE**

Seasoned management team found at <http://www.digimarc.com/about/management.asp>

### **FINANCIALS**

<http://finance.yahoo.com/q/is?s=DMRC&annual>

**Analyst's Statement:** "I have prepared this report, and the content within it, including all opinions, are solely my own." Kipley J. Lytel, CFA, is a member of CFA Institute & Los Angeles Society of Financial Analysts

**Company Contact: Digimarc Corp.,** 9405 SW Gemini Drive, Beaverton, OR Phone: 503-469-4800 <http://www.digimarc.com>

**Sources:** DMRC 10K, 10Q, 8K & other SEC filings, Company Web Sites, public Power Point Presentations, News Releases, Management Discussions, Footnoted References, etc.

This report and other reports regarding this company and others are at: <http://www.investtrend.com/articles/secondlevel.asp?level=182>; The company's InvestorPower™ page is at <http://www.investtrend.com/company/list.asp?sPathParam=yes> The analyst's biographical details are at <http://www.investtrend.com/articles/secondlevel.asp?level=238>

**Investrend Research and Investrend Research Syndicate, Div.,** Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com) . Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com).

**Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply "recommendations" to any reports nor the companies covered. Any usage of the word "recommendation," if any, is to be defined as a "rating" only. We subscribe to the "[Standards for Independent Research Providers](http://www.firstresearchconsortium.com)" at <http://www.firstresearchconsortium.com> © Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.



# Groen Brothers Aviation

(OTC BB – GNBA)

## SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY CRONUS CAPITAL MARKETS

Q3 2005

*Groen Brothers Aviation, Inc., through its subsidiaries, engages in the development, manufacture, and marketing of gyroplanes. Gyroplane is a hybrid aircraft with the off-runway operating capability of a helicopter.*

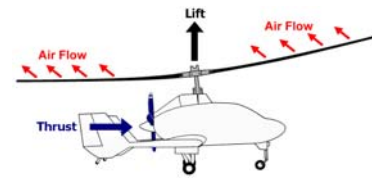
Stock Metrics	
Recent Price	\$0.43
52 Week Range	\$0.12 - \$0.50
Market Capitalization	\$57.6 million
Enterprise Value	\$65.3 million
Trading Volume	104,000
Beta	0.57

### Company & Homeland Security Products Overview

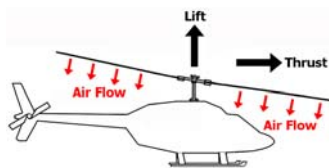
Groen Brothers Aviation (GBA) continues to market the Hawk 4 gyroplane to Federal Agencies and law enforcement entities. During this time, GNBA will be able to sell the aircraft to governmental agencies while awaiting FAA certification (expected within 2-3 years).

In the first report on GNBA, I described the company and its prospective use and customers in the home security field. I am going

to expand on the product description in this report to give you an idea of the products potential.



The gyroplane and the helicopter are rotorwing aircraft and derive lift from the spinning of their rotor system. In a gyroplane, thrust is provided by an engine driven propeller. A gyroplane's simple, freely turning rotor system is tilted back as the gyroplane moves forward. Oncoming airflow through the rotor causes it to spin, much like wind through a windmill, producing lift. This is called autorotation. The gyroplane cannot stall like a fixed wing aircraft, flies safely at low altitudes and low speeds, but cannot hover.



The helicopter's complex, powered rotor system produces both lift and thrust and is tilted forward. It can hover, but a powered rotor requires a heavy transmission, and a tail rotor to counteract the torque imposed on the aircraft. In the event of a power failure, a helicopter must have adequate forward speed and/or altitude to allow transition from powered flight into autorotation. The pilot must react immediately to complete this transition safely. If the power fails in a gyroplane, there is no transition as the gyroplane flies in constant autorotation. The pilot can easily guide the gyroplane to a safe landing with little or no ground roll, typically within the length of the rotor blades.



GBA has received letters from fifty-five government agencies, representing twenty-seven states, requesting federal funding for the Hawk 4 Gyroplane. Almost all of these requests are from Law Enforcement departments. These many agencies are specifically seeking the Hawk 4, instead of helicopters or fixed wing aircraft, because of the gyroplanes inherent simplicity, low cost, safety and ease of pilot training. Many of the individual mission requirements for these agencies tie directly into Homeland Security. GBA is seeking to qualify the aircraft for funding through the Office of Domestic Preparedness grant program. The Hawk 4 was used during the 2002 Winter Olympics by the Utah Olympic Public Safety Command (UOPSC) as an aerial observation platform. During its operational period, the Hawk 4 "Homeland Defender"<sup>TM</sup> gyroplane was available 24-7,

completing 67 missions and accumulating 75 hours of maintenance free flight time. The Hawk 4 is an ideal aircraft for aerial observation as it proved during its mission with UOPSC.

Sales of GBA's SparrowHawk kit plane have been doing very well during the quarter. GBA reports that they have now reached totals sales over 100 SparrowHawk Gyroplane and SparrowHawk/P modification kits. GBA now has over 30 SparrowHawk dealers worldwide. This product line is instrumental in providing cash flow to the company to allow it to continue to develop the Hawk 4. The gyroplane's simplicity translates directly into safety, higher performance and mission readiness, and lower acquisition and maintenance costs. Its ability to safely fly low and slow makes it an excellent choice for many governmental agencies including Law Enforcement, Border Patrol and Homeland Security. Other applications include agricultural aerial application, mosquito abatement, Public utility Monitoring and utility/passenger transport.

### **Financial Overview**

<http://finance.yahoo.com/q/ks?s=gnba.ob>

### **Positioning in Homeland Security Industry**

GNBA operates within the aerospace industry. The 'big boys,' such as Boeing, Textron, and Airbus dominate this industry. However, these companies do not make products that are directly comparable to Groen Brothers Aviation, giving GNBA a possible competitive advantage.

### **Competition**

Groen Brother's does face some significant competition, however the competitors do not produce similar products. Competitors include, but are not limited to, Boeing, Raytheon, Airbus, Lockheed Martin, and Northrop Grumman.

Other, smaller, lesser-known companies may actually be the major source of competition for GNBA. The strongest competitor seems to be Rotary-Air Force Marketing, a Canadian firm. RAF's product, called the RAF 2000 Gyroplane, is approved for use as an experimental / kit product in Canada, the US, Europe, and other countries. The RAF 2000 has been in production and use for over 15 years. However, GNBA's continued development of the Hawk 4 should make it the better product. Also, the Hawk can seat four while the RAF 2000 can only seat two.

### **Management**

Please see the Groen website for management bios.

### **Concluding Remarks**

Groen Brothers have a unique product that is suitable for Homeland Security missions. This company is extremely dependent on the success of this endeavor, but does have other product lines to help it continue needed development; sales of the SparrowHawk Gyroplane have surpassed 100 (as of 9/22/05). Competition is few and far between, and competitors with similar product are also small firms and not the larger, defense related contractors whose resources would be a major competitive advantage. GNBA may be considered a suitable addition a well-diversified portfolio.

**Analyst's Statement:** "I have prepared this report, and the content within it, including all opinions, are solely my own." The analyst is Gary Vassalotti. The analyst's biographical details are at <http://www.investrend.com/articles/secondlevel.asp?level=238> The analyst's biographical details are at <http://www.investrend.com/articles/secondlevel.asp?level=238>

**Groen Brothers Aviation, Inc.**, 2640 West California, suite A, Salt Lake City, UT 84104, Jay Groen., 801-973-0177 Web site:

<http://www.gbagyros.com> The company's InvestorPower™ page is at <http://www.investrend.com/company/list.asp?sPathParam=yes>

**Cronus Capital Markets**, P.O. Box 1022, TD Centre Postal Station, 77 King St. West, Toronto, Ontario M5K 1P2, Phone (888) 901-7090. e-mail: [query@cronuscapitalmarkets.com](mailto:query@cronuscapitalmarkets.com) Web site: <http://www.cronuscapitalmarkets.com>

**Investrend Research and Investrend Research Syndicate, Div.**, Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com) . Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com).

**Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply "recommendations" to any reports nor the companies covered. Any usage of the word "recommendation," if any, is to be defined as a "rating" only.

We subscribe to the "Standards for Independent Research Providers" at <http://www.firstresearchconsortium.com>

© Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.



## Viscount Systems, Inc. (OTC:BB – VSYS)

### SPOTLIGHT REPORT

HOMELAND SECURITY SECTOR RESEARCH COMMISSIONED BY CRONUS CAPITAL MARKETS

Q3 2005

Viscount offers innovative products under the name **MESH™** (Multimedia Embedded Security Hub), a new internally developed technology that converges voice (intercom, emergency communications), data (access control, elevator control, alarm) and some video to provide increased security at a reduced cost.

Stock Metrics	
Recent Price	\$0.61
52 Week Range	\$0.56- \$1.19
Market Capitalization <sup>1</sup>	\$9.9 million
Enterprise Value	n/a
Trading Volume	8,500
Beta	n/a

#### Company & Homeland Security Products Overview

Viscount Systems Inc. is a designer and manufacturer of telecommunications and electronic door control access systems for the security industry. From 1969-1997 Viscount was an R&D affiliate of Telus, itself a controlled subsidiary of GTE, now Verizon Communications. The company's diverse line of products is designed to improve safety and manage security for property owners and users. Viscount's products have been installed in approximately 35,000 sites in over 30 countries and are sold through a 500-member, North

America-wide dealer network comprised of security equipment vendors. In addition to **MESH™**, Viscount's current access control and security product lines include: Enterphone, a building intercom; Entercheck, a card access system; RadioClik and InfraClik, radio frequency and infrared remote controls; Elektra, liquid crystal display intercom panels; EmerPhone, emergency telephone entry systems; and various accessories.

**MESH™** technology is based on a proprietary software platform that can be used for a variety of security and access control applications as well as communications functions. The technology represents a departure from traditional access control and security systems that use controllers based on Wiegand technology with the capacity to control only 1 to 8 access points per controller. A building access system using the **MESH™** technology can control several hundred points of access from a single remote hardware and software platform. The technology also allows several previously independent building control systems to be hosted on a single hardware and software platform.

#### Recent Developments

On October 3, 2005 Viscount announced that the company's first **MESH™** technology certification conference was successfully conducted. The conference and training were held in Las Vegas with dealers and attendees from California, Nevada and Arizona. Separate training sessions were held for installation technicians and sales representatives. The entire press release can be viewed at: <http://biz.yahoo.com/iw/051003/096778.html>

#### Financial Overview<sup>1</sup>

On August 15, 2005 Viscount Systems announced financial results for its second quarter ended June 30, 2005. Highlights included: Revenues for the quarter ended June 30, 2005 were \$1,180,205 an increase of 14% when expressed in Canadian dollars, compared to the quarter ended June 30, 2004. Sales for the six months ended June 30, 2005 were \$2,503,950, an increase of 14.4% when expressed in Canadian Dollars, compared to the six months ended June 30, 2004. Sales of **MESH** continue to increase and accounted for 20% of revenue. Further info can be found at: <http://moneycentral.msn.com/scripts/webquote.dll?ipage=qd&Symbol=VSYS>

<sup>1</sup> The Company maintains its' financial statements in Canadian dollars (\$CDN). Financial metrics other than share price related are in \$CDN.

## Positioning in Homeland Security Industry

Through *MESH*<sup>™</sup>, Viscount is attempting to advance the state of the art in the access control systems industry. Virtually every low voltage building technology, except building access, has evolved using “intelligent” addressable network devices. Access control systems, however, continue to be based on a 30-year-old standard called Wiegand. The limitations of this standard continue to plague the industry due to the slow data transmission speed (9600 baud) between the reader and the host controller, the high cost and quantity of specialized and dedicated hardware, and the inability of the host computer to process voice or video signals. For example, buildings requiring elevator access control have traditionally required a significant amount of expensive dedicated hardware. The *MESH*<sup>™</sup> network with “intelligent” readers can accomplish these functions without dedicated hardware, resulting in cost reductions, both in terms of the actual hardware required and the labor, cable and conduit costs associated with installation. The *MESH*<sup>™</sup> system bypasses the need for specialized and dedicated hardware. Instead, *MESH*<sup>™</sup> provides a software-based platform that operates on an industrial computer server connected to “intelligent” readers transmitting data at high speed rates of up to 156,000 baud, while simultaneously running voice and video applications. Management believes that *MESH*<sup>™</sup> has the potential to dramatically reduce or eliminate the future use of legacy Wiegand technology due to the myriad benefits *MESH*<sup>™</sup> offers. .

## Competition

There are several large and a variety of smaller competitors in the security and building control industry, which has been rapidly consolidating recently. Large multi-national companies like Honeywell and Johnson Controls are attempting to gain share and leverage by integrating vertically through acquisitions. Notable acquisitions include the purchase of Cardkey by Johnson Controls, Guardall by Chubb and ADI/Northern Computers by Honeywell. The access control industry remains very fragmented with no dominant market share holder. There are estimated to be over 50 manufacturers of access control products in the US and at least six in Canada. Wiegand technology is the industry standard and is almost universally adopted by control host manufacturers. Technology limitations inherent in the standard technology result in most research and development being focused on cost reducing hardware and making the control hosts more network capable. Traditional Wiegand technology is limited from 1 to 8 doors per host.

## Analyst Coverage Commentary

Additional research is available at:

<http://www.investrend.com/company/company.asp?sCompany=92&Submit=Find>

## Senior Management Information

Additional information is available at: <http://www.viscount.com/irmanagement.html>

**Analyst’s Statement:** I, Michael R Andereg, certify that I have prepared this report, and (1) the views expressed in this report accurately reflect my personal views about all of the subject companies and securities and (2) no part of my compensation was, is or will be directly or indirectly related to the specific recommendations or views expressed in this report. The analyst is Michael R. Andereg, CFA. The **analyst’s biographical** details are at <http://www.investrend.com/articles/secondlevel.asp?level=238> **MRA Research**, Michael R. Andereg, 925-443-3860, E-mail: [MRAResearch@hotmail.com](mailto:MRAResearch@hotmail.com). The Company’s **InvestorPower**<sup>™</sup> page is at <http://www.investrend.com/company/company.asp?sCompany=92&Submit=Find> **Cronus Capital Markets**, P.O. Box 1022, TD Centre Postal Station, 77 King St. West, Toronto, Ontario M5K 1P2, Phone (888) 901-7090. e-mail: [query@cronuscapitalmarkets.com](mailto:query@cronuscapitalmarkets.com) Web site: <http://www.cronuscapitalmarkets.com>

**Investrend Research and Investrend Research Syndicate, Div.**, Investrend Communications, Inc., 603 W. 13th Street, Suite 1A-277, Austin, Texas 78701 Phone (718) 896-5060, Fax (718) 896-5316, e-mail: [contact@investrend.com](mailto:contact@investrend.com) . Web site: [www.investrend.com](http://www.investrend.com) and [www.investrendresearch.com](http://www.investrendresearch.com).

**Information, opinions or ratings** contained in this report are submitted solely for advisory and information purposes by the qualified professional analyst. Investrend Research provides analyst facilitation, report publication and distribution services only. The information used and statements of fact made have been obtained from sources considered reliable but neither guarantee nor representation is made as to the completeness or accuracy. No representation whatsoever is made by Investrend. Such information and the opinions expressed are subject to change without notice. This report or study is not intended as an offering or a solicitation of an offer to buy or sell the securities mentioned or discussed. Please read full disclosures at <http://www.investrendresearch.com> Neither Investrend nor the analysts apply “recommendations” to any reports nor the companies covered. Any usage of the word “recommendation,” if any, is to be defined as a “rating” only.

We subscribe to the “**Standards for Independent Research Providers**” at <http://www.firstresearchconsortium.com>

© Copyright, 2005, by Investrend Research, div., Investrend Communications, Inc.

## Contributors, Bibliography, Industry Links

- 
- <sup>i</sup> National Strategy for Homeland Security – Office of Homeland Security; July 2002
- <sup>ii</sup> National Strategy for Homeland Security – Office of Homeland Security; July 2002, pg 25
- <sup>iii</sup> [http://www.rand.org/pubs/testimonies/2005/RAND\\_CT250-1.pdf](http://www.rand.org/pubs/testimonies/2005/RAND_CT250-1.pdf)
- <sup>iv</sup> “Securing our Homeland” – U.S. Department of Homeland Security Strategic Plan - 2004
- <sup>v</sup> <http://www.9-11commission.gov/report/911Report.pdf#search=9/11%20Commission%20Report>
- <sup>vi</sup> <http://www.dhs.gov/dhspublic/display?theme=11&content=4353>
- <sup>vii</sup> ‘Homeland Security’s New Broom – Business Week, April 19, 2005
- <sup>viii</sup> [http://www.economist.com/displaystory.cfm?story\\_id=4174486](http://www.economist.com/displaystory.cfm?story_id=4174486)
- <sup>ix</sup> [http://www.dhs.gov/interweb/assetlibrary/DHS\\_OrgChart\\_2004.pdf](http://www.dhs.gov/interweb/assetlibrary/DHS_OrgChart_2004.pdf)
- <sup>x</sup> Washington’s Mega-merger – The Economist, November 21, 2002.
- <sup>xi</sup> Civitas Group – The FY 2006 Homeland Security Budget Request – Key Implications for the Private Sector – February 2005
- <sup>xii</sup> <http://abcnews.go.com/Politics/wireStory?id=1192674>
- <sup>xiii</sup> <http://online.wsj.com/article/0,,SB112804322732556400,00.html>
- <sup>xiv</sup> Guarding America – Barron’s June 28-July 4 2005
- <sup>xv</sup> <http://www.heritage.org/Research/HomelandDefense/bg1835.cfm>
- <sup>xvi</sup> Guarding America – Barron’s June 28-July 4 2005
- <sup>xvii</sup> <http://www.whitehouse.gov/omb/legislative/sap/107-2/HR4598-h.html>
- <sup>xviii</sup> <http://www.rand.org/publications/IP/IP218/IP218.pdf>
- <sup>xix</sup> [http://www.biometricgroup.com/reports/public/market\\_report.html](http://www.biometricgroup.com/reports/public/market_report.html)
- <sup>xx</sup> ‘Bioshield Drug Patent Plan Draws Fire – Wall Street Journal – 04.01.05
- <sup>xxi</sup> The Future is Still Smart – Economist – 06.24.04
- <sup>xxii</sup> [http://www.economist.com/agenda/displaystory.cfm?story\\_id=4318265](http://www.economist.com/agenda/displaystory.cfm?story_id=4318265)
- <sup>xxiii</sup> [http://www.rand.org/pubs/testimonies/2005/RAND\\_CT233.pdf](http://www.rand.org/pubs/testimonies/2005/RAND_CT233.pdf)
- <sup>xxiv</sup> Making the Internet Safe – Barron’s – May 2, 2005
- <sup>xxv</sup> [http://www.businessweek.com/investor/content/oct2005/pi20051011\\_2378\\_pi044.htm](http://www.businessweek.com/investor/content/oct2005/pi20051011_2378_pi044.htm)
- <sup>xxvi</sup> <http://online.wsj.com/article/SB112889637083663974-search.html?KEYWORDS=homeland+security&COLLECTION=wsjie/archive>
- <sup>xxvii</sup> Standard & Poor’s Industry Survey – October 7, 2004
- <sup>xxviii</sup> Homeland security now in base closure criteria – Gannett News Service – July 6, 2004  
[http://www.tucsoncitizen.com/index.php?page=national&story\\_id=070504b1\\_baseclose](http://www.tucsoncitizen.com/index.php?page=national&story_id=070504b1_baseclose)
- <sup>xxix</sup> “Still Haunting America” – the Economist, July 22, 2004
- <sup>xxx</sup> <http://www.aimglobal.org/technologies/rfid/resources/articles/dec03/Homeland.htm>
- <sup>xxxi</sup> [http://www.cbp.gov/xp/cgov/enforcement/international\\_activities/csi/csi\\_in\\_brief.xml](http://www.cbp.gov/xp/cgov/enforcement/international_activities/csi/csi_in_brief.xml)
- <sup>xxxii</sup> National Strategy for Homeland Security – Office of Homeland Security; July 2002, pg 31
- <sup>xxxiii</sup> National Strategy for Homeland Security – Office of Homeland Security; July 2002, pg 37
- <sup>xxxiv</sup> <http://online.wsj.com/article/SB112889637083663974-search.html?KEYWORDS=homeland+security&COLLECTION=wsjie/archive>
- <sup>xxxv</sup> Security Industry Annual Report – Lehman Brothers, October 15, 2004
- <sup>xxxvi</sup> <http://www.dhs.gov/dhspublic/archdisplay?theme=43,44,45,47&monthyear=092005>
- <sup>xxxvii</sup> [http://www.iseoptions.com/pdf/HSX\\_REPORT.pdf](http://www.iseoptions.com/pdf/HSX_REPORT.pdf)
- <sup>xxxviii</sup> Frederick Ruffy – Optionetics.com
- <sup>xxxix</sup> Sources: Company website, 10K filings, Reuters.com, Yahoo.com, Investrend.com