

# THE 9/10/11 PROJECT



BORDER  
SECURITY

## Are We Ready for the Day Before Tomorrow?

**Imagine it is September 10, 2011** – 9/10/11 – a full decade since the devastating terrorist attacks of September 11, 2001. Is our nation equipped for whatever catastrophe may happen tomorrow? How have our prevention, preparedness, response and resiliency structures changed, matured and become operational?

The Homeland Security & Defense Business Council's 9/10/11 Project looks at how far the country has come since the day before 9/11/2001. Through fresh interviews with industry leaders the Council is seeking to vividly illustrate the strides our government at all levels, working with the private sector, has made to secure the country and to stay at least one step ahead of events and disasters that could destroy our way of life.

On the 10th of each month through September 2011, the Council will provide a historical context for how far we have come and where we are now, as well as an assessment of the future of the most pressing homeland security issues. Each monograph will include a running timeline (interactive on our website) illustrating the events, incidents, and critical government responses pertinent to that month's topic. This month's monograph focuses on **Border Security**.

*At its core, border security means the control of people, goods and conveyances traveling across land, sea and air international boundaries. Border security has been on the national agenda since the United States was founded. As new concerns and threats have developed over the last 235 years, so too have the agencies responsible for executing the border security mission.*

This monograph looks at the evolution of border security agencies and missions leading up to the terrorist attacks of September 11, 2001, and examines the official response to those attacks. The paper surveys how industry is supporting U.S. efforts to enhance border security, and discusses future challenges.

### Before 9/11

#### Customs Collections

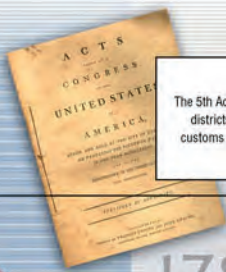
Customs collections to fund our fledgling government occupied the 1st Congress of the United States. In that session, Congress placed U.S. Ports of Entry under the jurisdiction of the Treasury Department. Treasury established the U.S. Customs Border Patrol in 1853 to guard U.S. land borders, and the Revenue Marine Division in 1871 to patrol our maritime borders.

#### Immigration

Most congressional immigration-related activity in the years immediately following the establishment of the United States focused on the criteria for citizenship. In 1875, Congress passed the first law directly regulating and restricting immigration. Aside from the unfortunate ethnically discriminatory provisions in early immigration laws, core congressional concerns with immigration policy have remained fairly static to this day – for example, how many immigrants do we wish to admit; will they assimilate; how will they improve American society and competitiveness; and, what persons must be denied admission because they may endanger Americans.

#### Smuggling

The U.S. Immigration Service Border Patrol was established in 1924 to control contraband smuggling and immigration. The agency adopted two early technologies – automobiles and airplanes – for surveillance and enforcement. As we entered the era of information technology, U.S. agencies implemented the Treasury Enforcement Communications System (TECS) to improve surveillance and tracking for customs violators in 1969, and the Automated Biometric Identification System (IDENT) for immigration violators in 1994 – a system



**JULY 1789**  
The 5th Act of the 1st Congress established 59 customs collection districts in the 11 states that ratified the Constitution. These customs collection districts were the foundation for what would become the U.S. Customs Service

**MAY 1924**  
Through the Labor Appropriation Act of 1924, Congress approved funding for the creation of the U.S. Border Patrol

**APRIL 1927**  
An independent Bureau of Customs was officially created in the Treasury Department. In 1973, it would be renamed the U.S. Customs Service

**JUNE 1933**  
The Immigration and Naturalization Service was created and placed in the Department of Labor. President Roosevelt transferred the INS to the Department of Justice in 1940

1789

1924

1940



SPONSORED BY



Border Security agents can't  
be everywhere at once.

Or can they?



Protecting the nation's borders demands monitoring that's grounded in proven intelligence. Raytheon delivers integrated border security solutions designed to detect, identify and classify threats before they can do us harm. From modeling and simulation to providing real-time border intelligence and surveillance in a common, integrated view, Raytheon delivers the proven technology and consulting expertise our nation relies on to address the full spectrum of today's border security requirements — and anticipate tomorrow's threats.



**INNOVATION IN ALL DOMAINS**

Visit [www.raytheon.com](http://www.raytheon.com)

Keyword: HLS-BS

© 2011 Raytheon Company. All rights reserved.  
"Customer Success Is Our Mission" is a registered trademark of Raytheon Company.

**Raytheon**

*Customer Success Is Our Mission*



originally developed by Raytheon. Numerous other IT projects to speed and improve data-sharing followed.

### Drug Trafficking Organizations

In response to the trade in illicit drugs and unprecedented illegal migration in the 1990s, the Border Patrol initiated a crackdown along Southwest urban hubs, over time forcing criminal organizations to shift their activities to rural and marine environments, and underground.

### Terrorism

In response to the increasing threat of international terrorism, the Department of State created the "TIPOFF" watchlist for suspected terrorists in 1987. In the 1990s, international terrorism arrived in the U.S. with the 1993 bombing attack on the World Trade Center, later followed by a series of disrupted plots. Demonstrating the point that trained and experienced officers will always be part of the equation, one plot was foiled in 1999 when an alert Customs officer at Port Angeles, Washington, noticed that an arriving passenger from Canada was acting "hinky" and so referred him for secondary inspection: that passenger was Ahmed Ressam, who planned to detonate a bomb at Los Angeles International Airport.

## The Response to 9/11

The September 11th terrorist attacks generated a new federal focus on greater centralization of border security responsibility and more effective information sharing with other federal counter-terrorism agencies. The threat continues to evolve – the violent drug trade, transnational organized crime, proliferation of Weapons of Mass Destruction technology and know-how, and pandemic disease all highlight the continued importance of reviewing mission needs based on new risks, identifying gaps, and developing strategies to address those gaps.

With the establishment of the U.S. Department of Homeland Security (DHS) in 2002, four legacy agencies merged to create the Bureau of Customs and Border Protection (CBP): the U.S. Border Patrol, U.S. Customs Service inspection functions, the U.S. Department of Agriculture's Animal and Plant Health Inspection Service, and inspectors from the Immigration and Naturalization Service. CBP's primary mission was defined as "keeping terrorists and their weapons out of the U.S. . . . securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws."

With respect to the international boundary between the Ports of Entry, CBP has implemented a multi-pronged border security strategy to achieve:

- **The right combination of personnel, technology and infrastructure.** The mix of these three components vary depending on the challenges of the focus area – in urban environments, CBP may only have seconds to

minutes to respond; in rural environments, CBP may have minutes to hours; in a remote environment, CBP may have hours to days. Cameras, ground sensors, radars and other technologies allow operators to detect entries, and to identify and classify threats, and CBP has invested substantially in them. CBP has also installed hundreds of miles of road, walls and vehicle barriers to support interdiction and to deter or slow illicit traffic. The Border Patrol has more than doubled in size to over 20,000 agents. To plan the right mix of assets for emerging threats in this complex environment, modeling and simulation will prove an important tool for operators.

- **Mobility and rapid deployment of people and resources.** Since its first Predator B in 2005, CBP Air & Marine has increasingly relied on UAVs to provide mobile, persistent surveillance against specific threats. CBP aircraft provide the ability to respond quickly to illicit traffic. CBP has also made increasing investments in mobile systems that provide a ground-based surveillance capability deployable on a threat-based approach.

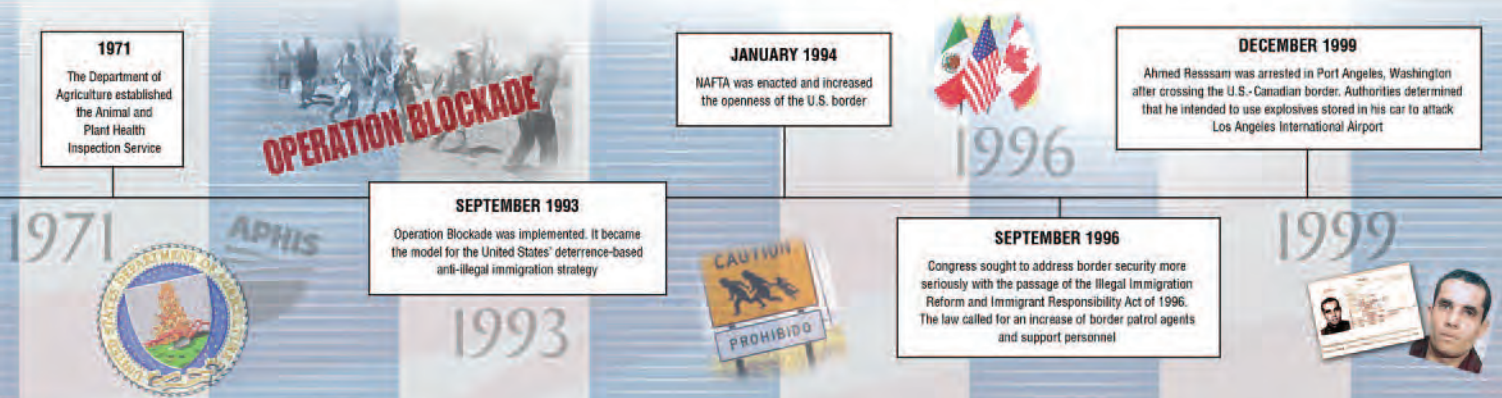
- **Defense-in-depth using interior checkpoints and coordinated enforcement operations.** Some portion of smugglers and illegal immigrants invariably evade CBP at the border. For that reason, CBP maintains checkpoints on and around important roadways in the U.S. interior. CBP is bringing modernized identity verification and Non-Intrusive Inspection technologies to these checkpoints to aid in effective risk assessment.

- **Partnerships with other law enforcement agencies.** Local first responders can be a force-multiplier for CBP, particularly in areas where technology is not yet deployed. Partnerships with local law enforcement agencies are therefore key to the interdiction of illegal crossers and the investigation of smuggling organizations.

CBP processes almost 1 million passengers and 60,000 cargo containers per day at U.S. ports of entry. Given the volume of travelers and cargo, limited infrastructure, finite resources, and limited time available for passenger processing, a number of capabilities have been developed to balance security and legitimate travel and trade:

- **Information sharing to drive targeting and screening.** The Aviation & Transportation Security Act required carriers to provide CBP with passenger and crew information for international air and ship traffic to and from the U.S. Likewise, the Trade Act of 2002 required vessel carriers to provide cargo manifests to CBP 24 hours before lading. CBP processes this data through its Automated Targeting System (ATS), where the information is compared against both watchlists and rule sets built from prior enforcement data to prioritize inspection resources against higher risk travel and trade.

- **Identity resolution.** Effective risk assessment requires accurate identification of the traveler in question. In 2004, DHS implemented the US-VISIT system to biometrically identify and verify the identities of most





foreign visa holders and Visa Waiver Program (VWP) participants arriving in the U.S. Historically more lenient identification standards for travel within the Western Hemisphere were also tightened, requiring all travelers – including U.S. citizens – to present a passport or other document denoting both identity and citizenship on entry. Further, the VWP was amended to require travelers to present more secure identity documents and to seek advance travel authorization through a new Electronic System for Travel Authorization (ESTA).

- **Scanning technology.** To assess cargo and conveyances, CBP now utilizes a number of scanning technologies to determine whether contraband or people are secreted inside without the need for a manual search. Active X-ray systems are used to identify anomalies, and radiation portal monitors are used to detect nuclear or radiological materials in containers. The Domestic Nuclear Detection Office is working with CBP to test a Raytheon-developed Advanced Spectroscopic Portal that would not only detect but also simultaneously identify the radioactive isotope at issue, thereby differentiating threat materials from naturally occurring radioactive material in real time.

- **Partnerships.** CBP has worked to build partnerships with industry and foreign governments to allow for risk assessment of passengers and cargo before departure for the U.S. Under the Container Security Initiative, CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism based on advance information and strategic intelligence, and then works with host customs agencies to prescreen high-risk containers generally before they depart for the United States. Under the Customs-Trade Partnership Against Terrorism (C-TPAT), CBP works with businesses to ensure the integrity of their security practices and verify the security guidelines of other business partners within their supply chain. In return, CBP offers benefits including reduced inspections and priority processing.

The use of tactical, operational, and strategic intelligence to assess risk, target enforcement efforts, and drive operations is critical at and between the ports of entry. Examining intelligence lapses, the 9/11 Commission found that even though the U.S. had maintained both border and visa-related lookout databases for some years before September 11th – and that the U.S. intelligence community had identified Khalid al Mihdhar and Nawaf al Hazmi as suspected terrorists (with existing U.S. visas) as early as January and March 2000 – this information was only very belatedly added to the TIPOFF database. The government has thus focused on building much stronger information sharing and interoperability between frontline border security databases and related systems in U.S. counterterrorism agencies. Some examples include the establishment of the Terrorist Screening Center and Terrorist Screening Database, plus the biometric

interoperability project between FBI and US-VISIT for IDENT and the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

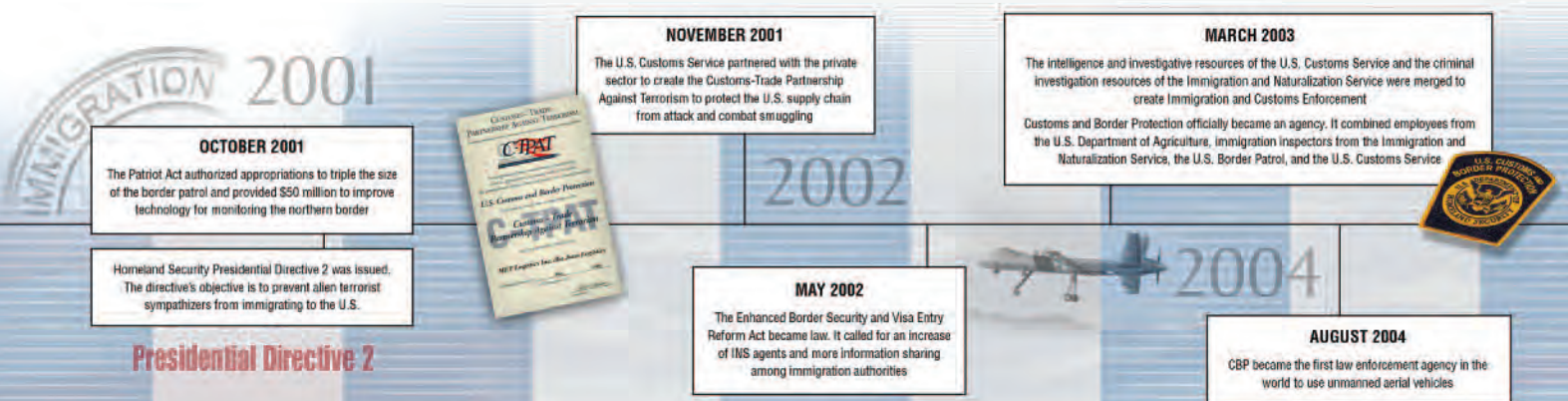
## Private Sector Contributions to Border Security

The private sector has made – and continues to make – substantial investments in innovative products, services and solutions to advance the land, sea and air border security mission. For example:

**Avaya** has developed an interoperability communications technology which ties together any phone device with software and servers so a CBP Agent can talk directly to a person in DC without having to first contact their dispatcher, then border headquarters, the DC point person, etc. This real-time point-to-point contact capability comes with first-responder priorities including presence, blast messaging, and other capabilities critical to COOP planning. Michael Strange, Avaya's Principal Representative for Government Solutions, describes this technology as a "force multiplier, which is important because Border patrol agents are generally on duty by themselves and if they need to call another agent for assistance they must have the same type of radio in order to communicate." Avaya's solution allows agents to communicate whether they are on foot, in a helicopter, or even on different networks.

**Boeing** served as the prime contractor for the *SBlnet* program. *SBlnet* was intended to be the technology leg of the Secure Border Initiative (SBI) program; personnel and infrastructure were the other two legs. Although the prototype, proof of concept P-28 system failed to meet expectations in the midst of the comprehensive immigration reform debate in the last Administration, lessons learned from P-28 were incorporated into follow on deployments of the BLOCK 1 system, which now covers about 53 miles of Arizona border and has proven effective in providing enhanced situational awareness and agent safety. *SBlnet* was cancelled because it failed to become the comprehensive "one-size-fits-all" border solution originally envisioned; however, core technology developed from the program, including networked integrated fixed towers with radars and day and night cameras, will remain important components of technologies deployed in the future, according to the information provided by DHS to the Congress. Fred Schwien, Director of Homeland Security Strategy at Boeing's Government Operations, expressed disappointment at the cancellation of the program but satisfaction that core technologies derived from *SBlnet* were shown to be effective in assisting the Border Patrol in gaining control of the border.

The history of *SBlnet* is complex and multi-dimensional due in part to the politically charged environment surrounding immigration reform and border control. Despite its recent cancellation, the program did have some success. Nelson Balido, President of the Border Trade Alliance, recently paid a





visit to explore the system and reported that, "SBI<sup>net</sup> has been instrumental in the apprehension of thousands of illegal aliens and more than \$25 million worth of narcotics seizures. Simply put, the system lets agents do their job more effectively, get home safely, and provides vastly improved security to communities along the border."

**DRS Technologies** is a leading supplier of integrated border and force protection solutions in support of DHS, military forces, intelligence agencies and prime contractors worldwide. DRS has advanced technology and subject matter expertise in systems architecture, sensors, processing, system design, implementation and production that is relevant to providing a rigorous and systematic design for border sensing solutions. DRS offers a family of security cameras, which provide low-cost, high-performance infrared technology, with a longer MTBF (mean time between failure) providing lower cost of ownership and more consistent border presence. DRS has also developed ARMOR X-CHANGE (Cross Communications Hub and Network Gateway Exchange), the next generation of communications gateways that address interoperability challenges and provide enhanced situational awareness. The gateway allows users to pass voice, video, and data over existing communications backbones or wideband data radios for both static and mobile applications.

**FLIR Systems Inc.** FLIR is a world leader in thermal imaging infrared sensors and their associated technologies. FLIR's systems detect thermal energy emitted by targets such as humans or vehicles; form a visual image; combine the image with TV, laser, and GPS data; then display, record, or transmit the image to operators for action. "These tools give border patrol the ability to see long-range under any types of conditions, day or night, and combine the thermal and visual images to tell the operator things that are much more than what your normal eye can see," says Kevin Tucker, Deputy President, Government Systems Division of FLIR. FLIR's detecting devices are currently being used along the Southwest border to successfully detect, for example, a car loaded with drugs, a person carrying a backpack, or other suspicious activity.

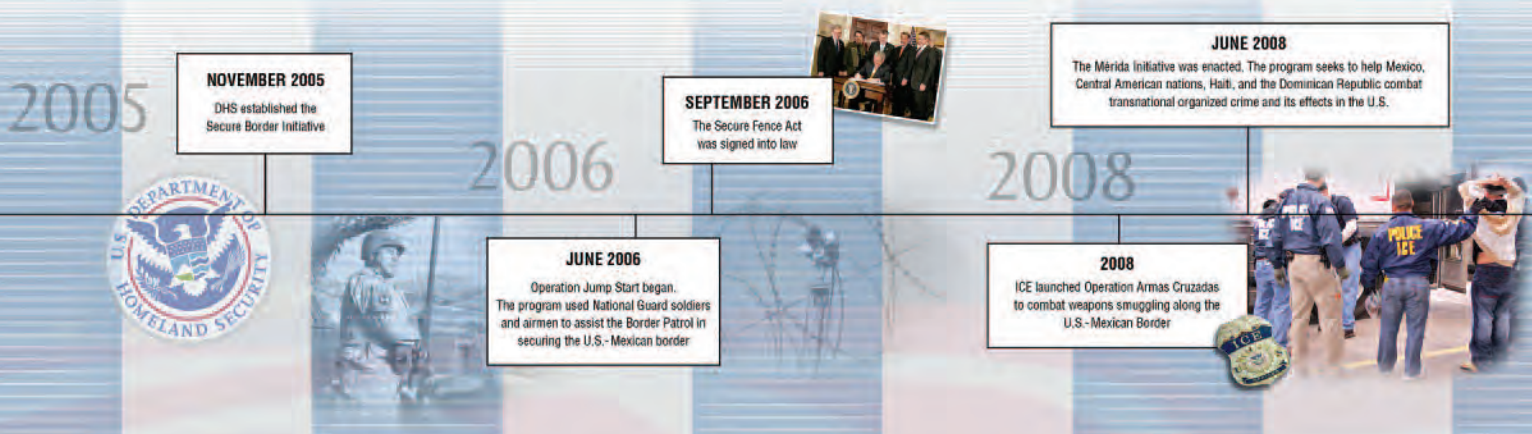
FLIR recently acquired ICx Technologies, a leader in emerging CBRNE sensor and RADAR technologies which, when integrated with FLIR cameras, provide a powerful source of data for Border Patrol. Eileen Parise, Director of Federal Programs, FLIR Government Systems Division, describes ICx's MDAS (Mobile Detection & Assessment System) which leverages multiple technologies to detect, identify and track items of interest up to 10 km away. The unit is mounted on a 450 Ford Bronco and includes a radar component which detects the item, plus a color camera and a FLIR thermal camera which track the item to determine if it is something to be pursued. This system has been a tremendously successful force multiplier for border

agents, particularly in remote areas which are hard to cover on foot. In addition, the unit is powered by its own generator and radio for communicating the radio and video data.

**ITT Defense & Information Solutions** can integrate huge amounts of structured and unstructured data (including sensor data) from a variety of data bases and networks. Mark Coomer, the Director of Homeland Security Business Development, explains; "We ingest their data (using COTS tools where possible) and put all of those feeds together to make sense of it on a geo-spatial reference map available to anyone who has access to the network. Every state, local and federal agency has deployed networks of information. This technology could help them connect the dots and give an accurate picture of imminent threats." By providing access to real-time information without needing a technological "translator," agents on the ground and in the air can get access to information when and where they need it, saving costs and time. ITT also plays a key role in protecting U.S. airspace from intrusion by suspect aircraft. ITT supports the Federal Aviation Administration's fielding of the Next Generation Air Traffic Control System (called ADSB). Still early in its fielding, this system has already improved our understanding of suspect air traffic in the Gulf of Mexico. ITT is also the prime contractor for the Tethered Aerostat Radar System, which helps identify smuggling aircraft crossing our southern border.

Anne Petera is the Director of Homeland Security Programs at **Lockheed Martin Corporation** and serves as the liaison between Lockheed Martin and DHS. Lockheed offers a suite of border protection solutions from mobile surveillance, tunnel detection, ultra-light aircraft, to a suite of biometrics capabilities. Lockheed's P-3 Airborne Early Warning and Control Aircraft and Tethered Aerostat Surveillance Systems – an integral component of U.S. border protection – provides real-time radar surveillance and defense across the Southern border for both air and surface threats. Lockheed is currently also building a prototype of a High Altitude Airship, a lighter-than-air vehicle which can be deployed at 60,000 feet. "Many of these have been deployed in the Middle East and are able to perform amazing surveillance from aerostats with long-range camera and night-vision capability and GPS tracking. We believe that's going to be a strong border solution moving forward," says Petera.

**Raytheon Company** is a major driver in efforts to enhance border security at and between ports of entry. Raytheon has decades of expertise in the deployment of command and control systems. Border View, a member of Raytheon's Clear View family of sensor integration and command & control products, was built specifically for the border security environment. Border View allows multiple sensors to "talk" to one another so that one sensor can automatically take over the tracking of an intruder when other sensors



can no longer “see” the target. The system maintains a constant track of targets to reduce false alarms, save operator time, and increase efficiency. In addition, Raytheon’s Athena C4ISR system — a network centric, multi-domain situational awareness system with functions enabling integration, analysis and knowledge management – has been deployed in support of maritime domain awareness operations along the U.S. border. Related Raytheon solutions include: tunnel detection, ultra-light aircraft detection, aerial surveillance, marine and ground surveillance radar, a marine small target tracker capability, signal intelligence & radio direction finding, plus capabilities to analyze and share both open source and classified intelligence, while maintaining privacy.

For port of entry-related needs, Raytheon’s Portera suite of systems enables collection and storage of electronic travel data, watchlist matching and alerting. Building on Raytheon’s experience with IDENT, Portera also enables the collection, cataloguing, and storage of biographic and biometric data to establish traveler identity, track traveler history, reduce visa fraud, support trusted traveler programs and enable enhanced watchlist matching. Portera also performs rules-based advanced risk assessment on arriving travelers.

## Challenges to Progress

Despite the tremendous investment made in strengthening border security, several key challenges remain.

### Expanded Domain Awareness

Even with the various technologies in place on our borders, we need more coverage – adapted to diverse terrain – and greater integration. Dr. Gary Shiffman, Managing Director of The Chertoff Group and former Chief of Staff of CBP, states, “We have made tremendous strides in collecting data and analyzing what’s crossing our borders, but we need more visibility – that should be our biggest priority. We need better information on who and what are crossing our borders and where they’re doing it.”

According to Raytheon’s Kevin Stevens, “Tactical field commanders should be able to exploit all available technology to detect, identify and classify a target of interest, but in order to do so they must be able to coordinate all of their assets. For example, when a group of drug smugglers activates an unattended ground sensor, the field commander should be able to know at a glance where to find the nearest asset capable getting ‘eyes on’ the target, and he should be able to direct that asset to provide him all available information related to the target.”

Anne Petera at Lockheed Martin also acknowledges the challenge of diverse terrain. “We have in the past sought a single solution from a single

provider when perhaps we should consider multiple solutions, each addressing a specific type of terrain or challenge. Says Eileen Parise of FLIR, “There’s no one solution that’s going to solve all 2,000 miles of border, but new products coupled with one-on-one training could make a significant impact, and quickly.”

### Technical Interoperability

The act of collecting the data itself is only half the battle. “The challenge is to make all of the intelligence and defense community’s data available for discovery by border security. Those databases could be exploited by someone sitting at a Port of Entry in El Paso so they can know whether to allow a cargo shipment in or a questionable person,” says Mark Coomer of ITT. “Information sharing is the force multiplier for homeland security. If you can fully deploy the technologies that are available, you essentially put 24,000 state and local law enforcement agencies on your team.”

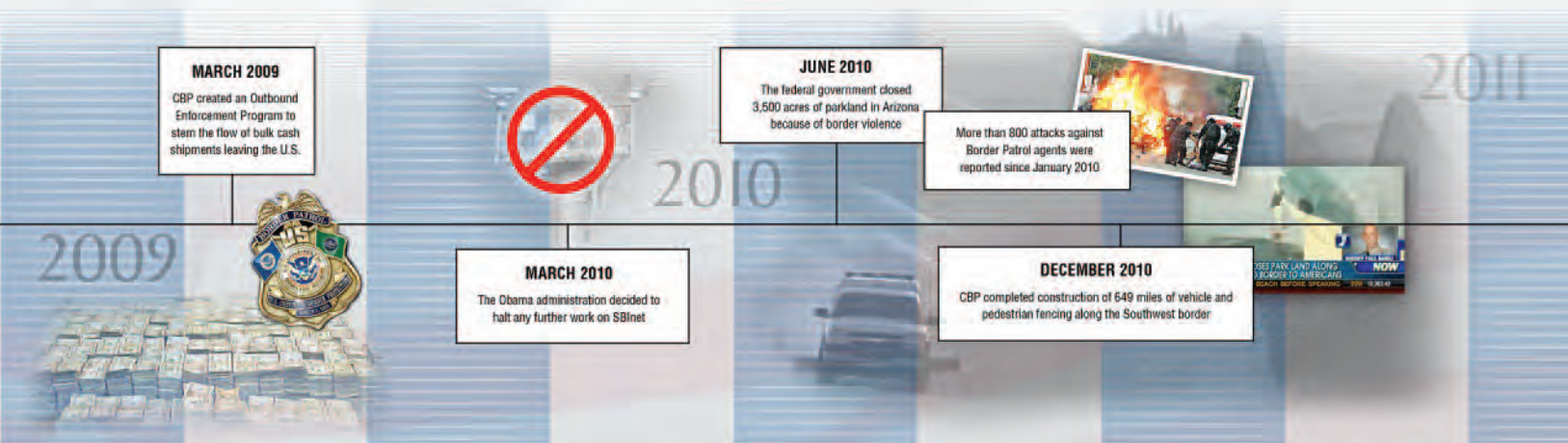
That said, the term “connect the dots” oversimplifies the challenge of information sharing, according to Raytheon’s Adam Isles. Effective identity and entity resolution, particularly for federated queries, continues to be a need, consistent with each data owner’s privacy and information sharing policies.

### Segmentation

Rules-based targeting techniques – wherein governments use historical interdiction, investigative and intelligence data to develop indicators of high-risk travel and trade – enable border security agencies to prioritize inspection resources on travelers and cargo that may warrant additional scrutiny, even if not on any specific lookout list. In the passenger environment, trusted traveler programs allow for expedited processing in exchange for an advance background check, biometric identification and interview. In the maritime cargo environment, programs such as CSI and C-TPAT provide pre-vetting to allow CBP to focus frontline inspection resources on higher risk passengers and cargo (although tampering with vetted cargo before arrival in the U.S. remains an issue). Of course, segmentation – be it through trusted traveler programs or rules – depends on effective access to (and analysis of) historical data from both CBP and partner agencies, again highlighting the importance of interoperability.

### Cargo Security

In the Implementing Recommendations of the 9/11 Commission Act of 2007, Congress required 100% rad/nuc scanning for all inbound cargo containers by July 2012. The Administration has announced it will delay implementation due to technology, logistics and manpower limitations. The recent Yemen-origin attempt to bomb air cargo flights highlights the challenge of risk assessing air cargo – which by its nature is often sent on





a just-in-time basis – for explosives in advance of departure. Partnerships with industry and foreign governments, use of mobile scanning and tracking devices deployed on a threat basis, and more robust analysis of underlying cargo data all factor into a potential strategy.

### **Border Violence and an Adaptive Adversary**

The continued influence of drug cartels presents a threat to the Mexican government and to our own national security. Because of this danger, the U.S. is increasing pressure on drug trafficking routes. Smugglers have reacted to border security improvements by changing tactics and methods of operation. They have adopted aggressive driving styles, varied the timing, size and composition of their narcotic loads, and increased their counter-surveillance of CBP. They have also increased the use of subterranean routes (drainage systems and tunnels), small “ultra-light” aircraft, and expanded maritime activity in the Pacific and Gulf of Mexico, using manned semi-submersibles (“narco-subs”) to move high-value loads. To win, it is key that the U.S. have the ability to predict shifting operational threats, and immediately confront activity with the right enforcement tactics before the criminal organizations are able to fully establish themselves in the new area of operations.

As border security is enhanced and frustrated criminal organizations compete for shrinking terrain, we can expect an increase in violence along the border. As the danger grows, stand-off, non-lethal systems offer agents a potential solution that enables them to contain a deadly threat.

Kevin Tucker of FLIR says, “The threat changes – it does not stay the same. When people realize that (their border penetration efforts) don’t work, they rapidly adapt and come up with a new way which is fast and flexible. It’s hard for us to be non-reactionary but we continue to push the edges.”

### **Resistance to Change**

“There can be resistance to trying something new. Even if the technology has been tried in the field and if the interoperability folks love it, but another decision-making group wants to keep their older, traditional solution, that hurts us,” says Michael Strange of Avaya.

### **Where Are We Now?**

Despite the challenges, the private sector maintains a creative and solution-oriented focus.

Simply getting the technology in the hands of the users could be a powerful move. “We need to bring the operators to the table,” says Eileen Parise of

FLIR. “We’re the best equipped to explain how the science works so operators can maximize its capabilities.” Bringing end-users into development is another idea which could have an immediate positive impact on a solution’s success or failure.

Adam Isles of Raytheon suggests sharing ideas and resources in the face of tighter budgets, “Can CBP and TSA leverage each other’s know-how and authorities more comprehensively? Also, different government agencies have potentially actionable data, but we need to better bring that data together to identify non-obvious relationships.”

Jack Mayer, Executive Vice President of Booz Allen Hamilton and Council Chairman, believes in addressing border security problems at their root cause. “The bottom line is that we’ve never addressed border security with a holistic approach. We can’t think of this only in terms of trying to lock down the border. The problem is larger than just an immigration problem. The biggest threat to our country is the narco-state. If that state exists in Mexico, anything is possible.” Mayer offers up a solution involving bi-national and public-private partnerships which recognize that unless we address Mexico’s economic problems, people will always take the risk to cross the U.S. border, drawn to the prospect of a better life. “Adopting a business perspective to interrupt the drug cartels’ supply chain at their distribution networks’ weak points could do serious damage to the cartels. This in turn will provide opportunities to strengthen the local population through future economic development.”

In the end, the U.S. is faced with an adaptive, changing threat environment that calls for the best use of varied technologies, in multiple layers, to protect our borders and those who patrol them. From managing those entering legally to stopping those smuggling illegal contraband – or worse, weapons of mass destruction – the U.S. must call upon all available resources and technologies. Only through the integration of local, state and federal law enforcement, federal agencies and the private sector will the nation be able to comprehensively combat the threat and stop any transgressor from inflicting harm.

*The Homeland Security & Defense Business Council (HSDBC) works to ensure that the perspective, innovation, expertise and capabilities of the private sector are recognized, respected and integrated with the public sector. The 9/10/11 Project has called upon critical thought leaders and subject matter experts, including the chief writer for this monograph, Liddy Heneghan. For more information on the Council’s 9/10/11 Project visit: [www.homelandcouncil.org/91011-Project.html](http://www.homelandcouncil.org/91011-Project.html)*

***For a more complete timeline, visit the Council’s website***

*For more information on the Homeland Security & Defense Business Council visit: [www.homelandcouncil.org](http://www.homelandcouncil.org)*

**Homeland Security & Defense Business Council** • 1140 Connecticut Avenue Suite 1008 • Washington, D.C. 20036 • (202) 470-6440

Marc A. Pearl, *President/CEO* • Kristina Tanasichuk, *Vice President & Project Director*



How do you accurately screen millions?  
In seconds.

Every day, millions of individuals and countless containers of cargo seek to enter and exit sovereign borders. Raytheon enables nations to assess and manage risk so high-risk travelers, weapons or smuggled contraband are identified in time to take immediate action. Raytheon Advanced Risk Assessment solutions gather and process data from hundreds of intelligence and information sources — and do so within seconds — in order to provide homeland security and law enforcement personnel with intelligence that's actionable and accurate. All while preserving the confidentiality and security of that data, at all times.



**INNOVATION IN ALL DOMAINS**

Visit [www.raytheon.com](http://www.raytheon.com)

Keyword: HLS-ARA

© 2011 Raytheon Company. All rights reserved.  
"Customer Success Is Our Mission" is a registered trademark of Raytheon Company.

**Raytheon**

*Customer Success Is Our Mission*