

# Effective Border Management Through Mission Critical Collaboration

by Mark Tanner & Heather Davies, Ph.D.

November 2006

CollabraSpace  
180 Admiral Cochrane Drive  
Suite 525  
Annapolis, MD 21401  
410.224.4343  
[www.collabraspace.com](http://www.collabraspace.com)

Strategic Analysis, Inc.  
One Virginia Square  
3601 Wilson Boulevard  
Suite 500  
Arlington, VA 22201  
703.527.5410  
[www.sainc.com](http://www.sainc.com)



*This document is a result of a workshop co-presented by the authors at the Border Management Summit hosted by the Institute for Defense and Government Advancement from October 23-25, 2006. The attendees included officials from federal, state and local agencies (e.g., border patrol agents, homeland security directors), policy analysts, and the private sector (e.g., program managers, business development managers).*

## **Introduction**

Since September 11, 2001, many federal agencies, including the Intelligence Community (IC), Department of Defense (DoD), Department of Homeland Security (DHS) and Department of Justice (DOJ) have been charged with improving inter- and intradepartmental communication to counter threats to homeland security and are required to involve state and local governments and the private sector. Such joint operational planning and coordination during execution is required for effective border management, and maximizing the effectiveness of operations requires collaboration. Collaboration, in this context, is not just a data sharing activity; it is a cognitive function involving real-time human interaction. It requires a dialogue, having access to experts who can evaluate the data, and provide the necessary context. The command and control methods and practices of the past, collocating personnel, conducting audio/video conferences, and/or sending and responding to emails, are insufficient given the state of technology today. Real-time collaboration can greatly enhance the quality of information necessary for decision makers when the hard decisions have to be made.

**Real-time collaboration can greatly enhance the quality of information necessary for decision makers when the hard decisions have to be made.**

This document begins with the vulnerabilities and threats at the border and the infrastructure used to protect our borders. This is followed by numerous information resources used by federal, state, local, and tribal agencies involved in protection and response. The paper discusses the push for increasing manpower and the coordination challenges created by time sensitive decision-making in a multi-organization environment. As part of the broader border security strategy, there are many joint operations whose success relies on collaboration. The paper describes how effective border management requires an ability to create and maintain situational awareness. Situational awareness in border management is satisfied with real-time data feeds, mapping tools, radar, etc. along with comprehensive collaboration tools. The paper concludes with a discussion of the requirement for not only specific assets—manpower and physical and virtual fences—but integrated response and collaboration technologies and decision support systems. Such collaboration technologies create situational awareness, aide decision-making support, and allow for participation of people in those decisions who may not otherwise have been involved. A collaboration model with proper implementation of process, procedures, and technologies will allow agencies to function as one, rather than a collection of individuals in multiple agencies supporting border security.

## **Vulnerabilities and Threats**

The vulnerabilities and threats to border security are diverse by varying geography, population, air, land, and sea. Management of risk at the border requires international cooperation as well as coordination of multiple agencies and organizations within the United States.

At Ports of Entry (POEs), vulnerabilities are created by the volume of traffic, corruption, inter-departmental coordination (or lack thereof), limited interoperability of systems, and limitations of infrastructure (i.e., fences, inspection lanes, surveillance equipment). Vulnerabilities near POEs (i.e., in surrounding communities) are complicated by the close proximity of private and commercial real estate with limited government access. Vulnerabilities in remote areas are complicated by limited or non-existent visual access and lengthy response times.

The threats exploiting these vulnerabilities include the smuggling of people, weapons, and drugs, theft of property, violent crimes of assault, murder, rape, and kidnapping, counterfeit goods. Countering the threats while allowing for legitimate commerce, is a challenging balance to achieve. Employing advanced technologies and improved business processes can mitigate risks and enhance legitimate travel and commerce.

## **Infrastructure**

As stated by DHS, “the Secure Border Initiative (SBI), (to enhance Border Management) is a comprehensive multi-year plan to secure America’s borders and reduce illegal migration which includes:

- More agents to patrol our borders, secure our ports of entry and enforce immigration laws;
- Expanded detention and removal capabilities to eliminate ‘catch and release’ once and for all;
- A comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of UAVs, and next-generation detection technology;
- Increased investment in infrastructure improvements at the border—providing additional physical security to sharply reduce illegal border crossings; and,
- Greatly increased interior enforcement of our immigration laws—including more robust worksite enforcement.”

There has been much debate about the types and the cost of state-of-the-art infrastructure for border management. The use of surveillance technologies is not a new effort. In the 1970s and 80s, the former Immigration and Naturalization Service (INS) used low-light video cameras and portable electronic intrusion-detection ground sensors. In 1997, the INS developed the “Integrated Surveillance Intelligence System” (ISIS) which deployed sensors, which proved difficult to maintain in a variety of weather conditions, and had no ability to differentiate animals from humans, etc.,

creating false alerts. In August 2004, DHS established the America's Shield Initiative, and replaced with SBI, a comprehensive multi-year plan.

U.S. Customs and Border Protection (CBP) is leading, managing and collaborating with industry integrators such as Boeing, to implement SBI net. Boeing's plan rests heavily on adapting military technology from the battlefield to the border and will help unify new and existing infrastructure, beginning with the 6,000 miles of border with the initial task order to cover 28 miles of border within the Tucson Sector. Along with staffing and response platforms, SBI's goal is to deploy a combination of multiple state-of-the-art systems and traditional security infrastructure into a comprehensive border security suite including, but not limited to, hardware and software systems, surveillance technologies, communication equipment, data analysis systems, command and control center equipment, information databases and intelligence analysis systems and dispatching systems.

For SBI net, some envision physical infrastructure including walls, fences, barriers, checkpoints, stations/bases, and all weather access roads. Whereas, others foresee a virtual fence to achieve operational control over the entire border through integrated systematic surveillance that employs detection equipment, infrared cameras, poles, ground-based sensors, infrared sensors, lighting, unmanned aerial vehicles, satellites, radars, and other high-tech tools. This will not be a 'one-size-fits all' deployment. For example, one portion of the border may require more technology solutions in relation to personnel than another portion, or may require more tactical infrastructure improvements than either personnel or technology.

The deployment of the various infrastructure components will consider current intelligence, operational environment, and field commanders' requirements. There are numerous requirements to ensure smooth data management among all land, air, space, environmental components via effective communication and collaboration. For the infrastructure to be effective, the information must be accurate, timely and appropriate. The information must be collected, recorded, monitored, transmitted, analyzed, and disseminated to the appropriate agency at the right time. The land, air, and marine infrastructure are intended to:

- Detect an entry when it occurs or is about to occur
- Identify what the entry is (vehicle, human, or animal)
- Classify its level of threat (who, how many, what)
- Respond effectively/efficiently and bring to law enforcement resolution
- Deter attempts to threaten or breach border security
- Delay penetration
- Defeat attempted penetration

There are numerous concerns about the proposed border security infrastructure. There will most certainly be technology malfunctions (e.g., false alarms), funding shortages and cost issues of implementing a state-of-the-art system, policy conflict, international coordination, and environmental issues. The information that will be

obtained from the proposed 6,000 miles of infrastructure will be difficult to manage. Information is already difficult to manage and sometimes gets to agencies and the appropriate individual too late. The requirements of a virtual fence include an ability to view the information in an understandable format and relay it to appropriate agencies. Information flow must accommodate push as well as pull requirements. Policies and procedures must not inhibit the full capabilities of the system to ensure successful collaboration and sharing of data. There are problems in collaboration with federal agencies (e.g., FAA is perceived as getting in the way of using unmanned air vehicles, creating environmental impact concerns). There is an economic impact of border security because security may slow commerce. International cooperation is essential to ensure the facilitation of legitimate trade.

Critics argue that as much as half of the illegal immigration problem is driven by the hiring of people who enter the U.S. through official border points, but use fraudulent documents or overstay visa. Additionally, physical and virtual fencing divert money away from programs that could help secure our borders by the screening of such individuals. There are critics that indicate that even the best virtual or physical fence may only be marginally effective because of the millions of illegal migrants in the U.S. entering legally through ports of entry and did not return in accordance with the terms of their visas. A means implemented to mitigate such issues is US-VISIT. A virtual fence on the Southern border will have a corresponding affect on the much longer U.S.-Canadian border. The Canadian government may need to end visa free travel from its NAFTA partner, Mexico, in order to deter transition from Mexico to the U.S., via Canada. There needs to be continued collaboration and agreements with countries and international extradition treaties.

The solutions identified by workshop participants for border security include improving international and domestic cooperation, streamlining of regulations, and modifications of policies, procedures, and laws. There also needs to be bi-national collaboration in law-enforcement and security that needs to deal with the hurdles of differences and socioeconomic disparities in federal organizational and political structures, and socioeconomic disparities across the border region, different priorities and perspectives, and regional variation.

### **Information Resources**

There are numerous information resources used in border management. Information resources include, but are not limited to open source (e.g., geographical information systems such as Google Earth), proprietary (e.g., ESRI, iMap, ChoicePoint, Lexis-Nexis, which compile public source information), or federal (e.g., ICE Enforce, DEA Narcotics and Dangerous Drugs Information System, DEA Merlin, FBI National Crime Information Center-NCIC, FBI Integrated Automated Fingerprint Identification System-IAFIS, FBI Automated Case Support, FBI Terrorist Screening Database). Special technologies provide for radiation detection, camera surveillance, and satellite imagery. There is disparate data that comes in many forms, format, times and from different agencies that must be shared. A multi-agency governance needs to address the requirements for managing the collection and dissemination of information from

SBI-net as well as accessible to SBI-net. Such governance must take into account state and local led fusion centers, federal led task forces, and intelligence community operations.

Some efforts are already addressing information sharing policies, technologies and standards (i.e., Global Justice XML Data Model (GJXDM), National Information Exchange Model (NIEM), IDENT/IAFIS interoperability, and Fusion Center Guidelines).

Biometric technologies will have a role in the SBI-net. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic including: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. The improvements in biometrics have expanded the capabilities and the amount of information. US-VISIT, an automated biometric entry-exit system, is becoming the main tool for screening travelers at the point of entry. The visitor's biometrics, such as a digital finger scan, are collected and checked against law enforcement databases. When the visitor arrives at the port of entry, CBP uses this identifier to verify the person at our port is the same person who received the visa, safeguarding against false identification. Examples of making use of biometrics include the FBI-Integrated Automated Fingerprint Identification System (IAFIS), FBI-Automated Biometric Fingerprint Identification System (IDENT), DHS-National Security Entry-Exit Registration System (NSEERS), DOS-Consular Consolidated Database, and DOS Visa Waiver Program and Biometric Passports. There are numerous implementation issues with biometrics including the integrity of the inspection process, providing technology and training to inspectors, access to intelligence information, cost, performance, security, user acceptance and standards.

Special technologies (electrochemical, mass sensors, optical sensors and biosensor) for the detection of chemical, biological, biological, and radiological threats will be employed. All of these sensors provide information that needs a timely and appropriate response from one or more agencies.

### **Agencies Involved**

Achieving border security must allow for a blend of physical resources such as equipment and personnel along with intangible elements such as useful intelligence and strong partnerships and collaboration with all the organizations involved. There are numerous international, federal, state, local, and tribal agencies involved in protection and response. Their involvement in border security depends on the activity and nature of the incident, some of which is intelligence support to avoid an incident from occurring. However, the discussion in this paper will focus on protection and response in close proximity to the physical borders.

The agencies that are involved in protection include Customs Border Protection, National Guard, sheriff offices, local police, private security and U.S. Coast Guard. Protection of our borders includes lethal and non-lethal approaches. Some of these agencies primary role for border management is protection (i.e., CBP, local police and sheriff departments of communities on the border). Others will have a secondary or

support role (i.e., providing intelligence to those with a primary role). The means to successful coordination include collocation, joint operations and task forces, and collaboration mechanism to ensure operational intelligence and situational awareness to these agencies.

The agencies involved in response include Customs Border Protection, sheriff offices, local police, state police, Immigration Customs Enforcement, FBI, DEA, and ATF. Again, some agencies primary role is response, whereas others support these primary response agencies. The agency that responds depends on where the detection occurs and the type of threat (e.g., biological, nuclear). The threats are typically not immediately identifiable and continuous communication during a response to an incident is essential. Outlined in the National Response Plan are the tactical and first responder responsibilities. However, because the role and responsibility of responding agencies is affected by the actual threat, continued clear communication between potentially affected agencies is essential.

***U.S. Customs and Border Protection (CBP).*** The CBP's top priority is to keep terrorists and their weapons from entering the United States. CBP's jurisdiction is confined to law enforcement activities at the border. CBP's immigration inspections are the initial and most vital components of enforcing U.S. immigration laws and assuring border security. CBP is charged with overseeing commercial operations, inspections and land border patrol functions. CBP provides the front line responder's to immigration and customs violations and serves as the law enforcement arm of DHS.

CBP employs three types of inspections in order to streamline the border crossing process: 1) verify travel documents 2) ensure all imports and exports comply with U.S. law and regulations, collect and protect U.S. revenue, and guard against smuggling of contraband 3) agriculture inspections at POE. CBP administers the US Visit Program requiring all incoming non-immigrant aliens to submit to a biometric scan.

***Bureau of Immigration and Customs Enforcement (ICE).*** ICE was created in March 2003, as the largest investigative branch of the DHS. ICE investigates immigrations and customs violations in the interior of the country. ICE's mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks. ICE mandates include uncovering national security threats such as weapons of mass destruction or potential threats, identifying criminal aliens for removal, probing immigration-related document and benefit fraud, investigating work-site immigration violations, exposing aliens and contraband smuggling operations, interdicting narcotics shipments, and detaining illegal immigrants and ensuring their departure (or removal) from the U.S.

***U.S. Coast Guard (USCG).*** The USCG is responsible for maritime and port security aspect of homeland security. Its primary jurisdiction is the protection of U.S.

ports and waterways. The Coast Guard is responsible for maritime drug interdiction, illegal migrant interdiction, as well as enforcement of US maritime law.

**State and Local Agencies.** State and locals are sometimes the first to witness immigration violations. They encounter individuals in transit at the border and within the U.S. during regular law enforcement operations, including traffic stops, arrests, etc. They are a critical component to stop and identify illegal immigrants who are trying to or have entered the U.S.

**U.S. National Guard.** The National Guard supports and assists DHS' security efforts, particularly with the Border Patrol as their new agents are trained and added. The Administration is coordinating with governors for the deployment of up to 6,000 National Guardsmen to the southern border. National Guard units will assist DHS by operating surveillance systems, analyzing intelligence, installing fences and vehicle barriers, building patrol roads, and providing training.

**Bureau of Land Management.** Additional Border Patrol agents and technology improvements have generally been deployed to the more populated areas near POEs. This has forced smuggling activities to more remote locations, such as the properties managed by the Department of the Interior. Bureau of Land Management mission involves managing the land for a variety of purposes relating to the conservation, preservation, and development of national resources, as well as land set aside for the use, occupancy, development, and governance by federally recognized tribes. Land management law enforcement officials have indicated that responding to increasing levels of illegal drug smuggling and border crossings have diverted their staff from more traditional law enforcement activities, such as routine patrols, traffic control, and wildlife enforcement activities.

There are requirements necessary for DHS and the Department of the Interior to collaborate on interagency efforts to enhance border management and at the same time prevent environmental degradation and lessen the threat of danger on land management by the Department of the Interior caused by illegal cross-border traffic. First, there is a need to coordinate the development and sharing of threat assessments. Second, there is a need to coordinate the development of plans for infrastructure and technology building on or near federal lands. Third, there needs to be coordination and sharing of information about operations and changes in personnel on or near federal lands.

### **Manpower Causes Collaboration Challenges**

Accomplishing border security takes tremendous manpower from state, local, tribal governments, federal government—DHS, DOJ, DOS, international partners, and the private sector. There has been a push for more manpower to assist with border security. More personnel leads to more coordination challenges. More information can result in information overload and make finding relevant information extremely difficult. There needs to be clearly delineated respective roles and responsibilities to prioritize and optimize resources. Local assets dedicated to national missions, limits

their availability for local operations. Assets need to be on standby to respond to certain situations. There are differences in priorities, security clearance levels, training and staff expertise that limit asset coordination. There needs to be common and integrated objectives among agencies to ensure they are complementing, not competing with each other. Collaborative mission planning (e.g., communication, policy, jurisdiction) will assist operational and jurisdictional issues.

Expanding the number of Border Patrol agents is one of the core elements of long-term border reform. The size and budget of the Customs Border Patrol has increased dramatically and additional agents are being trained and assigned. There were 9,096 agents when President Bush took office. Today there are approximately 11,600 (27% increase) agents, and by December 2008 there may be approximately 18,300 (101% increase). DHS has tripled the number of Border Patrol Agents along the northern border and doubled the number of inspectors.

Some studies have found no effect of the increase in Border Patrol, while others indicate a positive or negative relationship between border enforcement and illegal immigration. Aside from its questionable effectiveness of even increasing manpower, such a policy comes with numerous hurdles and collaboration challenges. The hurdles and the requirements for collaboration include managing attrition; finding qualified applicants who are willing to work in unpleasant weather, working away from family, lower paying jobs than other federal jobs; cost; hiring and training a recruiting department to target right audience, increase pay and benefits, engage the private sector in recruiting; consideration of private security firms; training capacity and standards; and managing increase in border patrol and collaboration with other agencies.

There are a number of other agencies that have expanded the number of personnel to address border management. For example, Operation Jump Start provided supplemental funds for National Guard support. In addition to acting as a force multiplier through the critical support they provide, these National Guard personnel have allowed Border Patrol Agents to return from administrative non-law enforcement duties to front-line patrol for border operations, apprehensions, and interdictions.

There are numerous other federal agencies that are supporting border security. For example, 300 additional, full-time Drug Enforcement Administration agents (60 each year for the next 5 years) will be hired, trained and deployed to the Southern border to address narcotics trafficking and money laundering. Also, 250 additional, full-time active duty Deputy U.S. Marshalls—50 each year for the next five years—will be hired, trained and deployed to the Southern border to address narcotics trafficking and money laundering. There are significant funding increases for ICE criminal investigators, fugitive operations teams, and detention beds.

Volunteer groups could perform functions to augment law enforcement and there has been a push to ensure accreditation, standards, and practical employment concepts. State Defense Forces (SDFs) are authorized under federal law as the principal

volunteer organizations for assisting in border control. Contractors have also been used to assist law enforcement functions, even if only temporary.

### **Response and Coordination**

In conjunction with federal, state, and local partners, and as part of the broader border security strategy, DHS and other Federal agencies have launched major joint operations to target drug trafficking, violent street gangs, and other criminal elements within our communities. There are numerous operations focused on specific crime problems (e.g., drug trafficking, immigration operations, stolen art, counter drug operations, money laundering), but few which comprehensively address a multitude of crime problems. DHS specific operations include:

***Operation Community Shield.*** Launched in March 2005, targets violent gangs that pose a threat to our communities and present concerns for national security. Operation Community Shield has resulted in the arrest of more than 3,100 gang members from more than 300 different gangs

***Operation Return to Sender.*** ICE agents and officers apprehended approximately 2,200 criminal aliens, illegal alien gang members, fugitive aliens, and other immigration status violators as part of a nationwide interior immigration enforcement effort. Roughly half of the individuals arrested had criminal records, and roughly 370 were members or associates of violent street gangs, including Mara Salvatrucha (MS-13)

***Integrated Border Enforcement Teams.*** Canada and the United States have identified certain geographical areas for the deployment or enhancement of Integrated Border Enforcement Teams (IBETs). IBETs are a prime example of Canada-U.S. law enforcement working together to protect our common border. Agencies included in IBETs are the Royal Canadian Mounted Police, Canada Border Services Agency, U.S. Coast Guard, Customs and Border Protection/Border Patrol, and U.S. Immigration Customs Enforcement. IBETs focus on criminals and terrorists that may attempt to cross the Canadian and U.S. border. These are cooperative unions of law enforcement agencies from all levels of government, and from both sides of the border that have been used at our most vulnerable areas. This unprecedented, collaborative effort has resulted in greatly enhanced intelligence sharing and integrated law enforcement operations along the northern border.

**Border Enforcement Security Task Forces (BEST).** BEST acts as a fusion center for federal, state, tribal and local law enforcement, and intelligence entities in identifying and combating emerging and existing threats. The challenge of these joint operations is coordination of planning, as well as, anticipating how the results may impact other agencies and/or locations. For instance, enhanced security at the Mexican border may shift illegal activities to maritime ports of entry.

### **Situational Awareness**

Effective border management also requires an ability to create and maintain situational awareness. Situational awareness in border management may be satisfied with real-time data feeds, mapping tools, radar, etc. along with comprehensive collaboration tools. Situational awareness means many things to many people. In a military context, it meets an objective to put the right asset on target, on time. However, in the border management context it means what is the threat, what is the right target, and what is the right response? Situational awareness must first allow for detection of the threat and then provide information relative to the size and complexity of the threat (i.e., is the intrusion by human, animal, or vehicle, is the weapon conventional, chemical, biological or nuclear, is the threat still beyond the border)?

Response to the threat requires another level of situational awareness. Commanders must know what and where their assets are located. There are now multiple agencies and multiple databases and imagery available. In order to avoid too much data, information and intelligence must be relevant to the mission.

Information resources are available in many forms. There must be a common access to documents and applications where appropriate. SBInet will provide for a virtual fence with sensor and imagery data. There is enhanced entry and exit information available from US-VISIT, integrated fingerprint identification data, and criminal history information. Intelligence information and threat reporting is now shared more extensively.

The situation will dictate the kind of response (i.e., an investigation or command post operation). The situation will also determine how to staff the response, including the skills necessary, number of personnel, location of personnel, and specific agency or organizations' participation. Once assembled, either by collocation or by network, several modes of human interaction will ensue with subject matter experts. There will undoubtedly be in-person meetings, online chat, instant messaging, audio/video conferences, email messages, and sharing of documents.

Whether the command and control involves an investigative response or command post operation, there are certain fundamental things that will occur. The Department of Homeland Security National Response Plan (December 2004) provides for

*“Awareness, prevention, and preparedness efforts that will be given similar emphasis to that traditionally afforded to the response and recovery domains. To make the response and recovery aspects of our nation’s readiness system as efficient and effective as possible, a cooperative national effort is essential, one with a unified approach to incident management and with the ultimate goal of a significant reduction in our nation’s vulnerability over time. Successful implementation of this new paradigm is critically dependent on information-sharing, consistent and timely communication between all institutions that are party to the National Response Plan, and a common planning framework that captures valuable best practices across the spectrum of contingencies.”*

If there has been an incident at the border (i.e., discovery of a weapon of mass destruction), the command must:

- Establish an inner perimeter
- Evacuate injured and innocent
- Coordinate outer perimeter requirements
- Open communication within and outside the Command Post
- Begin initial reporting and tactical planning
- Initiate verbal containment through negotiation, as appropriate
- Provide medical response, if necessary
- Contact and coordinate with other agencies and organizations

When managing a command post there are certain functional components that must be in-place. These include:

- Operational component—Responsible for investigative action (i.e., setting and covering leads).
- Intelligence component—Responsible for analyzing results of information collected by the Operational component, as well as, all source intelligence, providing same to command leadership.
- Administrative and technical support—Responsible for technical resources, to include information technology, technical coverage, and special operations equipment, as necessary. Also, responsible for personnel, supplies, and logistics to support the command post operations.
- Tactical Operations—Tactical operations may include Special Weapons and Tactics (SWAT), surveillance, and/or crisis negotiators, as necessary.
- Media and Public Affairs—Responsible for coordination and release of public information, as necessary.

### **Technologies and Decision Support Systems**

In addition to focusing on specific assets (manpower and fences) attention should also be paid to building integrated response and collaboration technologies and decision support systems. Technologies are needed to work outside the confines of daily activities and across organizations, agencies, and geographically dispersed across borders. All the personnel and agencies are not in the same building,

city/town/state and there must be ways to coordinate. Most border security personnel today use web sites and email for communication and coordination within and outside their organizations. The command and control methods and practices of the past, collocating personnel, conducting audio/video conferences, and/or sending and responding to emails, sending intelligence assessments and soliciting comments, and/or meeting periodically are insufficient given the state of technology today. Policies and procedures also inhibit them from successful collaboration. Several networks have been established to share information (i.e., Homeland Security Information Network-HSIN, Law Enforcement Online-LEO, Regional Information Sharing System Network-RISNET, and Intelink). Information is generally published and email services are provided, but real-time interaction does not occur over these networks. Additionally, security classification is still continuing to limit information sharing from federal agencies to local ones. Collaboration is core to work in fusion centers environment. Real-time collaboration tools can greatly enhance the quality of information necessary for decision makers when the hard decisions have to be made. With effective collaboration, information may be evaluated in a proper context, resulting in more timely, higher quality, and generally better decisions.

A new collaboration model with proper implementation of process, procedures, and technologies will allow communities to function as one team, rather than a collection of individuals in multiple agencies supporting border security. Effective collaboration requires human interaction to support cognitive work and greatly improve the productivity for border security. The mission critical requirement for collaboration is comprised of organizations whose success depends on collaboration. Collaboration affects any organization that must share and assess large amounts of data under time-sensitive conditions, often among dispersed workforces, both internally and with external constituents. These organizations, both public and private, also have a need to access experts who can evaluate the data, providing necessary context.

**Collaboration affects any organization that must share and assess large amounts of data under time-sensitive conditions, often among dispersed workforces, both internally and with external constituents.**

Collaboration tools will also improve inter- and intradepartmental communication. Collaboration tools, such as CollabraSuite®, may include shared documents, chat, whiteboards, presence awareness, paging, web conferencing, and/or audio-video conferencing. Effective collaboration will involve one or more of these components, will be a comprehensive application of communication options, and will be real-time.

Situational awareness may be satisfied with real-time data feeds, mapping tools, radar, etc. along with comprehensive collaboration tools. The types of technologies available include:

- **Document Storage and Retrieval**—sharing documents, securing access to documents, and read/write privileges and organizing those documents according to communities of interest and/or relevance
- **Presence Awareness**—knowing who's available, their expertise, and being able to contact them when necessary. Also, an ability to know who's online and participating in a collaborative session without taking role call as is currently done for conference calls and some video conferences
- **Instant Messaging and Paging**—an ability to communicate one-to-one and alert members to new activities whether or not they are online
- **Audio/Video and Webconferencing**—real-time communications for online meetings
- **Whiteboard**—creation of an image wherein participants can draw and make annotations
- **Wireless access**—utilization of notebook computers and/or personal digital associates (PDAs) for collaboration with deployed participants
- **Web-based Software**—timely collaboration and interagency participation will not allow for client application software loading
- **Open Standards**—enabling collaboration across multiple agencies architecture (i.e., PC, Mac, Linux, etc.)

These same technologies can be used for managing the planning of operations, collection of intelligence, and response. In addition, work-flow applications can be necessary to ensure proper authorities are informed and making decisions when appropriate.

## Conclusion

Border management is currently focused on infrastructure and information resources used by federal, state, local and tribal agencies to protect and respond to incidents at our borders. Effective border management requires an ability to create and maintain situational awareness. As manpower increases and more joint operations are established it is essential to improve coordination and collaboration. Border management requires manpower, physical infrastructure, and virtual fences but, more importantly an integrated response and collaboration technologies and decision support systems. A collaboration model with proper implementation of process, procedures, and technologies will allow agencies to function as one supporting border security. Collaboration tools will ensure that officials are making appropriate decisions with real-time input, comprehensive information, in the proper context for effective border management.

The new collaboration model is network centric. People are able to be connected and participate in decisions regardless of their physical location. Information resources are appropriately organized and secured to provide common operating pictures and situational awareness to decision-makers. Real-time collaboration provides for communication (i.e., chat, instant messaging, and audio/video conferencing), information sharing (i.e., document storage and retrieval, whiteboards, and webconferencing), and access to business applications. The new collaboration model promotes efficiency by providing access to appropriate information resources and effectiveness by allowing subject matter experts to support the decision process.

## About CollabraSpace

Headquartered in Annapolis, Maryland, CollabraSpace is an authority on web-based collaboration solutions for a wide variety of customers with dispersed workforces. The company develops and provides secure web-based collaboration systems that include audio/video sharing, document sharing and storage, whiteboarding and instant messaging, as well as a J2EE application development platform. More information about CollabraSpace can be found at [www.collabraspace.com](http://www.collabraspace.com).

## About Strategic Analysis

Strategic Analysis, Inc. (SA), a small service-disabled, veteran-owned professional services company, was founded in 1986 to provide U.S. government and private sector clients with the best in scientific and engineering services, policy studies and analysis, strategic planning, and program management support. The company's core business is in supporting research and development in the national defense and homeland security communities for identifying and deploying new capabilities and concepts. Strategic Analysis currently encompasses five professional service areas: Management and Programmatic Services; Policy and Strategy Services; Science and Technology Consulting; Information Technology Projects and Services; and Systems Engineering.

